U.S. CUSTOMS AND BORDER PROTECTION

DIRECTIVE NUMBER:
4320-025B

DIRECTIVE TITLE:
Disclosure of CBP Information to Foreign Authorities

EFFECTIVE DATE:
April 20, 2023

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

1300 Pennsylvania Avenue, NW
Washington, DC 20229

U.S. Customs and Border Protection

Commissioner

April 20, 2023

MEMORANDUM FOR: All CBP Personnel

FROM: Troy A. Miller
Acting Commissioner

SUBJECT: U.S. Customs and Border Protection Directive 4320-025B: *Disclosure of CBP Information to Foreign Authorities*

To ensure that U.S. Customs and Border Protection (CBP) is providing personnel with adequate guidance related to disseminating CBP data – and to guarantee that we remain compliant with established laws and U.S. Department of Homeland Security (DHS) policy – I have signed an updated version of CBP Directive 4320-025B, *Disclosure of CBP Information to Foreign Authorities*.

This directive is designed to provide you with procedures and practices for the disclosure of CBP-collected and CBP-maintained information (including records containing personally identifiable information) to foreign authorities. The directive was updated to: 1) align with the information-sharing process outlined in CBP Directive 4320-033: *Domestic Sharing of CBP Information for Law Enforcement and Security Purposes*; and 2) articulate the various authorities under which sharing with foreign authorities occurs at CBP.

CBP Directive 4320-025B applies to: 1) all information-sharing pursuant to 19 U.S.C. § 1628; 2) mutual assistance agreements and arrangements in place between the United States, DHS, or CBP and the requesting foreign governments or multilateral governmental organizations; and 3) any disclosures of information by CBP to foreign authorities consistent with the authorities and functions of CBP to enforce the customs, immigration, and other laws of the United States.

CBP DIRECTIVE NO. 4320-025B

DATE: April 20, 2023
ORIGINATING OFFICE: OC-PDO
REVIEW DATE: April 20, 2026

SUBJECT: DISCLOSURE OF CBP INFORMATION TO FOREIGN AUTHORITIES

1. PURPOSE

This Directive is designed to provide U.S. Customs and Border Protection (CBP) personnel with procedures and practices for the disclosure of CBP-collected and maintained information, including records containing personally identifiable information (PII), to foreign authorities.

2. SCOPE

This Directive applies to all personnel as defined in Section 5.12, particularly those individuals involved in the sharing of CBP-collected and maintained information with foreign authorities. This Directive applies to all information sharing pursuant to 19 U.S.C. § 1628; mutual assistance agreements and arrangements in place between the United States, the U.S. Department of Homeland Security (DHS), or CBP and the requesting foreign governments or multilateral governmental organizations; and any disclosures of information by CBP to foreign authorities consistent with the authorities and functions of CBP to enforce the customs, immigration, and other laws of the United States.[1]

This Directive does not apply to, nor permit, the sharing of classified national security information with foreign authorities.[2] This Directive does not supersede or otherwise affect existing and future agency policies regarding a demand, such as a subpoena, for official information in the possession of CBP for use in a foreign proceeding where the United States is not a party. Such demands shall continue to be processed pursuant to 19 CFR § 103.27.

3. POLICY

3.1 This Directive applies to all CBP personnel.

3.2 This Directive applies to the sharing of CBP-collected and maintained information with foreign authorities.

---

[1] Requests from foreign authorities processed under this Directive may include, but are not limited to, Letters Rogatory, Letters of Request, requests made pursuant to an existing Customs Mutual Assistance Agreement or Mutual Legal Assistance Treaty (MLAT), or through the Department of Justice's Office of International Affairs.
[2] Criteria for release of Classified National Intelligence is established by the Office of the Director of National Intelligence (ODNI) through *Intelligence Community Directive (ICD) 403, Foreign Disclosure and Release of Classified National Intelligence.*

3.3 This Directive provides procedures for all CBP personnel to ensure that the dissemination of CBP-collected and maintained records, including those containing PII, comply with all applicable laws, regulations, and policies.

3.4 The procedures set forth in this Directive must be followed for any sharing that is within the scope of this Directive before records maintained by CBP may be disseminated to a foreign authority.

> **3.4.1** The procedures set forth in this Directive are designed to ensure that all disclosures of CBP data to foreign authorities conform with applicable laws, regulations, and policies.

3.5 This Directive follows and implements DHS Directive 262-16, DHS Instruction 262-16-001, DHS Directive 047-01, DHS Instruction 047-01-001, and DHS Instruction 047-01-005. Any previous conflicting CBP Directives, policy statements, and manual supplements regarding CBP's disclosure of CBP data to foreign authorities, including CBP Directive 4320-025A, Disclosure of Official Information to Foreign Authorities, are superseded by this Directive.

3.6 This Directive does not supersede CBP policies pertaining to the disclosure of particular data which may require special coordination or handling in accordance with law and policy or the disclosure of which may be restricted by policy, to include, for example, Passenger Name Record (PNR)[3] data or other information accessed through the Automated Targeting System (ATS),[4] as well as protected person information (Violence Against Women Act (VAWA), T, and U visa holders).[5]

4. AUTHORITIES/REFERENCES

4.1 The Privacy Act of 1974, as amended (5 U.S.C. § 552a) (including the System of Records notices (SORNs) for applicable systems in which information is maintained pursuant to statutory authority)

4.2 Judicial Redress Act of 2015, Pub. L. 114-126 (JRA)

4.3 "Penalties for disclosure of information" (8 U.S.C. § 1367)

4.4 "Disclosure of confidential information generally" (18 U.S.C. § 1905)

4.5 "Exchange of information" (19 U.S.C. § 1628)

4.6 "Mandatory advance electronic information for cargo and other improved customs reporting procedures" (19 U.S.C. § 1415)

---

[3] CBP Directive No. 4320-035: Use and Disclosure of Commercial Air Passenger Name Record Data, (January 20, 2022).

[4] Memorandum on the Disclosure of Traveler, Cargo, and Conveyance Information from the Automated Targeting System (ATS), (July 14, 2015).

[5] CBP Directive No. 1450-023: Maintenance, Use, Sharing, and Protection of Section 1367 "Protected Class" Information, (December 17, 2019).

