

(b)(6);(b)(7)(C)

Subject: FW: West Texas CBP Twitter account

From: (b)(6);(b)(7)(C)

Sent: Saturday, September 10, 2022 7:08 PM

To: (b)(6)

(b)(6)

Cc: (b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

Subject: West Texas CBP Twitter account

(b)(6);(b)(7)(C)

The @CBPWestTexas Twitter handle is an OPA account assigned to field PAOs. I am referring the inappropriate posting conduct to OPR.

Our current problem trying to correct the issue is the two-factor authentication goes to an old @dhs.gov account which no longer exists. CoS (b)(6);(b)(7)(C) has directed we delete the account so we have reached out to Twitter via email; I have included (b)(6) in case she has a contact that can help us accomplish this.

Here is the OC approved statement for any inquiries:

"U.S. Customs and Border Protection has become aware of inappropriate content which was posted to the @CBPWestTexas Twitter account. CBP is taking action to delete the account and has referred the matter to it's Office of Professional Responsibility."

(b)(6);(b)(7)(C)

Deputy Assistant Commissioner

Office of Public Affairs

U.S. Customs and Border Protection

Office: (b)(6);(b)(7)(C)

Mobile:

Email: (b)(6);(b)(7)(C)

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

CBP INTERIM POLICY

DATE: December 20, 2019
ORIGINATING OFFICE: OPA

CBP Public Affairs Official Use of Social Media

1. **PURPOSE.** This interim policy establishes U.S. Customs and Border Protection (CBP) official public affairs use of social media platforms and tools. It describes the official use by CBP offices and components of a social media account as a means of communication and public engagement. This policy serves as the primary policy on official public affairs use of social media for all offices and components within the Agency.
2. **SCOPE.** This interim policy applies to all CBP offices and components. This policy does not apply to the Operational Use of Social Media nor online engagement in a personal capacity, except where such personal engagement gains national public attention.
3. **POLICY.** Social media tools are intended to be used as part of a larger, integrated communications program or project developed under the leadership of the CBP Office of Public Affairs (CBP OPA). It is the policy of CBP that social media tools be accessed and used in a responsible manner. Official use of social media to communicate and engage with the public must be in accordance with all applicable Federal laws, regulations, and policies including those regarding accessibility; records management; information quality; and intellectual property.
4. **BACKGROUND.** CBP encourages the use of social media to enhance the Agency's communication efforts. The use of social media enables enhanced awareness and education about CBP, its mission and operations. Social media facilitates improved communications that are relevant, timely, credible, and responsive to the CBP mission and public interest.
5. **AUTHORITIES.** Authorities applicable to this policy are provided below. Additional federal policies, regulations, and laws that guide how digital/social media tools can and should be used are provided in the Appendix.
 - A. The President's January 21, 2009, Memorandum on Transparency and Open Government
 - B. Presidential Memorandum on Building a 21st Century Digital Government, May 23, 2012
 - C. OMB M-10-06, Open Government Directive, December 8, 2009
 - D. OMB Memorandum M-10-23, Guidance for Use of Agency Third-Party Websites and Applications, June 25 2010
 - E. OMB Memorandum for the Heads of Executive Department Agencies, and

~~FOR OFFICIAL USE ONLY~~

Independent Regulatory Agencies, Social Media, Web-Based Interactive Technologies

- F. OMB Memorandum M-17-06, Policies for Federal Agency Public Websites and Digital Services.
- G. Appropriate Use of the Internet
- H. Rules of Behavior for Computer Network Users
- I. *The Standards of Ethical Conduct*, 5 C.F.R. Part 2635
- J. CBP Directive 51735-013A Standards of Conduct
- K. CBP Directive #51713-011 Anti-Discriminatory Harassment
- L. CBP Directive #1440-026A Reporting Allegations of Employee Misconduct
- M. CBP Directive #51735-010C Administrative Inquiries
- N. LER Supervisor's Reference Guide
- O. CBP Directive #5410-001B OPA Roles, Functions, and Responsibilities
- P. CBP Directive #5230-031A Limited Personal Use of Government Office Equipment
- Q. CBP Memo - Social Media Posts
- R. CBP Directive #5220-038 Purchasing Seals, Logos, and Branding-Related Merchandise
- S. Anti-Discrimination and Anti-Harassment, June 5, 2019
- T. OGE Legal Advisory LA-15-03
- U. CBP RIM Directive (2110-040)

6. DEFINITIONS.

Social Media – The sphere of websites, applications, and web-based tools that connect users to engage in dialogue, share information and media, collaborate, and interact. Social media takes many different forms, including but not limited to: web-based communities and hosted services, social networking sites, video and photo sharing sites, blogs, virtual worlds, social bookmarking, and other emerging technologies. This definition does not apply to internal intranets or applications.

