



DHS OPERATIONAL USE OF SOCIAL MEDIA

This template is used to assess the Department's Operational Use of Social Media, consistent with Management Directive 110-01.

The DHS Privacy Office has created this template to determine privacy compliance with Management Directive 110-01, *Privacy Policy for Operational Use of Social Media*. For the purposes of the Management Directive and this template, "Operational Use" means authorized use of social media to collect personally identifiable information for the purpose of enhancing situational awareness, investigating an individual in a criminal, civil, or administrative context, making a benefit determination about a person, making a personnel determination about a Department employee, making a suitability determination about a prospective Department employee, or for any other official Department purpose that has the potential to affect the rights, privileges, or benefits of an individual. Operational use does not include the use of search engines for general Internet research, nor does it include the use of social media for professional development such as training and continuing education or for facilitating internal meetings. The following uses of social media are exempt from the Management Directive and are not subject to this requirement¹:

- a) Communications and outreach with the public authorized by the Office of Public Affairs (covered by the existing PIAs: [DHS/ALL/PIA-031 - Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue](#) and [DHS/ALL/PIA-036 - Use of Unidirectional Social Media Applications](#));
- b) The conduct of authorized intelligence activities carried out by the Office of Intelligence and Analysis, the intelligence and counterintelligence elements of the United States Coast Guard, or any other Component performing authorized foreign intelligence or counterintelligence functions, in accordance with the provisions of Executive Order 12333, as amended.

This template shall be used to document the process to be followed by all programs engaging in operational uses of social media; to identify information technology systems, technologies, rulemakings, programs, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer; and to assess whether there is a need for additional Privacy Compliance Documentation. Components may appeal to the Deputy Secretary for Homeland Security if there is disagreement over the DHS Privacy Office determination of privacy compliance for the operational use of social media.

¹ Gathering information by the Office of Operations Coordination and Planning (OPS) to enhance situational awareness is exempt from this requirement and is covered by the existing PIA: [DHS/OPS/PIA-004\(d\) - Publicly Available Social Media Monitoring and Situational Awareness Initiative Update](#).



DHS OPERATIONAL USE OF SOCIAL MEDIA

Please complete this form and send it to your Component Privacy Officer.
Upon receipt, your Component Privacy Officer and the DHS Privacy Office will review this form and may request additional information.

SUMMARY INFORMATION

Date submitted for review: 1/2/19

Name of Component: U.S. Customs and Border Protection

Contact Information: (b) (6), (b) (7)(C)

Counsel² Contact Information: (b) (6), (b) (7)(C) Deputy Associate Chief Counsel,
Enforcement & Operations, Office of Chief Counsel, U.S. Customs and Border Protection, (b) (6), (b) (7)(C) (Main)

IT System(s) where social media data is stored: The information may be stored on CBP SharePoint sites, CBP workstations, or in DHS electronic mail.

Applicable Privacy Impact Assessment(s) (PIA):

- The CBP Privacy Office finds that overarching PIA coverage for this effort is provided by:
 - DHS/ALL/PIA-056 DHS and Component Network IT Security Operations and Privacy and IT Security Incident Response, which outlines the Department's efforts to protect the confidentiality, integrity, and availability of DHS information and information assets.
 - Coverage under this PIA includes situations where CBP OIT identifies an issue of concern on Social Media in which the PII of the individual that posted it is not relevant or necessary. In those instances, CBP OIT would redact PII from any notifications or work products that are produced or stored.
 - DHS/CBP/PIA-010(a) Analytical Framework for Intelligence, which outlines CBP's efforts to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk, and aids in the enforcement of customs, immigration, and other laws enforced by DHS.
 - Coverage under this PIA includes situations where CBP OIT identifies a social media post in which a cyber-threat actor indicates an intent to conduct an attack on or hack of CBP. In these instances, the PII of the

² Counsel listed here must certify that appropriate authority exists to engage in particular operational activities involving social media.



individual that created the post is relevant and would be included in notifications and work products, and would be retained in AFI.

- The CBP Privacy Office is working with the Department and other Components to develop more specific coverage in the future, however DHS/ALL/PIA-056 and DHS/CBP/PIA-010(a) cover all aspects of this effort, including the collection and use of social media.

Applicable System of Records Notice(s) (SORN):

The CBP Privacy Office finds that SORN coverage for this effort is provided by DHS/CBP-024 Intelligence Records System (CIRS) System of Records, September 21, 2017, 82 FR 44198, which describes CBP's collection, maintenance, and use of records in order to identify, apprehend, or prosecute individuals who pose a potential law enforcement or security risk; aid in the enforcement of the customs and immigration laws, and other laws enforced by DHS at the border; and enhance U.S. border security.



DHS OPERATIONAL USE OF SOCIAL MEDIA

SPECIFIC QUESTIONS

1. Describe the category of use for collecting personally identifiable information from social media sources. Examples include: law enforcement intelligence, criminal investigations, background investigations, administrative investigations, professional responsibility investigations, benefit or employment determinations, or situational awareness. If use does not fit into one of these categories, please describe in full below. If your component has multiple categories of use, please submit separate template for each category.

