

**FOR OFFICIAL USE ONLY**

**U.S. DEPARTMENT OF HOMELAND SECURITY  
U.S. Customs and Border Protection**

**CBP DIRECTIVE NO. 1450-027**

**DATE: February 1, 2024**

**ORIGINATING OFFICE: OC-PDO**

**REVIEW DATE: February 1, 2027**

**DISCLOSURE OF PERSONALLY IDENTIFIABLE INFORMATION FOR PUBLIC  
AFFAIRS PURPOSES**

1. **PURPOSE.** This Directive is designed to provide U.S. Customs and Border Protection (CBP) personnel with procedures for the disclosure of CBP information associated with individuals encountered by or in the custody of the agency for external, public communications purposes to ensure compliance with all applicable statutes, regulations, and U.S. Department of Homeland Security (DHS) or government-wide policies.<sup>1</sup>
2. **SCOPE.** This Directive applies to all CBP personnel as defined in Section 5, particularly those individuals with job-related duties that include the public disclosure of CBP information, specifically personally identifiable information (PII), through the generation and dissemination of media releases, images, or posts to agency-owned social media accounts.
3. **POLICY.** It is the policy of CBP to permit the disclosure of agency-owned information containing PII to the news media, social media, and the public at large, in certain circumstances as described below. As a matter of policy, and for the purpose of this Directive, CBP applies the same administrative protections associated with the disclosure of information afforded under the Privacy Act<sup>2</sup> to all individuals regardless of their citizenship, nationality, or immigration status.
4. **AUTHORITIES.**
  - 4.1 “E-Government Act of 2002,” as amended, Public Law 107-347 Section 208 (Title 44, United States Code (U.S.C.), § 3501 note).
  - 4.2 “The Freedom of Information Act”, 5 U.S.C. § 552.

---

<sup>1</sup> This Directive does not apply to the disclosure of information associated with CBP personnel through media releases or postings related to misconduct, internal investigations, or arrests as a result of actions outside the agency.  
<sup>2</sup> 5 U.S.C. § 552a.

**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

- 4.3 The Privacy Act of 1974, as amended (5 U.S.C. § 552a).
- 4.4 “Privacy Officer” (6 U.S.C § 142).
- 4.5 The Federal Information Security Management Act of 2002, as amended (FISMA) (44 U.S.C., Chapter 35, Subchapter II, “Information Security”).
- 4.6 “Disclosure of records and information” (Title 6, Code of Federal Regulations (CFR), Chapter 1, Part 5).
- 4.7 “Availability of Information” (19 CFR Chapter 1, Part 103).
- 4.8 Office of Management and Budget (OMB) M-17-12 “Preparing for and Responding to a Breach of Personally Identifiable Information” (January 3, 2017).
- 4.9 DHS Directive 262-16, “DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information (May 4, 2022).
- 4.10 DHS Directive 262-19 “DHS Use of Social Media and other Third-Party Digital Services” (July 28, 2023).
- 4.11 DHS Instruction 262-16-001, “Implementing Instruction for DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information (May 4, 2022).
- 4.12 DHS Instruction 047-01-005, “Component Privacy Officer” (February 6, 2017).
- 4.13 DHS Instruction 047-01-007, “Handbook for Safeguarding Sensitive PII” (December 4, 2017).
- 4.14 DHS Instruction 047-01-008 “Privacy Incident Handling Guidance” (April 28, 2020).
- 4.15 DHS Instruction 262-19-001 “DHS Use of Social Media and other Third-Party Digital Services (Instruction)” (July 28 2023).
- 4.16 CBP Directive 2120-010A, “Privacy Policy, Compliance, and Implementation” (July 29, 2022).

## 5. DEFINITIONS

- 5.1 **CBP Information:** Any item, collection, or grouping of information about an individual (i.e., personally identifiable information) that is collected or maintained by CBP. The release of any information maintained by CBP but owned by another agency is not CBP Information for purposes of this Directive and must be expressly authorized by the owning agency prior to its disclosure.