CBP Components – The operational and support elements of U.S. Customs and Border Protection, such as: the Office of the Commissioner, Enterprise Services, Air and Marine Operations, Office of Field Operations, Office of Intelligence, Office of Operations Support, Office of Trade, Office of Professional Responsibility, and U.S. Border Patrol.

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.

Account Manager – CBP employee who manages an official CBP social media account.

7. OFFICIAL USE OF SOCIAL MEDIA. CBP offices and components use social media to communicate their missions to the public. CBP OPA provides current guidance on the use of social media, including specific types of social media platforms available for use.

7.1 CBP offices and components may use only approved social media platforms. Social media

~~FOR OFFICIAL USE ONLY~~

platforms are approved for use following official review by CBP OPA.

7.2 Employees must be granted approval by CBP OPA to use social media, or other third-party services, in an official capacity to directly support or enhance activities being undertaken. This includes receiving approval to create social media accounts for locations, programs, offices, and employees that are to be used for official work. Content created in an official capacity may constitute a federal record and is subject to relevant information related laws and regulations, including the Freedom of Information Act.

7.3 CBP offices and components must follow the approval process detailed in the Standard Operating Procedures when creating social media accounts. Any social media account that has not been approved via the approval process detailed is subject to immediate termination. Approval is required to ensure:

- Cross-departmental alignment of social media efforts and reduce duplication in accounts; and
- When appropriate, information is delivered to the general public in the context of unified themes or messages.

7.4 CBP will maintain a list of all official social media accounts on its public website.

7.5 Official social media accounts (both new and already existing) must have a primary point of contact who is responsible for managing account security and overseeing activity on the account. The contact must be a full-time, permanent federal employee.

7.6 Before gaining access to an official social media account, employees must take CBP OPA's social media training.

7.7 Content published to official social media accounts must be approved through appropriate communication channels before publication or distribution. For more information, contact CBP OPA's Director of Digital Engagement.

7.8 Records must be maintained for original or unique content created or published to social media accounts or platforms, including information posted by individuals acting on behalf of the Agency.

8. **GUIDING PRINCIPLES FOR OFFICIAL USE OF SOCIAL MEDIA.** The following principles should be employed when using social media platforms in an official capacity within CBP:

i. Do not post any information that is considered non-public information and has not been approved for release through the procedures set forth. The posting of internal (e.g., For Official Use Only), sensitive (e.g., Law Enforcement Sensitive), proprietary, or classified information is strictly prohibited. Failure to comply may result in disciplinary action.

ii. Do not use social media platforms as the sole venue for conducting official government business or disseminating information related to official CBP functions. Press releases and other official announcements should also be provided in another publicly available format such as the CBP website.

iii. When representing CBP in an official capacity, the account owner is responsible for the content published. Any content posted to a social media platform while acting in an official capacity is considered public content, regardless of any privacy controls that restrict access to that content. Always assume the content will be available to a large

~~FOR OFFICIAL USE ONLY~~

audience, may be published and discussed in the media, and is subject to FOIA, discovery, and other rules requiring public disclosure.

iv. When using social media in an official capacity (when either managing an official organizational account or an official individual account), know and follow all applicable laws, regulations, and guidelines, such as the Appropriate Use of the Internet, Rules of Behavior for Computer Network Users, and the Standards of Ethical Conduct for Employees of the Executive Branch. Restrictions include, but are not limited to:

1. Do not use vulgar or abusive language, personal attacks of any kind, or offensive terms targeting individuals or groups.
2. Do not endorse products or services.
3. Do not solicit donations of any kind.
4. Do not engage in activity directed toward the success or failure of political parties, candidates, or groups.
5. Do not advocate for a policy or particular piece of legislation.