4.7 "Procedure in the event of a demand for CBP information in a foreign proceeding" (19 CFR § 103.27)

4.8 "Release of information to foreign agencies" (19 CFR § 103.33)

4.9 "Disclosure to third parties" (8 CFR § 208.6)

4.10 "Federal Information Policy - Purposes" (44 U.S.C. § 3501)

4.11 "Privacy Officer" (6 U.S.C. § 142)

4.12 "Disclosure of records and information" (6 CFR, Chapter 1, Part 5)

4.13 DHS Sensitive Systems Policy Directive 4300A, Version 13.2, (September 2022)

4.14 DHS Delegation 7010.3 "Delegation of Authority to the Commissioner of U.S. Customs and Border Protection"

4.15 DHS Directive 215-01-001 "Disclosure of Section 1367 Information to National Security Officials for National Security Purposes"

4.16 DHS Instruction Number 002-02-002 "Implementation of Section 1367 Information Provisions"

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

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

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

4.20 DHS Instruction 047-01-007 "Handbook for Safeguarding Sensitive Personally Identifiable Information (PII)" (December 4, 2017)

4.21 DHS Directive 262-16 "DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information" (May 4, 2022)

4.22 DHS Instruction 262-16-001 "DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information" (May 4, 2022)

4.23 CBP Commissioner Delegation Order (DO-18-210): "Delegation of Authority to Disclose Information to Foreign Governments" (March 7, 2019)

4.24 CBP Directive 2120-010A "Privacy Policy, Compliance, and Implementation" (June 29, 2022)

4.25 CBP Directive 1450-015 "Disclosure of Business Confidential Information to Third Parties"

4.26 CBP Directive 1450-023 "Maintenance, Use, Sharing, and Protection of Section 1367 'Protected Class' Information"

4.27 CBP Directive 4320-035 "U.S. Customs and Border Protection Use and Disclosure of Commercial Air Passenger Name Record Data"

5. DEFINITIONS

5.1 CBP Privacy Officer: The senior privacy official within CBP with primary responsibility for privacy compliance and policy, including: 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 personnel; contributing CBP information responsive to the public reporting requirements of the DHS Privacy Office; and communicating CBP privacy initiatives, both internally and externally.

5.2 Certified Records: Records that, through attestation by the custodian of the system in which the record is maintained, serve as the official record maintained by CBP. Certified records are often required for federal, state, and local Law Enforcement agencies seeking warrants; to set court, trial, prosecution, or grand jury dates and discovery; or to meet other requirements involving litigation to which such agencies are party.

5.3 Classified National Security Information: Information that has been determined, pursuant to Executive Order 13526, as amended, or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status.

5.4 Customs Mutual Assistance Agreements (CMAAs): Government-to-government agreements that assist CBP and DHS in ensuring compliance with any customs law or regulation enforced or administered by CBP. Note that U.S. Immigration and Customs Enforcement (ICE) is also covered by such agreements. Generally, CMAAs are used to assist in investigative, judicial and quasi-judicial proceedings involving suspected violations of the customs laws enforced by CBP and ICE and to assist foreign customs administrations undertaking comparable actions. Review of a particular CMAA is necessary to determine the scope of cooperation intended.

5.5 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.

5.6 Foreign Authorities: Any foreign governments or multilateral governmental organizations, or representatives thereof.

5.7 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 records related to covered persons, as defined by the JRA.

5.8 Need-to-know: A determination made by an authorized holder of information that a prospective recipient requires access to specific information to perform or assist in a lawful and authorized governmental function, i.e., access is required for the performance of official duties. For an example of how the "need-to-know" standard is employed, see the Privacy Act of 1974 (5 U.S.C. § 552a(b)(l)).

5.9 Law Enforcement Purpose: An activity conducted by an appropriate authority charged with investigating or prosecuting a violation, or enforcing or implementing a law, rule, regulation, or order.

5.10 Law Enforcement Sensitive Information: Information that requires confidentiality protections because of the potential negative impact unauthorized disclosure would have on law enforcement activities and effectiveness. Unauthorized release of such information could interfere with law enforcement investigations and proceedings, deprive a person of a fair trial, disclose the identity of a confidential source, disclose techniques and procedures used by law enforcement which could be used to circumvent the law, endanger the physical safety of an individual, including a law enforcement officer, and undermine the agency's ability to receive information to facilitate its mission responsibilities.

5.11 Personally Identifiable Information (PII): Any information that permits the identity of an individual or person 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.[6]

5.12 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.

5.13 Record: Any item, collection, or grouping of information about an individual or person that is maintained by an agency, including their name, identifying number, symbol, or other identifying particulars.[7]

---

[6] *See* 5 U.S.C. § 552a. 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). In some instances, Business Identifier Information (BII) collected by CBP can qualify as PII, including when such data is linked with a particular individual.

[7] 44 U.S.C. § 3301 further defines Records as including all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the

5.14 Routine Use: The purposes for disclosure of a record from a System of Records outside of DHS which is compatible with the purpose for which it was collected and in accordance with the conditions of disclosure under the Privacy Act. Routine Uses are included in an agency's System of Record Notices and are published in the Federal Register.

5.15 System of Records: A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual.

5.16 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; the ways in which the information is generally shared by the agency; and notice of the mechanisms available for individuals to exercise their Privacy Act rights to access and correct the PII that CBP maintains about them.[8]

6. RESPONSIBILITIES

6.1 All CBP personnel with access to records maintained by CBP, including travel and encounter data, trade data, case files, and other information or intelligence products are responsible for:

6.1.1 Complying with this Directive and with privacy and information sharing policies[9] and procedures issued by the DHS Chief Privacy Officer or by CBP's Privacy Officer;

6.1.2 Ensuring that any disclosure of PII belonging to individuals covered by the Privacy Act (U.S. Citizens and Lawful Permanent Residents (LPR) and the Judicial Redress Act (JRA))[10] are:

6.1.2.1 Made from a CBP System of Records to a foreign authority in accordance with a Routine Use that has been established and described in the relevant SORN for the system from which the records originated.[11]

---

organization, functions, policies, decisions, procedures, operations or other activities of the Government or because of the informational value of the data in them.

[8] *See* 5 U.S.C. § 552a(e)(4).

[9] For the purposes of this Directive, there is no distinction between formal and informal sharing of information. Any CBP data provided proactively or in response to a request from Foreign Authority, regardless of the format of the sharing (oral or in writing) is considered a disclosure and all requirements of this Directive apply.

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

[11] 5 U.S.C. § 552a(b)(3).

6.1.2.2 Provided only to a party with a need-to-know in the performance of their official duties.[12]

6.1.3 Ensuring that any disclosures of PII from a CBP System of Records to a party outside of DHS are properly accounted for;

6.1.4 Protecting PII from unauthorized disclosure, including preventing releases of information that are not compliant with established policies, information sharing agreements, or have not been authorized by the CBP Privacy Office; and

6.1.5 Coordinating with the CBP Privacy Office (privacy.cbp@cbp.dhs.gov) and/or the Office of Chief Counsel, as necessary, when questions related to the sharing of CBP-collected and maintained records containing PII with Foreign Authorities arise:

6.1.5.1 Consideration should be given to whether the disclosure of PII is necessary and prudent, balancing the privacy interests of the individual with the law enforcement need of the Foreign Authority receiving CBP records. Any questions or concerns related to the inclusion of PII in a disclosure should be directed to the CBP Privacy Office; and

6.1.5.2 Any disclosure of records for use in foreign judicial proceedings shall be coordinated through the Office of Chief Counsel via the Associate Chief Counsel (Enforcement and Operations) or a local Office of the Associate or Assistant Chief Counsel.

