U.S. CUSTOMS AND BORDER PROTECTION

DIRECTIVE NUMBER:
51250-025

DIRECTIVE TITLE:
Public Disclosure of Employee Information

EFFECTIVE DATE:
February 10, 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

U.S. CUSTOMS AND BORDER PROTECTION DIRECTIVE

CBP DIRECTIVE NO. 51250-025 **DATE: February 10, 2023**

ORIGINATING OFFICE: OC-PDO

REVIEW DATE: February 10, 2026

SUBJECT: PUBLIC DISCLOSURE OF EMPLOYEE INFORMATION

1. PURPOSE

This Directive is designed to provide U.S. Customs and Border Protection (CBP) personnel with guidance and procedures related to the disclosure of employee data, specifically personally identifiable information (PII), in response to third-party requests (e.g., media inquiries).

2. SCOPE

This Directive applies to all personnel as defined in Section 5, including records maintained on individuals that are no longer employed by, or assigned to, CBP. In accordance with the Office of Personnel Management's (OPM) Data Release Policy,[1] and its designation of CBP as a Security Agency,[2] CBP will treat all records associated with employees as non-releasable in response to third-party requests, except as outlined in this Directive.

This Directive is not intended to limit disclosure of information pursuant to an Official Sharing request[3] or covered by an established Information Sharing and Access Agreement (ISAA), including Memoranda of Agreement (MOAs) and Memoranda of Understanding (MOUs); requests for information from domestic law enforcement agencies[4]; the sharing of information

---

[1] See: The U.S. Office of Personnel Management (OPM) Data Release Policy, (August 2020), available at https://www.opm.gov/policy-data-oversight/data-analysis-documentation/data-policy-guidance/data-standards/data-release-policy-august-2020.pdf.

[2] On January 16, 2020, the Director of OPM issued a letter in response to a request by CBP seeking designation as a Security Agency under OPM's official Data Release Policy. Following its review of CBP's request, OPM determined that all CBP employees are subject to a heightened risk of harassment or attack by virtue of their employment at CBP, and the designation of CBP as a Security Agency with regard to its official Data Release Policy was appropriate.

[3] Disclosures in response to requests from Congressional Committee Chairpersons acting on behalf of their committees, federal courts, federal, state, local, tribal, and foreign law enforcement and other administrative agencies having a need for information in the performance of their official duties. These disclosures are generally made pursuant to routine uses that are listed in system of records notices (SORN) or pursuant to another authorized disclosure stated in the Privacy Act. All official sharing requests must be analyzed to determine whether a Routine Use or other Privacy Act conditions of disclosure applies.

[4] See: CBP Directive No. 4320-033, Domestic Sharing of CBP Information for Law Enforcement and Security Purposes, (May 24, 2021)

with foreign governments or nongovernment entities[5]; the provision of information when CBP is legally required to provide the information, such as in response to a court order; disclosures pursuant to a Privacy Act Waiver signed by the subject[6]; nor does it apply to the disclosure of information in response to Freedom of Information Act (FOIA) requests, or any routine uses that are listed in system of records notices (SORNs) or pursuant to another condition of disclosure stated in the Privacy Act.

3. POLICY

3.1 This Directive applies to all CBP personnel.

3.2 This Directive applies to the public release of information about CBP personnel in response to media, Freedom of Information Act (FOIA), or other inquiries where CBP personnel information may be made public.

3.3 This Directive provides procedures for all CBP personnel to ensure that public disclosure of records related to CBP personnel complies with all applicable laws, regulations, and policies.

3.4 The procedures set forth in this Directive must be followed before information/records maintained by CBP related to CBP personnel may be disseminated to a third party.

3.4.1 Pursuant to the processes outlined in this directive, authorized CBP personnel may release records associated with an employee when[7]:

3.4.1.1 The employee is arrested by another jurisdiction or law enforcement agency;

3.4.1.2 CBP's Office of Professional Responsibility (OPR) takes action against an employee during, or as a result of an investigation; and

3.4.1.3 When an employee is identified by media reporting as related to a specific incident, action, or activity conducted in support of normal agency operations.[8]

3.5 This Directive follows and implements the OPM Data Release Policy, DHS Directive 047-01, DHS Instruction 047-01-001, DHS Instruction 047-01-005, and DHS Privacy Policy Guidance Memorandum 2017-01; any previous conflicting CBP Directives, policy statements, and manual supplements regarding CBP's privacy policy are superseded by this Directive.

4. AUTHORITIES/REFERENCES

---

[5] See: CBP Directive No. 4320-025A, Disclosure of Official Information to Foreign Authorities, (April 14, 2014)

[6] CBP Form 6360: "Privacy Waiver Authorizing Disclosure to a Third Party", or any other official waiver provided by the subject of the request can be used to authorize CBP to disclose information and/or records about an individual to a third party.