9. **PERSONAL (NON-OFFICIAL) USE OF SOCIAL MEDIA.** Official CBP social media accounts should remain distinctly separate from personal social media accounts. The Federal Standards of Ethical Conduct prohibit employees from using their official titles, positions, or any authority associated with their public office for private gain. The CBP Standards of Conduct further require that "... employees will not use the authority of their position in any way that might result in adversely affecting public confidence in the integrity of CBP and of the government." Statements intended as personal opinion can be mistaken for official expressions of agency policy or position. Care must be taken to ensure that personal use of social media does not create the appearance of official use of social media, such as by the use of a government title or position in a manner that would create an appearance that the Government sanctions or endorses one's activities. Employees should refrain from utilizing Agency insignia, uniforms, and titles in personal postings because of the likelihood of confusion that could arise among the public or the appearance of government endorsement that could be created. Identifying an official title or position in an area of a personal social media account designated for biographical information, though, is ordinarily permissible. Employees should also avoid supplemental citations to their job or title, or using their insignia or uniform or similar images, when posting personal content. Additionally, many ethics laws, regulations, and policies that apply to an employee's official activities also apply to employee activities in their personal lives. Where confusion or doubt is likely to arise regarding the personal nature of social media activities, employees should include a clear and conspicuous disclaimer on their personal social media page clarifying that their social media communications reflect only the employee's personal views and do not represent the views of CBP or the United States. An example of an appropriate disclaimer:

This post represents my own opinion and does not represent the positions, strategies, or work of the U.S. Department of Homeland Security, Customs and Border Protection, or the Federal Government.

Such a disclaimer does not mitigate the employee's professional responsibilities under the aforementioned regulations and policies, nor does it eliminate the Agency's authority to take

~~FOR OFFICIAL USE ONLY~~

disciplinary action against the employee. Employee conduct, whether on-duty or off-duty, whether online or in person, must consistently embody CBP's core values, service to our nation, and commitment to each other. By doing so, it protects against policy and ethical violations, while also protecting the integrity of the Agency.

In the event an image, video, or other posting of CBP employees regarding CBP-related topics gains public attention or popularity, affected employees must promptly report and coordinate responses through OPA (cbpmediarelations@cbp.dhs.gov). Employees shall not respond on behalf of CBP without explicit authorization.

Questions concerning ethics restrictions applicable to the personal use of social media should be directed to the Office of Chief Counsel.

10. **PRIVACY.** While CBP may use social media, most platforms are controlled and operated by third parties that maintain and provide their own privacy and use policies. CBP employees shall make every effort to protect the privacy of the public, self and others.

10.1 CBP will engage on these platforms in a manner that protects privacy, respects the intent of users and does not solicit or collect personally identifiable information (PII).

10.2 The creation and use of official CBP accounts on third-party websites and applications may cause personally identifying information to become available or accessible to the Agency. Such information may become available to the Agency when a user provides, submits, communicates, links, posts, or associates information with official CBP accounts (e.g., through "liking," "following," responding to tweets, or commenting on content provided by the Agency). The Agency does not control, moderate, or endorse the comments or opinions provided by social media users on official CBP accounts.

10.3 Anyone can follow official CBP accounts. Official CBP accounts shall only follow verified accounts, including local, federal and state agencies, Departments, White House, POTUS, VP, FLOTUS, Second Lady, official Administration accounts, news outlets, and reporters.

11. **COMMENT POLICY.** CBP respects different opinions. CBP does not pre-moderate users' comments on social media accounts. This means that users' comments are automatically published, but they may be removed by a CBP official if they violate the below comment policy.

Comments may be removed from CBP social media accounts if they:

- Contain obscene, indecent or profane language;
- Contain threats or defamatory statements;
- Contain hate speech directed at race, color, sex, sexual orientation, national origin, ethnicity, age, religion or disability;
- Contain sensitive or personally identifiable information;
- Multiple successive off-topic posts by a single user or repetitive posts copied and pasted by multiple users, or spam; and/or
- Promote or endorse specific commercial services or products.

Questions concerning the removal of comments should be directed to the Office of Chief

~~FOR OFFICIAL USE ONLY~~

Counsel and CBP OPA.

12. **RECORDS MANAGEMENT.** All content generated by CBP is subject to the National Archives and Records Administration (NARA) records retention schedules for retention, storage and publication. Some official records may exist on third party social media platforms. It is the responsibility of the account manager and/or creator of the social media post to capture and preserve these records, along with relevant metadata such as the time, date, and author. The NARA-approved DHS Enterprise-wide records retention schedule requires social media records be retained for at least 5 years: https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/departments-of-homeland-security/rg-0563/daa-0563-2013-0003_sfl15.pdf.