6.2 The CBP Privacy Office is responsible for:

6.2.1 Overseeing the implementation of information disclosure processes at CBP and ensuring compliance with established legal and DHS policy requirements;

6.2.2 Providing guidance to operational offices, officers, agents, and analysts regarding matters related to the disclosure of information, ***specifically for requests involving the use of CBP records containing PII in support of investigations***;

6.2.3 Reviewing proposed agreements and arrangements, and updates to established agreements and arrangements, involving the disclosure of CBP records to external parties to ensure compliance with established policy requirements; and

[12] CBP applies the same "need-to-know" concept to disclosures outside of DHS as is required for disclosures within the Department pursuant to 5 U.S.C. § 552a(b)(1), which requires that records only be shared with individuals who have a need for the record in the performance of their duties.

6.2.4 Conducting evaluations of agency information disclosure processes and ensuring compliance with this Directive.

6.3 The Office of Chief Counsel is responsible for:

6.3.1 Providing CBP personnel with legal guidance regarding matters related to the disclosure of information, ***especially for requests involving the use of CBP records in foreign judicial proceedings***; and

6.3.2 Reviewing proposed agreements and arrangements, and updates to established agreements and arrangements, involving the disclosure of CBP records to external parties to ensure compliance with established legal requirements.

7. INFORMATION SHARING

7.1 Information collected and maintained by CBP may be disclosed to appropriate representatives of Foreign Authorities with a need-to-know such information, consistent with applicable law, relevant agreements and arrangements, and policies, including those set forth in this Directive.

7.2 CBP will manage the disclosure of information to Foreign Authorities to ensure the security of the United States and the safety of the U.S. public and U.S. official personnel.

7.2.1 It is the policy of CBP not to provide information to representatives of a Foreign Authority where such information is requested on behalf of a private party for use in a civil proceeding, administrative action or private matter, unless required pursuant to an applicable international agreement and otherwise permitted by U.S. law.

7.2.2 All disclosures of CBP information to Foreign Authorities will conform with applicable law, including, but not limited to, the Privacy Act of 1974 (5 U.S.C. § 552a); the E-Government Act of 2002 (44 U.S.C. § 3501 note); the Trade Secrets Act (18 U.S.C. § 1905); the Computer Security Act (40 U.S.C. § 759); the Bank Secrecy Act (31 U.S.C. § 5311, et seq); and the Trade Act of 2002, as amended (19 U.S.C. § 1415(a)(3)(F));[13]

7.2.3 All disclosures of CBP information to Foreign Authorities will conform with established agency data protection policies,[14] such as those associated with Passenger Name Record (PNR) data;[15] Protected Class Data

---

[13] Requests from Foreign Authorities for advance electronic export data for purposes that fall outside of the purposes outlined in 19 U.S.C. 1415(a)(3)(F), should be referred to the Department of Commerce, United States Census Bureau for handling in accordance with Title 15 § 30.60 Confidentiality of Electronic Export Information.

[14] All CBP Policies and Directives are available via the PODS tool at https://pods.cbp.dhs.gov/.

[15] CBP Directive No. 4320-035, U.S. Customs and Border Protection Use and Disclosure of Commercial Air Passenger Name Record Data (January 20, 2022) (PNR Directive), or any superseding PNR Directive.

(Violence Against Women Act (VAWA), T, and U visa holders); [16] and information collected from electronic devices during border searches;[17] CBP personnel will also abide by general non-disclosure requirements of information associated with Asylum and Credible Fear Applications,[18] Protected Class Data, Advance Cargo Information, and any other applicable non-disclosure requirements;

7.2.3.1 Information relating to noncitizens who are seeking or have been approved for immigrant status as battered spouses, children and parents under provisions of the Violence Against Women Act (VAWA), as victims of a severe form of human trafficking or as noncitizens who have suffered substantial physical or mental abuse and are cooperating with law enforcement authorities, including applicants or beneficiaries of the T Visa, U Visa, or VAWA protections, may not be shared with a Foreign Authority unless authorized by DHS Instruction Number 002-02-001 or DHS Instruction Number 215-01-001, and pursuant to CBP Directive 1450-023 implementing such directive and instructions; and

7.2.3.2 Pursuant to 19 U.S.C. § 1415(a)(3)(F), advance cargo information collected by CBP may only be used for "ensuring cargo safety and security, preventing smuggling, and commercial risk assessment targeting, and shall not be used for any commercial enforcement purposes, including for determining merchandise entry." Among others, this restriction generally prevents CBP from supporting requests from foreign governments for export information to be used to assist the foreign government with determining the duties or taxes owed by an entity importing goods into the foreign country.

7.2.4 CBP will facilitate disclosures of information generated by third agencies (which for purposes of this directive, include information generated by DHS or its other components) to appropriate representatives of Foreign Authorities only after informing and obtaining the consent of the third agency, as appropriate. In the event that a request pertains solely to information owned by a third agency, it may be appropriate to refer the request to such third agency for handling.

7.2.4.1 Care should be given before referring a Foreign Authority to the agency that owns the data in cases where such a referral might on its own reveal information (e.g., do not direct a requester to the Terrorist

---

[16] CBP Directive No. 1450-023, Maintenance, Use, Sharing, and Protection of Section 1367 "Protected Class" Information (December 17, 2019).

[17] CBP Directive No. 3340-049A, Border Searches of Electronic Devices (January 4, 2018).

[18] Information regarding, contained in or pertaining to an application for asylum, a credible fear determination or a reasonable fear determination under the immigration laws of the United States ordinarily may not be disclosed in response to a request for information from a Foreign Authority. Any questions regarding this restriction and whether an exception may apply in a particular case may be directed to the Associate Chief Counsel (Enforcement and Operations) or local Associate or Assistant Chief Counsel.

Screening Center for information if doing so may reveal the person is watchlisted; do not direct an agency to a third agency if doing so could reveal or compromise an ongoing investigation).

7.3 Sharing must occur in accordance with the processes outlined in Section 8 of this Directive and pursuant to the following:

7.3.1 Sharing must comply with 19 U.S.C. § 1628 (Exchange of Information),[19] 19 CFR § 103.33 (Release of information to foreign agencies),[20] and DHS Delegation Number 7010.3,[21] pursuant to which authority to disclose information to foreign customs and law enforcement agencies has been delegated to the Commissioner of CBP:

7.3.1.1 The Commissioner of CBP has further delegated that authority to: Deputy Commissioner, Chief of the United States Border Patrol, Executive Assistant Commissioner for the Office of Field Operations, Executive Assistant Commissioner for Air and Marine Operations, Executive Assistant Commissioner for the Office of Trade, Executive Assistant Commissioner for Enterprise Services, Executive Assistant Commissioner for Operations Support, Assistant Commissioner for the Office of International Affairs, Assistant Commissioner for the Office of Intelligence, Assistant Commissioner for the Office of Professional Responsibility; and Assistant Commissioner for Laboratories and Scientific Services;[22] and

7.3.1.2 Pursuant to 19 U.S.C. § 1628 and 19 CFR 103.33, information must not be provided to a Foreign Authority that has violated the assurances outlined in Section 10.1 of this Directive.