FOR OFFICIAL USE ONLY

## FOR OFFICIAL USE ONLY

- 5.2 CBP Privacy Office:** The CBP Privacy Office is a division within the CBP Privacy and Diversity Office, under the Office of the Commissioner. The CBP Privacy Office is tasked with developing and fostering a culture of privacy at CBP by promoting transparency and data integrity in all border security, immigration, and law enforcement activities; as well as assuring that the use of technologies sustains, and does not erode, privacy protections relating to the use, collection, and disclosure of personal information.
- 5.3 CBP Privacy Officer:** The senior official within CBP with primary responsibility for privacy compliance and policy, including, but not limited to: monitoring CBP compliance with all federal privacy laws and regulations; implementing corrective, remedial, and preventative actions; assisting in drafting and reviewing all forms of privacy compliance documentation; serving as the point of contact to handle privacy incident response responsibilities; implementing and monitoring privacy training for CBP personnel; contributing CBP information responsive to the public reporting requirements of the DHS Privacy Office; and communicating CBP privacy initiatives, both internally and externally.
- 5.4 Employee or Personnel:** All permanent and temporary CBP employees, non-CBP personnel serving with CBP, contract personnel, and any other personnel that are assigned duties related to communicating with internal and external entities.
- 5.5 Individual:** Any natural person.<sup>3</sup>
- 5.6 Personally Identifiable Information (PII):** Any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, or a visitor to the United States.<sup>4</sup> For the purposes of this Directive, a photograph, even if obfuscated, may include PII based on other information, such as extremely unique clothing or rare items present in the image that are linkable to a specific person.<sup>5</sup>

---

<sup>3</sup> As a matter of law, the Privacy Act of 1974 (Privacy Act), as amended (5 U.S.C. § 552a), prohibits non-disclosure of Privacy Act records, absent an authorized disclosure exception, only for U.S. citizens and Lawful Permanent Residents. This prohibition of Privacy Act records extends to covered persons under the Judicial Redress Act of 2015, Pub. L. 114-126 (JRA). As a matter of policy, DHS extends this prohibition to all persons, regardless of immigration status, consistent with the Fair Information Practice Principles and applicable law.

<sup>4</sup> 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).

<sup>5</sup> For the purposes of this directive, "extremely unique" describes any custom, rare, or original articles of clothing, jewelry, luggage, or other accessories; or a combination of regular articles of clothing, jewelry, luggage, or other

FOR OFFICIAL USE ONLY

## FOR OFFICIAL USE ONLY

- 5.7 Privacy Incident:** The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users have access or potential access to PII in usable form, whether physical or electronic, or where authorized users access PII for an unauthorized purpose. Privacy Incidents include both suspected and confirmed incidents involving PII that raise a reasonable risk of harm. The determination of what constitutes a Privacy Incident will be made by the CBP Privacy Office, subject to confirmation and oversight by the DHS Privacy Office. The term “Privacy Incident” will be used synonymously with the term “breach.”
- 5.8 Public Affairs Liaison (PAL):** Employees outside the GS-1035 series who, in either a collateral-duty or full-time capacity and working on behalf of a CBP component or office, assists in internal and external communications efforts. While task direction flows from respective Executive Assistant Commissioner, Chief of the U.S. Border Patrol or Assistant Commissioner, programmatic direction in these efforts flow from the Office of Public Affairs.
- 5.9 Public Affairs Specialist (PAS):** GS-1035 series employees assigned to the Office of Public Affairs who are responsible for administering, supervising, or performing work involving communications between CBP and internal, external, foreign, or domestic audiences; specifically the development of informational materials that inform the public of the agency's policies, programs, services and activities, identifying communications needs, and planning, executing, and evaluating the effectiveness of information and communication programs in furthering agency goals.
- 5.10 Sensitive Personally Identifiable Information (SPII):** Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfair treatment of an individual.<sup>6</sup>

## 6. RESPONSIBILITIES

- 6.1 All CBP personnel who seek to disclose agency information containing PII are responsible for:**
- 6.1.1** Complying with this Directive and with privacy policies and procedures issued by the DHS Chief Privacy Officer and by CBP’s Privacy Officer;

---

accessories together with the physical attributes of an individual (tattoos, height, body stature, hair color, etc.), that could allow for the identification of a specific individual.

<sup>6</sup> Examples include Alien Registration Number, Social Security number, financial account numbers, license number, passport number, or biometric identifiers.