[7] The disclosure of information pertaining to CBP personnel is generally limited to those data elements identified in Section 7.2 of this directive.

[8] Information should not be disclosed in response to a request about an individual simply because they are an employee of CBP. Any disclosures pursuant to this section should involve a balancing test of the employees right to privacy against the public's interest in a specific incident and the need of the agency to shed light on its operations.

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

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

4.3 "Privacy Officer" [6 U.S.C § 142]

4.4 5 C.F.R. part 293 "Personnel Records"

4.5 U.S. Office of Personnel Management Data Release Policy (August 2020)

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

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

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

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

4.10 DHS Privacy Policy Guidance Memorandum 2017-01 "DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information" (April 27, 2017)

4.11 CBP Directive 2120-010 "Privacy Policy, Compliance, and Implementation" (January 25, 2015)

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

5. DEFINITIONS

5.1 **CBP Privacy Officer:** The senior 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 **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.

5.3 **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. In accordance with DHS Privacy Policy Guidance Memorandum 2017-01, "DHS

Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information," DHS treats all persons not covered by the Privacy Act, regardless of immigration status, consistent with the Fair Information Practice Principles and applicable law.

5.4 **Official Sharing:** Disclosures in response to requests from Congressional Committee Chairpersons acting on behalf of their committees, federal courts, federal, state, local, tribal, and foreign law enforcement and other administrative agencies having a need for information in the performance of their official duties. These disclosures are generally made pursuant to routine uses that are listed in System of Records Notices (SORN) or pursuant to another authorized disclosure stated in the Privacy Act. All official sharing requests must be analyzed to determine whether a Routine Use or other Privacy Act conditions of disclosure applies.

5.5 **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.[9]

5.6 **Personnel:** All permanent, temporary, and former 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.

5.7 **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 particular assigned to an individual, such as a finger or voice print or a photograph.

5.8 **Routine Use:** The disclosure of a record from a System of Records outside of DHS for a purpose that is compatible with the purpose for which it was collected. Routine Uses are included in an agency's System of Record Notices and are published in the Federal Register.

5.9 **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.

5.10 **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 of a 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

[9] *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).

for individuals to exercise their Privacy Act rights to access and correct the PII that CBP maintains about them.[10] and

5.11 **Third Party:** A party who is not the subject of the record(s), a representative of the subject, or a party who is not covered under Official Sharing, involving the disclosure of PII. All disclosures to a third party must involve an analysis under applicable law that ensures that the information being shared is appropriate for release to the public.

6. RESPONSIBILITIES

6.1 **All CBP personnel with access to records maintained by CBP**, specifically information/records related to CBP personnel, are responsible for:

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

6.1.2 Ensuring that any disclosure of records associated with CBP personnel to third parties are:

6.1.2.1 Made from a CBP System of Records in accordance with a Routine Use that has been established and described in the relevant SORN;[11] and

6.1.2.2 Made based on a Fair Information Practice Principles (FIPPs) analysis, using the Routine Uses from the SORNs associated with related systems as a guide, to ensure that the intended use is consistent with the purpose for the collection;[12] or other Privacy Act condition of disclosure.

6.1.3 Ensuring that any disclosures of PII from a CBP System of Records to a third party are properly accounted for, as detailed in Section 7.7.1;

6.1.4 Protecting PII from unauthorized disclosure, including preventing releases of information for purposes that have not been authorized by the CBP Privacy Office; and

6.1.5 Coordinating with the CBP Privacy Office (privacy.cbp@cbp.dhs.gov) when questions related to the disclosure of information/records related to CBP personnel arise.

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;

6.2.1.1 Coordinating, as necessary, with the DHS Privacy Office on the release of information related to CBP personnel;

---

[10] *See:* 5 U.S.C. § 552a(e)(4).
[11] 5 U.S.C. § 552a(b)(3).
[12] *See*: Privacy Policy Guidance Memorandum 2017-01, DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information, (April 27, 2017)

6.2.1.2 Coordinating, as necessary, with the CBP Office of Chief Counsel and the DHS Office of General Counsel on the release of information related to CBP personnel; and

6.2.1.3 Coordinating with the Office of Congressional Affairs on the release of information related to CBP personnel in support of Official Sharing requests from members of Congress.[13]

6.2.2 Providing guidance to operational offices, officers, agents, and analysts regarding information disclosure issues; and

6.2.3 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.