---

[19] In accordance with the 19 U.S.C. § 1628, the Secretary of DHS may authorize customs officers to exchange information or documents with foreign customs and law enforcement agencies if the Secretary reasonably believes the exchange is necessary to: (1) insure compliance with any law or regulation enforced or administered by the Customs Service; (2) administer or enforce multilateral or bilateral agreements to which the United States is a party; (3) assist in investigative, judicial and quasi-judicial proceedings in the United States; and (4) support a comparable action undertaken by a foreign customs or law enforcement agency, or in relation to a proceeding in a foreign country.

[20] The Commissioner of CBP may authorize Customs officers to exchange information or documents with foreign customs and law enforcement agencies if the Commissioner or their designee believes the exchange of information is necessary to: (1) Ensure compliance with any law or regulation enforced or administered by Customs; (2) Administer or enforce multilateral or bilateral agreements to which the U.S. is a party; (3) Assist in investigative, judicial and quasi-judicial proceedings in the U.S.; and (4) support a comparable action undertaken by a foreign customs or law enforcement agency, or in relation to a proceeding in a foreign country.

[21] DHS Delegation Number 7010.3: Delegation of Authority to the Commissioner of U.S. Customs and Border Protection (May 11, 2006).

[22] CBP Commissioner Delegation Order (DO-18-210): "Delegation of Authority to Disclose Information to Foreign Governments", March 7, 2019. This authority may be further delegated to each office's Principal Field Officials and other appropriate CBP personnel within their respective offices, but not below the supervisory GS-13 level.

7.3.2 Existing agency, department, or intergovernmental agreements, such as a Customs Mutual Assistance Agreement (CMAA) or Mutual Legal Assistance Treaty (MLAT);

7.3.2.1 Requests under such agreements and arrangements shall be directed to the Office of International Affairs, or such other point of contact as may be set forth in the relevant agreement or arrangement (e.g., Mutual Legal Assistance Treaty requests must be directed by Foreign Authorities to the Department of Justice, which then coordinates the requests with CBP and other relevant agencies).

7.3.2.2 Information may be exchanged with agencies of the governments of Mexico and Canada pursuant to the United States-Mexico-Canada Agreement (USMCA) if CBP reasonably believes the request is necessary to implement Chapters 2, 4, and 5 of the USMCA, CBP obtains assurances of confidentiality from the country received such information consistent with Section 10.1 of this Directive and 19 CFR 182.2(b), and such sharing is otherwise consistent with applicable law and policy:

7.3.2.2.1 The CBP Attaché-Ottawa should be notified of any Canadian USMCA-related requests for the disclosure of information to the Government of Canada.

7.3.2.2.2 The CBP Attaché-Mexico City should be notified of any Mexican USMCA-related requests for the disclosure of information to the Government of Mexico.

7.3.2.3 All agreements or arrangements (e.g., Memoranda of Understanding, Letters of Intent, etc.) providing for the sharing of information with a Foreign Authority shall be coordinated with the Office of International Affairs, Privacy and Diversity Office,[23] and the Office of Chief Counsel.

7.3.3 Authorized CBP personnel may proactively initiate the disclosure of information (in the absence of a request) to Foreign Authorities when the CBP employee believes the Foreign Authority has a need-to-know and the disclosure complies with all other aspects of this Directive and the reason for disclosing the information is appropriately documented as outlined in Section 8 below.

7.4 Any questions regarding requirements for sharing or restrictions associated with specific types of data, and whether an exception may apply in a particular case may be directed to the Privacy and Diversity Office (Privacy Division), the Associate Chief Counsel (Enforcement and Operations), or local Associate or Assistant Chief Counsel, as applicable.

---

[23] CBP Directive 2120-010A "Privacy Policy, Compliance, and Implementation" (June 29, 2022).

8. INFORMATION SHARING PROCEDURES

8.1 For any sharing of CBP data in response to requests from Foreign Authorities, all CBP Personnel must:

8.1.1 Ensure that requests are submitted in writing,[24] and maintain those requests in a manner that will facilitate review and auditing as necessary to ensure compliance with established policy and legal requirements;[25]

8.1.1.1 Requests must provide sufficient detail to identify the agency or entity requesting the information; the specific type of information requested; the reason the information is being requested, including how the information supports the receiving authority's official duties (e.g., an investigation); any applicable laws indicating the recipient's authority to obtain and/or use the data; whether onward disclosures of the requested information are expected and, if so, the details of such onward disclosure; where the requested information should be sent; whether the requested records need to be certified or any other applicable requirements to be met by CBP for the Foreign Authority to be able to use the CBP information provided; and the date by which the information is needed, as applicable.

8.1.1.2 In exigent circumstances where a written request cannot be submitted before disclosure, the CBP official responding to the request shall ensure that the request is promptly reduced to writing by the Foreign Authority.

8.1.2 Ensure that any disclosure of CBP data to a Foreign Authority supports:

8.1.2.1 Compliance with any law or regulation enforced or administered by CBP;

8.1.2.2 The administration or enforcement of a multilateral or bilateral agreement to which the United States is a party;

8.1.2.3 An investigation, judicial, or quasi-judicial proceeding in the United States; or

8.1.2.4 An action comparable to the above undertaken by a foreign customs or law enforcement agency, or in relation to a proceeding in a foreign county.

8.1.3 Ensure that any disclosure of information is from a CBP source system;[26]

---

[24] 5 U.S.C. § 552a(b) and CBP Directive 2120-010A: Privacy Policy, Compliance and Implementation.

[25] Written requests include a signed memorandum on official agency letterhead, or the submission of an email from an official agency address.

[26] For data accuracy purposes, data must be retrieved from agency source systems, rather than data aggregators or collaboration tools.