FOR OFFICIAL USE ONLY

**FOR OFFICIAL USE ONLY**

- 6.1.2** Protecting PII as required by the Privacy Act, as well as DHS and CBP privacy policy, from unauthorized disclosure, public dissemination and display;
  - 6.1.3** Reporting any suspected or actual Privacy Incidents, including unauthorized disclosures or unauthorized uses of properly disclosed PII, as required by Section 8 of this Directive and the DHS Privacy Incident Handling Guidance; and
  - 6.1.4** Requesting CBP Privacy Officer's approval for release of Privacy Act Information not authorized by this Directive.
- 6.2 Public Affairs Specialists (PAS) and Public Affairs Liaisons (PAL) are responsible for:**
- 6.2.1** Disseminating timely and accurate CBP information to the public through the development of news releases (PAS) and/or social media postings (PAS and PAL) to CBP-owned accounts;
  - 6.2.2** Protecting sensitive, proprietary, or personal information from unauthorized disclosure;
  - 6.2.3** Coordinating with the CBP Privacy Office, and Office of Chief Counsel (OCC) as appropriate, prior to the public disclosure of PII via a public release, social media posting, or in response to a request from a representative of the media; and
  - 6.2.4** Ensuring the removal or adequate redaction of any PII that has not been authorized for disclosure in a news release or social media posting.
- 6.3 Supervisors are responsible for:**
- 6.3.1** Providing appropriate supervisory oversight of news releases and postings containing CBP information to agency-owned social media accounts to ensure compliance with applicable laws and policies, including this Directive.
- 6.4 The CBP Privacy Officer is responsible for:**
- 6.4.1** Ensuring compliance with established legal and DHS policy requirements associated with the release of CBP information containing PII, to include consultation and approval from the DHS Chief Privacy Officer and DHS Office of the General Counsel;

**FOR OFFICIAL USE ONLY**

## **FOR OFFICIAL USE ONLY**

- 6.4.2 Providing guidance to the Office of Public Affairs related to the disclosure of information, specifically for requests involving the use of CBP information containing PII; and
- 6.4.3 Reviewing proposed disclosures to ascertain compliance with this Directive as needed.

### **6.5 The Office of Chief Counsel (OCC) is responsible for:**

- 6.5.1 Providing CBP personnel with legal guidance related to any proposed disclosures, as needed, particularly those involving ongoing litigation.

### **6.6 The Assistant Commissioner for the Office of Public Affairs (OPA) is responsible for:**

- 6.6.1 Ensuring that OPA personnel, including Public Affairs Specialists assigned to field locations and Public Affairs Liaisons assigned to CBP components or offices, adhere to procedures regarding the release of PII as part of news releases and social media posts as established under Section 8 of this Directive;
- 6.6.2 Providing oversight of the use of CBP information in news releases or social media posts to CBP-owned accounts, as well as those occurring in response to media requests (this Directive does not mandate the release of information to the news media; all releases are made solely at the agency's discretion consistent with its authorities); and
- 6.6.3 Ensuring designated personnel are provided appropriate training on the roles and responsibilities of Public Affairs Specialists, prior to any active engagement in the development of news releases or social media posts.

## **7. DISCLOSURE OF CBP INFORMATION CONTAINING PII**

### **7.1 General Prohibitions or Limitations on Disclosures of CBP information containing PII:**

- 7.1.1 Disclosures of CBP Information containing PII, including images, as part of a news release or social media post are not permitted unless approved by the CBP Privacy Officer (or designee). OPA shall use the procedures described in Section 8 to request case-by-case approval for such releases.
- 7.1.2 CBP Information, including photographs of any individual, whether blurred or unblurred, shall not be released without specific approval from the CBP Privacy Officer (or designee).
- 7.1.3 CBP information that is subject to restrictions on disclosure due to its association with individuals in a protected class must not be disclosed as part

**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

of a news release or social media posting. This includes, but is not limited to, information protected by 8 U.S.C. § 1367 (related 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, as victims of a severe form of human trafficking who generally are cooperating with law enforcement authorities, or as aliens who have suffered substantial physical or mental abuse and are cooperating with law enforcement authorities); 8 C.F.R. § 208.6 (related to certain refugee and asylee information); and 8 C.F.R. § 244.16 (related to Temporary Protected Status application information). Consult with CBP Office of Chief Counsel and the CBP Privacy Office if the response to a media inquiry or agency-generated release may involve protected class data.