(b) (6)

Michael J. Friel
(Acting) Assistant Commissioner
Office of Public Affairs

~~FOR OFFICIAL USE ONLY~~

Appendix

Federal Policies Applicable to the Official Use of Social Media

CBP employees using social media for official public affairs purposes are required to comply with all relevant federal laws, regulations, and policies, including, but not limited to, Section 508, Records Management, the Privacy Act, and the Freedom of Information Act.

Publicity, Propaganda, and Anti-Lobbying Provision

Annual appropriation acts typically contain provisions that generally prohibit the use of funds for publicity or propaganda purposes or in a way that tends to promote public support or opposition to any legislation pending before Congress. Exceptions to the general prohibitions include official presentations of the agency's stance on pending legislation when briefing Congress or in Congressional hearings, and certain actions undertaken by Senate confirmed Presidential appointees. The use of government resources, including social media accounts and employee time, to post social media messages that constitutes publicity, propaganda, or lobbying activities violate these provisions. Agencies directly appealing for members of the public to contact Congress is also prohibited.

Additionally, the Government Accountability Office (GAO) has determined that social media campaigns that promote agency messaging but conceal or otherwise mislead the public as to the agency's role in creating the campaign is prohibited activity. GAO has also found agency hyperlinks to external websites that contain calls to contact members of Congress in support or opposition of pending legislation is likewise prohibited.

Resources: 18 U.S.C. § 1913 for the general Anti-Lobbying Act

Section 508 (Accessibility)

Section 508 of the Rehabilitation Act of 1973, (as amended), requires that electronic and information technologies purchased, maintained, or used by the Federal Government meet certain accessibility standards. These standards are designed to make online information and services fully available to the 54 million Americans who have disabilities that would otherwise prevent them from having access to that content. Agencies are already required by Federal Acquisition Regulations to modify acquisition planning procedures to ensure that the section 508 standards are properly considered and to include the standards in requirements documents. The OMB reminds agencies to disseminate information to the public on a timely and equitable basis, specifically mentioning meeting the Section 508 requirements in OMB Memorandum M-06-02. Agencies employing non-Federal social media platforms are required to ensure that persons with disabilities have equal access to those services as defined in the Accessibility Standards. Third-party services have a varying degree of accessibility support, therefore it is incumbent upon offices to make their content as accessible as possible on those services. However, equivalent access to the same information should be made available on any CBP website.

FOR OFFICIAL USE ONLY

All content displayed on CBP websites must adhere to section 508 standards regardless of whether or not the content is created and hosted by CBP. Content created and hosted by a third party and displayed on a CBP website via a widget is subject to 508 compliance standards.

In January 2017, the federal government revised existing section 508 standards with the more comprehensive requirements of the Web Content Accessibility Guidelines (WCAG) 2.0, level AA standards. All CBP websites must conform to WCAG 2.0 Level AA standards.

Resources: 29 U.S.C. § 794(d) - Section 508 of the Rehabilitation Act, About the Section 508 Standards, and current and future OMB memos.

Records Management

When using electronic media, whether it is a blog, a website, social media, or any other type of electronic communication, the laws and regulations that govern proper management and archiving of records still apply. The National Archives and Records Administration offers resources and guidance to agencies to ensure proper records management.

Resources: OMB Circular A-130, "Management of Federal Information Resources," (see section 8a4); Implications of Recent Web Technologies for NARA Web Guidance

Information Quality

The public places a high degree of trust in government content and considers it an authoritative source. Under the Policies for Federal Agency Public Websites and Digital Services, agencies are required to maximize the quality, objectivity, utility, and integrity of information and services provided to the public. With regard to digital products, agencies must reasonably ensure suitable information and service quality consistent with the level of importance of the information. Reasonable steps include: (1) clearly identifying the benefits and limitations inherent in the information dissemination product (e.g., possibility of errors, degree of reliability, and validity), and (2) taking reasonable steps to remove the limitations inherent in the product or information produced. Agency management must ensure that the agency position is reflected in all communications rather than one person's opinion.

Resource: M-17-06: Policies for Federal Agency Public Websites and Digital Services Section 11

Availability of Information to Persons Without Internet Access

Agencies are required to provide members of the public who do not have internet connectivity with timely and equitable access to information, for example, by providing hard copies of reports and forms upon request.