8.1.4 Ensure that appropriate redactions and/or markings as outlined in Section 9 of this Directive are applied to records being disclosed;

8.1.5 Ensure that information provided by CBP to a Foreign Authority will not be released to other parties without obtaining the prior express written permission of CBP;

8.1.6 Ensure that, in the event of any unauthorized release, their government will intercede on behalf of CBP as necessary and assume responsibility for any and all expenses, costs, or liabilities arising therefrom, as well as immediately notify CBP of the unauthorized release so that appropriate action can be taken as outlined in Section 11 of this Directive; and

8.1.7 Apply appropriate protections to information prior to disclosure, including the use of password protections, encryption, or coversheets as applicable depending on the method of disclosure.[27]

9. REDACTIONS AND MARKINGS

9.1 Records to be disclosed to a representative of a Foreign Authority should be properly redacted prior to disclosure to ensure that only the information which is responsive to a request or relevant to the subject for which the information is being provided, is disclosed. The Privacy and Diversity Office (Privacy Division), the Office of Associate Chief Counsel (Enforcement and Operations) or local Associate or Assistant Chief Counsel, as appropriate, may be contacted in the event an authorized official has questions regarding whether information should be redacted prior to disclosure. Information which should be redacted includes:

9.1.1 Any identifiable names, Social Security numbers and other personally identifiable information of DHS personnel, except when providing the names of relevant CBP personnel is a necessary and appropriate part of CBP's response (e.g., where the names of CBP personnel authorized to testify in a foreign judicial proceeding must be provided unredacted in an underlying record to be used in that case);

9.1.2 Any identifiable information of individuals that are not identified in the request, except when providing the names are a necessary and appropriate part of CBP's response (e.g., where the purpose of the disclosure is to provide information to a requestor regarding individuals unknown to the requestor, such as information regarding a traveler's associates or co-travelers needed for purposes of an investigation);

---

[27] Pursuant to DHS Sensitive Systems Policy Directive 4300A, Version 13.2, September 20, 2022, DHS personnel must protect sensitive information, particularly sensitive PII, when transmitting it outside the dhs.gov domain. Additionally, the DHS Privacy Policy Directive 047-01-007, Handbook for Safeguarding Sensitive PII, further requires that such information be encrypted.

9.1.3 Any computer screen codes, internal file codes, or system codes;

9.1.4 Any Law Enforcement Sensitive (LES) information, whether it is explicitly marked as such, or if the release of unmarked information could compromise an open case or investigation, except when providing LES information is the purpose of the disclosure;

9.1.5 Sensitive Security Information (SSI) (e.g., terrorist watchlist status);

9.1.6 Information owned by another agency or a foreign entity that has not been approved for disclosure; and

9.1.7 Any other information that is not appropriate for disclosure that may be present (e.g., information included in a document otherwise appropriate for disclosure that the Foreign Authority does not have a need to know).

9.2 Law Enforcement Sensitive (LES) and intelligence information released to the representative of a Foreign Authority shall be marked as "For Official Use Only - Law Enforcement Sensitive" consistent with DHS Management Directive 11042.1 and any other applicable guidance or regulation. This marking shall clearly indicate that the information is being exchanged solely for the law enforcement purpose supporting the request. Additionally, such information should clearly state that it was provided by CBP, referencing the agreement or arrangement under which the information was provided, if applicable. Sample markings are attached to this Directive as Appendix B.[28]

9.2.1 Before sharing LES information, the authorized disclosing official, in consultation with the Office of International Affairs, as appropriate, shall take appropriate deconfliction efforts to ascertain whether the disclosure could interfere with the enforcement interests of CBP, DHS or its components, or another agency of the U.S. government.

9.2.2 The Office of Intelligence, specifically the Foreign Disclosure Office (cbpfdo@cbp.dhs.gov), must be consulted prior to the release of intelligence products, including raw informational products and finished intelligence products, to determine if the Department (in particular, the DHS Foreign Disclosure Office) has identified any sensitivity concerns which may impact CBP's decision to disclose the information to a Foreign Authority,[29] and so that appropriate markings associated with the release of information to a particular country may be added.

---

[28] When LES information is to be used by the recipient as a lead in an investigation, markings must include clear restrictions on the use of the information and a requirement to obtain further authorization from CBP prior to any onward sharing or use of the information in a judicial proceeding.

[29] While offices conducting a particular sharing are responsible for assessing the records, including determining whether specific elements should be shared, they must also consider any other factors associated with a request in determining whether the disclosure should occur. Coordination with INA and OI should focus on assessing these factors and considerations.

9.3 In the event particular markings are required by policy governing certain data (e.g., intelligence products, PNR data, T/U/VAWA, etc. (see section 3.7 of this Directive)), those other markings shall apply in lieu of or in addition to, as appropriate, these more general marking requirements.

10. DOCUMENTATION OF DISCLOSURES

10.1 Any disclosure of CBP data to a Foreign Authority must be accompanied by text (e.g., a cover letter, email, or other document) outlining that the provided information will:[30]

> **10.1.1** Be held in confidence and not be further disclosed to another entity within the Foreign Authority, or other Foreign Authority, without the express prior written permission of CBP;
>
> **10.1.2** Be safeguarded to prevent unauthorized access or use; and
>
> **10.1.3** Only be used for the purpose for which CBP provided the information.

10.2 Any disclosures of CBP records containing PII to a Foreign Authority must be properly accounted for through either a system generated or electronically filed (e.g., scanned hard copy) DHS-191 Form, other Privacy Act Disclosure Record, or other form or process specifically authorized by the Chief Privacy Officer;[31] and

> **10.2.1** The record of disclosure (DHS -191 Form or other approved mechanism) must be retained by the CBP office providing the information for a period of five years. A copy must also be submitted to the CBP Privacy and Diversity Office, Privacy Division, at privacy.cbp@cbp.dhs.gov.[32]
>
> **10.2.2** The office that shared information with a Foreign Authority must maintain a copy of the request, a copy of the information provided, information related to the recipient, the reason for the disclosure, and, if the disclosure contained PII, a copy of the DHS-191 (or other CBP Privacy Officer-approved mechanism to account for disclosures) for a period of 5 years.

10.3 Any additional record keeping requirements necessary for specific data types (such as PNR data) must also be completed.

11. PRIVACY INCIDENT HANDLING

11.1 In the event CBP personnel become aware of or suspect unauthorized access to, or disclosure of, CBP records to or by a Foreign Authority has occurred, they must report it to:

---

[30] Sample cover letters reflecting these requirements are attached hereto in Appendix A.
[31] 5 U.S.C. § 552a(c).
[32] See Retention Authority: NARA General Records schedule 4.2, item 50, available at, https://www.archives.gov/files/records-mgmt/grs/grs04-2.pdf.

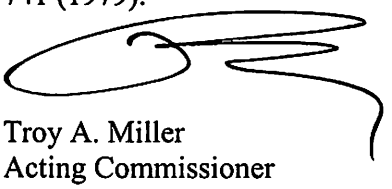
11.1.1 The CBP Privacy Office (PRIVACYINCIDENTS@CBP.DHS.GOV);

11.1.2 The Assistant Commissioner for the Office of International Affairs, who is responsible for providing guidance regarding Foreign Authorities which have violated assurances associated with the exchange of data; and

11.1.3 The relevant CBP Attaché or agency representative as identified in the information sharing agreement under which the records were disclosed.

12. NO PRIVATE RIGHTS CREATED

This Directive is an internal policy statement of CBP and does not create or confer any rights, privileges, or benefits for any person or entity. United States v. Caceres, 440 U.S. 741 (1979).