7. INFORMATION DISCLOSURE PROCEDURES

7.1 All disclosures of records associated with employees to third parties require coordination between the CBP Privacy Office (privacy.cbp@cbp.dhs.gov) and the Office of Public Affairs, as well as personnel from the Office of the Commissioner, the Office of Human Resources Management, and the relevant operational components. Disclosures may occur following:

7.1.1 An analysis that demonstrates that the privacy interests of the subject are outweighed by the legitimate public interest or by the Agency's need to shine light on its activities and operations;

7.1.2 A determination by the CBP Privacy Officer that the release aligns with a condition of disclosure under the Privacy Act;[14] and

7.1.3 An analysis to ensure the release aligns with an approved Routine Use listed in an applicable SORN as determined by the CBP Privacy Officer.

7.2 Information may be proactively disclosed if the information provided by CBP would clarify erroneous media reporting or the public's understanding of a specific incident or the involvement of a CBP employee in an incident.

7.3 Disclosures in response to third-party requests should be limited to name and duty status (active, indefinite leave, absent without leave, no longer employed, etc.):

---

[13] The provision of records associated with CBP personnel to a member of congress is limited to those members of congress serving as a Committee Chairperson, on a committee with standing and oversight of DHS/CBP operations, acting on behalf of their committees. A request from a member of congress on behalf of a constituent will not be treated as an official sharing.

[14] 5 U.S.C. § 552a(b)(1)-(12).

7.3.1 Disclosures must not include Social Security Number; date of birth; disability status; race and national origin; ethnicity; gender; citizenship status; Federal Employees Health Benefits Program data; Federal Employees Group Life Insurance data; Salary information; Federal Employees Retirement System coverage; veterans' preference; educational achievement and/or degree attained; performance rating level; current appointment authority; legal authority; dynamics category (broad categories of accessions, separations, and terminations); or any other information specifically protected from release under OPM policy.[15]

7.4 All requests must be reviewed to determine whether the proposed use of any disclosed records is consistent with the purpose for which DHS collected the records, and that their disclosure is in line with the FIPPs.[16]

7.5 All requests from third parties must be submitted in writing and maintained in a manner that will facilitate review and auditing as necessary to ensure compliance with established policy and legal requirements.

7.6 Ensure that releases only involve records collected and maintained by CBP, and that the records or information contained therein do not belong to another agency.[17]

7.7 Ensure that the information being disclosed is appropriately marked and/or redacted in accordance with Section 8 of this Directive.

7.8 Ensure that any disclosures of records associated with employees are properly accounted for through the completion of a DHS-191 Form, other Privacy Act Disclosure Record, or other form or process specifically authorized by the Chief Privacy Officer:[18]

7.8.1 The original DHS-191, or other approved method of Privacy Act Disclosure Record, must be retained by the CBP office releasing the information for a period of five years. A copy must also be submitted to the CBP Privacy and Diversity Office at privacy.cbp@cbp.dhs.gov.

8. Redactions

---

[15] See: The U.S. Office of Personnel Management (OPM) Data Release Policy, (August 2020), available at https://www.opm.gov/policy-data-oversight/data-analysis-documentation/data-policy-guidance/data-standards/data-release-policy-august-2020.pdf.

[16] The FIPPs form the basis of the Department's privacy compliance policies and procedures governing the use of personally identifiable information (PII). These principles are: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing.

[17] Third Agency Information. In instances where the requested data belongs to another agency, CBP personnel must coordinate with the agency that owns the information for written approval to share it or direct the requestor to the agency that owns the information.

[18] 5 U.S.C. § 552a(c).

8.1 A review must be conducted to ensure that all necessary redactions and/or markings have been completed before records associated with employees are disclosed, including:

8.1.1 Ensuring that information about individuals who are not the subject of a request is either excluded or redacted;[19]

8.1.2 Redacting any computer screen codes, internal file codes, or system codes;

8.1.3 Redacting any Law Enforcement Sensitive (LES) information,[20] whether it is explicitly marked as such, or if the release of unmarked information could compromise an open case or investigation;

8.1.4 Redacting any information owned by another agency or foreign entity that has not been approved for disclosure;

8.1.5 Redacting any other information that is not appropriate for disclosure that may be present; and

8.1.6 The crossing out of markings (e.g., FOUO/LES) already included on the copy of the record that is being disclosed.

9. NO PRIVATE RIGHT 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

[19] Pursuant to Section A. "The Presumption of Openness" of the Attorney General's Freedom of Information Act Guidelines (March 15, 2022), CBP treats identifying information associated with Senior Executive Service (SES) personnel as generally releasable, classifying them by policy as public officials.

[20] Law Enforcement Sensitive data is information or records from law enforcement systems or collections that are used for investigative or confidential purposes by law enforcement officers.