Resources: OMB Circular A-130 (See 5(e)(2)(f))

~~FOR OFFICIAL USE ONLY~~

Usability of Data

Many digital technologies allow users to take data from one website and combine it with data from another, commonly referred to as "mashups." Agency public websites are required, to the extent practicable and necessary to achieve intended purposes, to provide all data in an open, industry-standard format that permits users to aggregate, disaggregate, or otherwise manipulate and analyze the data to meet their needs. Agencies need to ensure that these open industry-standard formats are followed to maximize the utility of their data.

Resource: [OMB Memo M-05-04](#)

Intellectual Property

CBP employees and components must comply with Copyright Law of the United States of America and Related Laws Contained in Title 17 of the United States Code and other Federal policies and directives when posting images, text, video, audio files in blogs or on third party social media websites.

Generally, U.S. Government works are not protected by intellectual property law. However, the absence of intellectual property protections does not mean that all Government works are considered Public Domain and public dissemination may be restricted by other authorities.

In addition, where an employee generates a joint work with outside entities pursuant to a contract or other agreement, the outside entity may have intellectual property rights to the final product as governed by the agreement. Employees should be careful about the nature of the work before posting to social media.

Resources: [Cendi](#), [Copyright.gov](#), [U.S. Trademark Law](#)

Privacy

Federal public websites and digital services are required to comply with all relevant Federal laws and policies, including the Privacy Act of 1974, E-Government Act of 2002, and Office of Management and Budget (OMB) policy. Agencies must provide privacy policies on websites, mobile applications and digital services, implement privacy controls to protect individual privacy, and post a privacy notice or "Privacy Act Statement" when personally identifiable information (PII) is collected that describes the legal authority for the collection, the purpose, and how the data will be used and shared. Privacy policies must be written in plain language and in a standardized machine readable format, and address the nature, purpose, use and sharing of information collected from individuals through websites or digital services.

Individuals may provide PII to CBP when communicating, posting, blogging, linking, submitting,

~~FOR OFFICIAL USE ONLY~~

or other comparable functions. Employees must take care to limit any collection of PII to that which is authorized and necessary for the performance of official duties in support of the CBP mission. A privacy notice should be provided at the point of collection or prominently displayed on pages where PII may be made available so individuals have an opportunity to read the notice and make informed choices about what information they wish to provide or how they want to interact with the agency. The provision of information should be voluntary in accordance with Federal law and CBP privacy policy. Alternatives should be provided (where possible) for individuals seeking information, assistance, or who do not want to provide PII.

Resources: Privacy Act of 1974, E-Government Act of 2002, OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies, OMB Memorandum M-17-06, Policies for Federal Agency Public Websites and Digital Services

Information Collection & Paperwork Reduction Act

Agencies are required, when possible, to use electronic forms and filing to conduct official business with the public, and social computing technologies can be used in many cases to meet this need. Federal public websites must ensure that information collected from the public minimizes burden and maximizes public utility. The Paperwork Reduction Act (PRA) covers the collection of data from the public. The PRA requires OMB approval of all surveys given to ten (10) or more participants. This includes any sort of survey in which identical questions are given to ten (10) or more participants, regardless of the format. The exception to the survey rule is an anonymous submission form where users can provide open-ended comments or suggestions without any sort of Government guidance on the content.

Resources: Paperwork Reduction Act, OMB Memorandum, "Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act"

Freedom of Information Act (FOIA)

Government-sourced content posted via social media sites or on public Government Web servers becomes part of the public domain upon posting. With limited exceptions, such content is therefore not exempt from FOIA requests.

Resource: FOIA (5 U.S.C. §552)

Ethics

When writing for, posting or participating on social media, an employee is either acting in their official capacity as a CBP employee or acting in a personal capacity. Typically, an activity is undertaken in official capacity when it is consistent with statutory authority and agency or office mission and assigned duties.

In particular there are specific rules around the use of personal social media with regards to political

~~FOR OFFICIAL USE ONLY~~

activity. If you have concerns that your personal use of social media may be interpreted as official use, please contact the Office of Chief Counsel.

All Government-wide and CBP standards and codes of ethical behavior for employees apply to employees' use of social networking and social media tools for both official and personal use including:

- 1) Hatch Act: FAQs on Federal Employees and the Use of Social Media and Email
- 2) Standards of Conduct as Applied to Personal Social Media Use

~~FOR OFFICIAL USE ONLY~~