Troy A. Miller
Acting Commissioner
U.S. Customs and Border Protection

Appendix A

Sample Cover Letter - *For sharing under 19 U.S.C. Section 1628*

[DATE]

[ADDRESSEE]

Subject: [FOREIGN DISCLOSURE REQUEST]

Enclosed please find information/records provided by U.S. Customs and Border Protection (CBP) in response to the above-referenced request, dated [DATE]. This information is provided to [NAME OF FOREIGN LAW ENFORCEMENT AUTHORITY] in support of [DESCRIPTION OF OPERATION OR INVESTIGATION SUPPORTING THE REQUEST]. This data is being provided pursuant to 19 U.S.C. Section 1628 to support the law enforcement activities of your agency.

The enclosed materials consist of [NUMBER OF PAGES AND DESCRIPTION OF RECORDS; REFERENCE BATES STAMP NUMBERING, IF APPLICABLE].

[FOLLOWING TO BE USED AS APPLICABLE: Information was redacted from the printouts provided to protect the identities of law enforcement officers and the integrity of CBP computer systems. Certain law enforcement sensitive information which is used for internal CBP purposes has also been redacted from the records, as the release of such information would impede the effectiveness of law enforcement activities or disclose techniques and procedures for law enforcement investigation or prosecutions and could reasonably be expected to risk circumvention of the law.]

These documents are being provided subject to the restrictions, mandated by 19 U.S.C. Section 1628. Accordingly, the enclosed information is provided to achieve one or more of the objectives set forth in subsection 1628(a) and applicable to your request. The enclosed information is provided subject to your assurance that this information will be held in confidence and used only for the law enforcement purposes identified above.

Any other use of the information is not authorized. This information cannot be released to any other third parties without CBP's express written permission. In the event of any unauthorized release of the provided information, [NAME OF FOREIGN LAW ENFORCEMENT AUTHORITY] or the Government of [RECEIVING COUNTRY] must intercede on CBP's behalf and assume responsibility for any and all expenses, costs, or liabilities arising therefrom.

Should you have any questions regarding this matter, please contact [POINT OF CONTACT responsible for this release]

Sincerely,

[INSERT NAME OF AUTHORIZED OFFICIAL]

cc: Office of Assistant Commissioner (International Affairs)
[INSERT ASSISTANT COMMISSIONER FOR BUSINESS OWNER(S) OF THE REQUESTED INFORMATION] [Business owner(s) of the requested information]

Sample Cover Letter - *For sharing under USMCA*

[DATE]

[ADDRESSEE]

Subject: [FOREIGN DISCLOSURE REQUEST]

Enclosed please find information/records provided by U.S. Customs and Border Protection (CBP) in response to the above-referenced request, dated [DATE]. This information is provided to [NAME OF FOREIGN LAW ENFORCEMENT AUTHORITY] in support of [DESCRIPTION OF OPERATION OR INVESTIGATION SUPPORTING THE REQUEST]. This data is being provided pursuant to [INSERT TITLE OF AGREEMENT THIS SHARING IS OCCURING UNDER]

The enclosed materials consist of [NUMBER OF PAGES AND DESCRIPTION OF RECORDS; REFERENCE BATES STAMP NUMBERING, IF APPLICABLE].

[FOLLOWING TO BE USED AS APPLICABLE: Information was redacted from the printouts provided to protect the identities of law enforcement officers and the integrity of CBP computer systems. Certain law enforcement sensitive information which is used for internal CBP purposes has also been redacted from the records, as the release of such information would impede the effectiveness of law enforcement activities or disclose techniques and procedures for law enforcement investigation or prosecutions, and could reasonably be expected to risk circumvention of the law.]

[IN THE CASE OF INFORMATION PROVIDED TO A GOVERNMENT AGENCY OF A USMCA COUNTRY TO IMPLEMENT USMCA CHS. 2, 4 OR 5: This information is provided subject to your assurance that the information will be held in confidence and used only for governmental purposes.]

[IN ALL OTHER CASES: Accordingly, the enclosed information is provided to achieve one or more of the objectives set forth in subsection 1628(a) and applicable to your request. The enclosed information is provided subject to your assurance that this information will be held in confidence and used only for the law enforcement purposes identified above.]

Any other use of the information is not authorized. This information cannot be released to any other third parties without CBP's express written permission. In the event of any unauthorized release of the provided information, [NAME OF FOREIGN LAW ENFORCEMENT AUTHORITY] or the Government of [RECEIVING COUNTRY] must intercede on CBP's behalf and assume responsibility for any and all expenses, costs, or liabilities arising therefrom.

Should you have any questions regarding this matter, please contact [POINT OF CONTACT]

Sincerely,

[INSERT NAME OF AUTHORIZED OFFICIAL]

cc: Office of Assistant Commissioner (International Affairs)
[INSERT ASSISTANT COMMISSIONER FOR BUSINESS OWNER(S) OF THE REQUESTED INFORMATION] [Business owner(s) of the requested information]

Sample Cover Letter - *For sharing under MLAT*

[DATE]

[ADDRESSEE—DEPARTMENT OF JUSTICE POINT OF CONTACT]

Re: [MLAT FOREIGN DISCLOSURE REQUEST]

Enclosed please find information provided by U.S. Customs and Border Protection (CBP) in response to the above-referenced request, dated [DATE]. This information is provided to the U.S. Department of Justice, Office of International Affairs (OIA) to support the law enforcement activities of [SPECIFIC FOREIGN GOVERNMENT AGENCY OR COMPONENT SUBMITTING THE REQUEST], specifically [DESCRIPTION OF SUBJECT OF INVESTIGATION].

OIA, as the Central Authority pursuant to the Mutual Legal Assistance Treaty between the United States and XXXX is authorized to release this information to the appropriate XXXX authorities pursuant to the agreement.

The enclosed materials consist of [NUMBER OF PAGES, DESCRIPTION OF RECORDS, REFERENCING BATES STAMP NUMBERS, IF APPLICABLE].

[FOLLOWING TO BE USED AS APPLICABLE: Information was redacted from the printouts provided to protect the identities of law enforcement officers and the integrity of CBP computer systems. Certain law enforcement sensitive information which is used for internal CBP purposes has also been redacted from the records, as the release of such information would impede the effectiveness of law enforcement activities or disclose techniques and procedures for law enforcement investigation or prosecutions and could reasonably be expected to risk circumvention of the law.]

These materials are provided for purposes of facilitating the law enforcement investigation or operation referenced above. These materials are provided on the condition that this information may only be used in conformity with the provisions of the [INSERT RELEVANT MUTUAL LEGAL ASSISTANCE AGREEMENT].

Should you have any questions regarding this matter, please contact [COUNSEL POINT OF CONTACT].