- 7.1.4 The disclosure of CBP Information associated with individuals on the Terrorist Screening Dataset (TSDS) watchlist, Classified or National Security data; or information attributed to Intelligence Community (IC) partners as part of a news release or social media posting is prohibited. Consult with CBP Office of Intelligence, CBP National Targeting Center, CBP Office of Chief Counsel, and the CBP Privacy Office to ensure a response to a media inquiry or agency-generated posting does not involve the release of such information.
  - 7.1.5 The disclosure of booking photographs or images maintained within a CBP law enforcement system in association with a criminal or immigration encounter is prohibited. However, CBP personnel may disclose images captured for the specific purpose of a media release subject to the requirements in this Directive.
  - 7.1.6 Releases identifying DHS or CBP personnel performing work-related functions while on duty, whether by photograph or through the inclusion of other information, should, where practicable, only be used when the subject personnel provided consent.
  - 7.1.7 CBP Information that originates from another agency may not be released without the express prior consent of the owning agency.
- 7.2 Generally Permissible Disclosures of CBP Information containing PII:
- 7.2.1 De-identified descriptions of individuals who are the subject of encounters or enforcement actions. Personnel drafting, reviewing, approving, or disseminating media releases or social media postings shall ensure the individual is not named or otherwise able to be identified. The specific location or time of an encounter or arrest may need to be withheld or generalized to ensure these individuals cannot be identified.

FOR OFFICIAL USE ONLY

## FOR OFFICIAL USE ONLY

- 7.2.2** Identifying information associated with individuals who are the subject of encounters or enforcement actions with the approval of the CBP Privacy Officer (or designee). News releases or social media postings may include:
- 7.2.2.1** Name, age, country of citizenship, nationality, and photograph;
  - 7.2.2.2** The circumstances immediately surrounding an encounter or arrest, including the time and place, resistance, pursuit, possession and use of weapons, a description of any items seized, as well as the resolution of the encounter; and
  - 7.2.2.3** Criminal history, specifically any felony crimes that the individual has either been convicted of or has an active warrant for.
- 7.2.3** Prior to a proposed release, the office generating the disclosure should make reasonable efforts to deconflict the proposed release, ensuring that the disclosure will not negatively impact or undermine ongoing operations or law enforcement activities.
- 7.2.4** Information containing PII may be released to the media or social media if an individual has provided written consent authorizing the release, so long as the individual has the capacity to consent (i.e., is not a minor) and is not in custody at the time of the waiver. Questions regarding the validity or scope of an individual's consent waiver should be directed to the CBP Privacy Office and the Office of Chief Counsel. Copies of consents and waivers must be maintained by OPA (if executed by a Public Affairs Specialist) or the respective CBP component or office (if executed by a Public Affairs Liaison) for five years in accordance with the accounting for disclosure requirements explained in this Directive.
- 7.3** News releases or social media postings including photographs must be redacted to ensure that the subject is unrecognizable, unless the use of unredacted images is otherwise authorized pursuant to this Directive or by the CBP Privacy Office:
- 7.3.1** The bodies, facial features, and any identifiable clothing or belongings of children and other vulnerable populations<sup>7</sup> must be blurred until all distinguishing characteristics are distorted;
  - 7.3.2** The use of black boxes or rectangles over the eyes of an individual are not sufficient;

---

<sup>7</sup> Vulnerable populations include but are not limited to children, victims of human trafficking, and individuals experiencing medical emergencies.

FOR OFFICIAL USE ONLY



## FOR OFFICIAL USE ONLY

7.3.3 All photographs of individuals,<sup>8</sup> whether redacted or not, will be submitted to the CBP Privacy Office ([cbp-privacymediareleases@cbp.dhs.gov](mailto:cbp-privacymediareleases@cbp.dhs.gov)) for review and approval prior to use.

### 8. SUBMISSION, REVIEW, AND APPROVAL PROCESS

8.1 The CBP Privacy Officer authorizes the release of CBP information containing PII through a news release or posting to CBP-owned social media accounts on a case-by-case basis. All releases must meet the following standards:

8.1.1 The release must not constitute an unwarranted invasion of personal privacy.

8.1.2 If there is no unwarranted invasion of privacy as determined by the CBP Privacy Officer (or designee), the release must meet one of the following criteria:

8.1.2.1 There is legitimate public interest in the release of the information;

8.1.2.2 Release sheds light on agency operations;

8.1.2.3 Release is necessary to preserve confidence in the integrity of CBP; or

8.1.2.4 Release is necessary to demonstrate the accountability of CBP personnel.

8.2 Public Affairs Specialists and Public Affairs Liaisons will send a request for authorization to release information about an individual to the CBP Privacy Office ([cbp-privacymediareleases@cbp.dhs.gov](mailto:cbp-privacymediareleases@cbp.dhs.gov)). To ensure a timely response, the request shall be drafted based upon guidelines below:

8.2.1 The submission email should outline the nature of the disclosure, including whether the release is proactive or in response to a request (e.g., reporter asked specific questions about individual situation and CBP wishes to issue a press release);

---

<sup>8</sup> Exempt from this review requirement are photographs depicting CBP personnel engaged in their assigned duties and individuals in a public space so long as they were not previously, or subsequently will be, in CBP custody.

FOR OFFICIAL USE ONLY

## FOR OFFICIAL USE ONLY

**8.2.2** Requests must include a draft of the proposed news release or social media posting and contain sufficient information and context for the CBP Privacy Officer to make an informed decision; and

**8.2.3** Appropriately redacted versions of any images or photographs to be included with the news release or social media posting.

**8.3** Where possible, and in coordination with relevant CBP operational offices as appropriate, PAS and PAL personnel should deconflict all news releases and social media postings with appropriate Law Enforcement entities to ensure that the public release of information will not undermine ongoing criminal investigations; and

**8.4** In accordance with established DHS and CBP System of Records Notices, any release containing information covered by the Privacy Act or Departmental policy extension<sup>9</sup> must be approved by the DHS Chief Privacy Officer, in consultation with the Office of General Counsel.<sup>10</sup>

## 9. PRIVACY INCIDENT HANDLING AND RESPONSE

**9.1** Any unauthorized disclosure of CBP information containing PII, including images, is considered a Privacy Incident and must be promptly reported to the Joint Intake Center.

**9.2** In accordance with DHS Privacy Incident Handling Guidance (DHS Instruction 047-01-008), all Privacy Incidents are to be immediately reported, as appropriate, to the CBP Privacy Office ([privacyincidents@cbp.dhs.gov](mailto:privacyincidents@cbp.dhs.gov)) or DHS Security Operations Center (SOC) at (703) 921-6507 for review, investigation, and remediation, as necessary.

**9.3** Unauthorized disclosure of CBP information containing PII may be grounds for disciplinary action, consistent with applicable law and CBP policy, and may be subject to criminal sanctions.

**10. MEASUREMENT/AUDIT.** CBP Privacy and Diversity Office, may elect to conduct formal or informal audits or reviews to assess compliance with this Directive.

---

<sup>9</sup> 5 U.S.C. § 552a. As a matter of policy, DHS Privacy Policy 262-16 extended administrative Privacy Act certain rights and protections to all individuals, regardless of their citizenship. Additionally, covered persons are granted certain Privacy Act rights and protections under the Judicial Redress Act of 2015, Pub. L. 114-126 (JRA).

<sup>10</sup> DHS and CBP System of Records Notices (SORNs) contain the following Routine Use: "To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy."

FOR OFFICIAL USE ONLY

**FOR OFFICIAL USE ONLY**

**11. TRAINING REQUIREMENTS**

**11.1** All CBP personnel assigned to Public Affairs Specialists or Public Affairs Liaison roles must complete training as designated by OPA annually to include OPA social media training if managing social media accounts on behalf of CBP;


**11.2** All CBP personnel must complete “Privacy at DHS: Protecting Personal Information” in the DHS Learning Management System or successor training course annually; and

**11.3** All CBP personnel must complete remedial or refresher training as required in response to a Privacy Incident.

**12. POINT OF CONTACT.** Any questions regarding this directive, the process that it establishes, and/or the requirements outlined above can be directed to the CBP Privacy Officer ([privacy.cbp@cbp.dhs.gov](mailto:privacy.cbp@cbp.dhs.gov)).

**13. NO PRIVATE RIGHT CREATED.** This document is for internal CBP use only and does not create or confer any rights, privileges, or benefits for any person or entity.

**13. APPROVAL.**

 FEB 01 2024  
\_\_\_\_\_  
Troy Miller (Date)  
Senior Official Performing the Duties of the Commissioner  
U.S. Customs and Border Protection

**FOR OFFICIAL USE ONLY**