Sincerely,

[INSERT NAME OF RESPONDING OFFICE OF CHIEF COUNSEL PERSONNEL]

cc: Office of International Affairs
[Business owner(s) of the requested information]

Sample Cover Letter - *For sharing under CMAA*

[DATE]

[ADDRESSEE]

Re: [CMAA FOREIGN DISCLOSURE REQUEST]

Enclosed please find information provided by U.S. Customs and Border Protection (CBP) in response to the above-referenced request, dated [DATE]. This information is provided to [NAME OF FOREIGN CUSTOMS ADMINISTRATION] in order to support the customs and law enforcement activities of your agency, specifically [DESCRIPTION OF COVERED OPERATION OR INVESTIGATION].

The enclosed materials consist of [NUMBER OF PAGES, INCLUDING BATES STAMP NUMBERS, IF APPLICABLE, AND DESCRIPTION OF RECORDS].

[FOLLOWING TO BE USED AS APPLICABLE: Information was redacted from the printouts provided to protect the identities of law enforcement officers and the integrity of CBP computer systems. Certain law enforcement sensitive information which is used for internal CBP purposes has also been redacted from the records, as the release of such information would impede the effectiveness of law enforcement activities or disclose techniques and procedures for law enforcement investigation or prosecutions and could reasonably be expected to risk circumvention of the law.]

These documents are being provided pursuant to the authority, and subject to the restrictions created by, [INSERT NAME OF THE AGREEMENT BETWEEN THE GOVERNMENT OF THE UNITED STATES AND THE FOREIGN GOVERNMENT] (the "CMAA"). Accordingly, the enclosed information is provided to support the operation or investigation referenced above and may be used for additional purposes only after obtaining the consent of CBP. This restriction shall not, however, preclude the use or disclosure of information to the extent that there is an obligation to do so under the laws of [INSERT NAME OF REQUESTING COUNTRY] in connection with a criminal prosecution. CBP hereby requests advance notice be provided of any such disclosure.

[INSERT NAME OF FOREIGN CUSTOMS ADMINISTRATION] is authorized to use the enclosed materials subject to the conditions set forth in this letter and the terms of the CMAA. Any other use of the information is not authorized.

Should you have any questions regarding this matter, please contact [POINT OF CONTACT]

Sincerely,

[INSERT NAME OF AUTHORIZED OFFICIAL]

[Business owner(s) of the requested information]

Appendix B - *Sample Markings*

Sample 1 (No agreement in place):

This information is For Official Use Only/Law Enforcement Sensitive and has been provided by U.S. Customs and Border Protection (CBP) strictly for use in connection with [describe request]. This information may not be used for any other purpose and may not be distributed outside of [INSERT AGENCY(S) OR OFFICIALS] without the express written prior authorization from CBP. Failure to abide by these terms will make the recipient of this information ineligible to receive further information from CBP.

Sample 2 (Agreement in place):

This information is For Official Use Only/Law Enforcement Sensitive and has been provided by U.S. Customs and Border Protection (CBP) under the terms of [INSERT NAME OF AGREEMENT/ARRANGEMENT]. This information may not be used for any other purpose and may not be distributed outside of [INSERT AGENCY(S) OR OFFICIALS] without express written prior authorization from CBP. Failure to abide by these terms will make the recipient of this information ineligible to receive further information from CBP.

Appendix C – *Disclosure Process Flow*

U.S. Customs and Border Protection

Step 1

The Directive on the "Disclosure of CBP Information to Foreign Authorities" applies if the request for information is received from representative of Foreign Authority or CBP-initiated disclosure

Step 2

CBP Evaluation to Ensure (1) sufficiency of the request for information, (2) the foreign authority has articulated their need to know the information, and how CBP information supports their investigation, and (3) the authority of CBP to release the information.

Step 3

CBP Coordination with business/record owner with the authority to release information to a foreign authority, and review of information to (1) redact non-responsive and sensitive information, (2) designate law enforcement sensitive information, coordinate and deconflict, and (3) ensure personally identifiable information is marked and safeguarded appropriately.

Step 4

Redacted and marked information may be disclosed to the requesting Foreign Authority accompanied by appropriate admonishments and conditions regarding safeguarding and subsequent disclosure.

Step 5

Appropriate record keeping much be completed

U.S. Customs and Border Protection

Step 1:

Does the Directive “Disclosure of CBP Information to Foreign Authorities” apply to this request?

- Has CBP received a request for information or records from an official, with the authority to make such a request, representing a Foreign Authority?
- Is CBP seeking to proactively disclose records to a Foreign Authority?

This Directive applies to all personnel as defined in Section 5.12, particularly those individuals involved in the sharing of CBP collected and maintained information with foreign authorities. This Directive applies to all information sharing pursuant to 19 U.S.C. § 1628; mutual assistance agreements and arrangements in place between the United States, the U.S. Department of Homeland Security (DHS), or CBP and the requesting foreign governments or multilateral governmental organizations; and any disclosures of information by CBP to foreign authorities consistent with the authorities and functions of CBP to enforce the customs, immigration, and other laws of the United States. This Directive does not apply to, nor permit, the sharing of classified national security information with foreign authorities. This Directive does not supersede or otherwise affect existing and future agency policies regarding a demand, such as a subpoena, for official information in the possession of CBP for use in a foreign proceeding where the United States is not a party. Such demands shall continue to be processed pursuant to 19 C.F.R. § 103.27.

U.S. Customs and Border Protection

Step 2:

CBP Evaluation to Ensure (1) sufficiency of the request for information, (2) the foreign authority has articulated their need to know the information, and how CBP information supports their investigation, and (3) the authority of CBP to release the information.

Request Details

Was the request submitted in writing and does it provide sufficient detail to identify the agency or entity requesting the information; the specific type of information requested; the reason the information is being requested, including how the information supports the receiving authority's official duties (e.g., an investigation); what potential onward disclosure may occur; and where the information should be sent?

Their Authority

Does the requester have authority to obtain and/or use the data, and what applicable laws is that authority rooted in?

Our Authority

Does the CBP official responding to the request have the authority to disclose agency information to a Foreign Authority?

Review Assistance:

- OCC can assist with legal guidance regarding matters related to the disclosure of information, especaily for requests involving the use of CBP records in foreign judicial proceedings
- The Privacy Office can assist with guidance regarding matters related to the disclosure of information, specifically for requests involving CBP records containing PII in support of investigations
- The Office of International Affairs can assist with deconfliction efforts and determining whether a disclosure could interfere with the enforcement interests the U.S. government

U.S. Customs and Border Protection

Step 2: Our Authority

Authority for CBP personnel to share information/records with a Foreign Authority must be derived from one of the following:

For ad hoc requests, not pursuant to an existing agreement or arrangement, authority provided under the **CBP Commissioner Delegation Order (DO-18-210):** "Delegation of Authority to Disclose Information to Foreign Governments", March 7, 2019.

- Delegates authority under 19 U.S.C. § 1628 (Exchange of Information), 19 CFR § 103.33 (Release of information to foreign agencies), and DHS Delegation Number 7010.3, for the authority to disclose information to foreign customs and law enforcement agencies
- Authority has been delegated to: Deputy Commissioner, Chief of the United States Border Patrol, Executive Assistant Commissioner for the Office of Field Operations, Executive Assistant Commissioner for Air and Marine Operations, Executive Assistant Commissioner for the Office of Trade, Executive Assistant Commissioner for Enterprise Services, Executive Assistant Commissioner for Operations Support, Assistant Commissioner for the Office of International Affairs, Assistant Commissioner for the Office of Intelligence, Assistant Commissioner for the Office of Professional Responsibility, and Assistant Commissioner for Laboratories and Scientific Services.
- This authority may be further delegated to each office's Principal Field Officials and other appropriate CBP personnel within their respective offices no lower than the supervisory GS-13 level .

International Agreement or Arrangement: Existing agency, department, or intergovernmental agreements, such as a Customs Mutual Assistance Agreement (CMAA) or Mutual Legal Assistance Treaty (MLAT) and non-binding international agreements;

- Information may be exchanged with agencies of the governments of Mexico and Canada pursuant to the United States-Mexico-Canada Agreement (USMCA)

Step 3:

U.S. Customs and Border Protection

CBP Coordination and review of information to (1) redact non responsive and sensitive information, (2) designate law enforcement sensitive information, coordinate and deconflict, and (3) ensure personally identifiable information is marked and safeguarded appropriately.

Privacy Office	Provides guidance to operational offices, officers, agents, and analysts regarding matters related to the disclosure of information, ***specifically for requests involving the use of CBP records containing PII in support of investigations.***
Office of Chief Counsel	Provides CBP personnel with legal guidance regarding matters related to the disclosure of information, ***especially for requests involving the use of CBP records in foreign judicial proceedings.***
Business/Record Owner	Identifies information or specific data elements within the records that should be redacted or withheld prior to the disclosure of a record to a Foreign Authority.
Office of International Affairs	Supports deconfliction efforts before sharing law enforcement sensitive (LES) information to ascertain whether the disclosure could interfere with the enforcement interests of CBP, DHS or its components, or another agency of the U.S. government.
Office of Intelligence	Supports the identification of (in particular, the DHS Foreign Disclosure Office) specific concerns related to the type of information being shared or the suitability of the Foreign Authority records are being shared with, which may impact CBP's decision to disclose the information.

U.S. Customs and Border Protection

Step 3: Non-Disclosure

Some types of data are generally protected from disclosure, including information associated with Asylum and Credible Fear Applications, Protected Class Data, Advance Cargo Information.

Protected Class

Information relating to individuals who are seeking or have been approved for immigrant status as battered spouses, children and parents under provisions of the Violence Against Women Act (VAWA), as victims of a severe form of human trafficking or as aliens who have suffered substantial physical or mental abuse and are cooperating with law enforcement authorities, including applicants or beneficiaries of the T Visa, U Visa, or VAWA protections, may not be shared with a Foreign Authority unless authorized by DHS Instruction Number 002-02-001 or DHS Instruction Number 215-01-001, and pursuant to CBP Directive 1450-023 implementing such directive and instructions

Advance Cargo Data

Advance cargo information collected by CBP may only be used for ensuring cargo safety and security, preventing smuggling, and commercial risk assessment targeting, and shall not be used for any commercial enforcement purposes, including for determining merchandise entry. Among others, this restriction generally prevents CBP from supporting requests from foreign governments for export information to be used to assist the foreign government with determining the duties or taxes owed by an entity importing goods into the foreign country.

Third Agency

It is the policy of CBP to either coordinate with, or refer to, any request for information owned or generated by third agencies (which would, strictly for purposes of this directive, include information generated by DHS or its other components). CBP personnel will obtain consent of the third agency prior to disclosing any information to a Foreign Authority. In the event that a request pertains solely to information owned by a third agency, it may be appropriate to refer the request to that agency for handling

U.S. Customs and Border Protection

Step 3: Redactions & Markings

(1) redact non responsive and sensitive information, (2) designate law enforcement sensitive information, coordinate and deconflict, and (3) ensure personally identifiable information is marked and safeguarded appropriately.

Redactions

Information which should be redacted includes:

- Any identifiable names, Social Security numbers and other personally identifiable information of DHS personnel
- Any identifiable information of individuals that are not the subject of, or relevant to, the request
- Any computer screen codes, internal file codes, or system codes
- Sensitive Security Information (SSI) (e.g., terrorist watchlist status)
- Information owned by another agency or a foreign entity that has not been approved for disclosure; and
- Any other information that is not appropriate for disclosure that may be present

Certain identifying information may be exempt from redaction when providing that information is a necessary and appropriate part of CBP's response (e.g., where the names of CBP personnel authorized to testify in a foreign judicial proceeding must be provided unredacted in an underlying record to be used in that case or where the purpose of the disclosure is to identify associates or co travelers unknown to the requester);

LES Markings

Law Enforcement Sensitive (LES) information released to the representative of a Foreign Authority shall be marked "For Official Use Only - Law Enforcement Sensitive" consistent with DHS Management Directive 11042.1 and any other applicable guidance or regulation. This marking shall clearly indicate that the information is being exchanged solely for the law enforcement purpose supporting the request. Additionally, such information should clearly state that it was provided by CBP, referencing the agreement or arrangement under which the information was provided, if applicable.

Protected Class Data

Policy governing certain data sets (e.g., PNR data, T/U/VAWA, etc.), may require supplemental markings. The relevant policies for specific data sets should be consulted before sharing is conducted.

U.S. Customs and Border Protection

Step 4:

Every disclosure of information/records to a Foreign Authority must be accompanied by text outlining the required protections and data use limitation associated with the sharing. Template cover letters are included in Appendix A of the Directive.

Safeguarding

Information/records provided by CBP to a Foreign Authority must be safeguarded to prevent unauthorized access or use.

Use Limitation

Information/records provided by CBP to a Foreign Authority must only be used for the purpose for which CBP provided the information.

Onward Disclosure

Information/records provided by CBP must be held in confidence and not be further disclosed to another entity within the Foreign Authority, or other Foreign Authority, without the express prior written permission of CBP.

U.S. Customs and Border Protection

Step 5:

Any disclosures of CBP records to a Foreign Authority must be properly accounted for through the retention of information related to the request/sharing

The Request

The office that shared information with a Foreign Authority must maintain a copy of the request, any information related to the recipient, and documentation of the reason for the disclosure.

The Disclosure

The office that shared information with a Foreign Authority must maintain a copy of information/record provided.

DHS 191

Any disclosures of CBP records containing PII to a Foreign Authority must be properly accounted for through either a system generated or electronically filed (scanned hard copy) DHS-191 Form, other Privacy Act Disclosure Record, or other form or process specifically authorized by the Chief Privacy Officer. The DHS-191 must be retained by the disclosing office for a period of 5 years.