This SMOUT addresses the operational use of social media in support of the protection and cybersecurity of CBP information systems and networks. The personnel using social media under this SMOUT are Cyber Threat Analysts employed in CBP's Cyber Threat Intelligence (CTI) team in the Office of Information and Technology (OIT), Cybersecurity Directorate, Security Operations Division. (b) (7)(E)

(b) (7)(E)

CTI's mission statement is to "enhance the cybersecurity posture of CBP information systems and networks through the aggregation, correlation, and dissemination of intelligence and information on cyberspace threats."

- **Aggregation and Correlation:** The primary role of the operational use of social media is to enable CTI team to identify and collect information on cyberspace threats either currently impacting CBP's information technology environment or with the potential to impact that environment. When a threat is identified, the CTI team

(b) (7)(E)

- In some cases, the CTI team will receive information from the CBP Security Operations Center that CBP was affected by specific cyber threat activity (e.g., phishing emails targeting CBP employees, malware on employee workstations, reconnaissance activities against CBP's network). In other cases, the CTI team will receive or identify a report, article, blog, or other open source information suggesting that a cyber-threat actor is conducting malicious activity against U.S. Government or



other relevant entity. And in other cases, the CTI team will receive an alert related to a suspicious website related to CBP that warrants further investigation using a secured Internet browsing capability. Regardless of the situation, the CTI team will

(b) (7)(E)

NOTE: The sole purpose of the CTI team maintaining access to social media is to view the publicly-available posts in the event that such posts contain information related to cyber threat activity; not to engage with individuals on social media. In addition,

(b) (7)(E)

- **Storage:** Once the CTI team identifies specific information of interest, the team will typically either save a screenshot of the resulting website or create a PDF copy of the resulting website, including social media posts. Typically, CTI will save the file to their workstation and upload the file to an internal, restricted-access SharePoint website on CBPNet that contains CTI's investigation information. The information posted on the website is restricted to personnel within the Cybersecurity Directorate with a need-to-know (i.e., the CTI team, CBP Security Operations Center personnel, Security Operations Division leadership, and the Chief Information Security Officer). The purpose of uploading this information to the site is to ensure that it is available to all CTI and other cybersecurity analysts during ongoing investigation activities. In addition, the site also provides a historical record in the event that the CTI team must conduct retroactive analysis of the related investigation. The information is stored subject to the applicable records retention policies.

Dissemination: Other than the SharePoint site, the dissemination of information gathered will almost always be limited to email communications. The vast majority of information gathered and shared is between the CTI team and the CBP Security Operations Center personnel. It is also possible that the CTI team would share information outside of CBP or DHS, such as the FBI or other U.S. Government



Departments or Agencies with cyber threat intelligence and/or cybersecurity missions. The CTI team will be required to mark the information with proper handling instructions before sharing, whether inside or outside of DHS. The CTI team understands the need-to-know concept, and ensures that operational information related to ongoing investigations is retained for the duration of that investigation.

2. Based on the operational use of social media listed above, please provide the appropriate authorities.
- Homeland Security Act of 2002, as amended, 6 U.S.C. § 101, et seq.
 - Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551, et seq.
 - DHS Directive 110-01, Privacy Policy for Operational Use of Social Media (June 8, 2012), and Instruction 110-01-001, Privacy Policy for Operational Use of Social Media (June 8, 2012)
 - CBP Directive No. 5410-003, Operational Use of Social Media (January 2, 2015)
 -

(b) (5)

3. Is this use of social media in development or operational?
- ☒ In development. ☐ Operational. Date first launched:
4. Please attach a copy of the Rules of Behavior that outline the requirements below.
5. Please describe the Rules of Behavior in effect for the listed operational use of social media. If users do NOT follow a particular Rule, please detail reasoning for not following that Rule:
- a) *Equipment.* Use only government-issued equipment when engaging in the operational use of social media;
- ☒ Yes. ☐ No. If not, please explain:
- b) *Email and accounts.* Use online screen names or identities that indicate an official DHS affiliation and use DHS email addresses to open accounts used when engaging in social media in the performance of their duties;



(b) (7)(E)

- c) *Public interaction.* Access publicly available information through social media only by reviewing posted information without interacting with any individual who posted the information;

(b) (7)(E)

- d) *Privacy settings.* Respect individuals' privacy settings and access only information that is publicly available;

(b) (7)(E)

- e) *PII collection:* Collect the minimum PII necessary for the proper performance of their authorized duties except for systems subject to Final Rules for Exemption from certain aspects of the Privacy Act;

☒ Yes. ☐ No. If not, please explain:

- f) *PII safeguards.* Protect PII as required by the Privacy Act (if applicable) and DHS privacy policy;

☒ Yes. ☐ No. If not, please explain:

- g) *Documentation.* Document operational use of social media, including date, site(s) accessed, information collected and how it was used in the same manner as the component would document information collected from any source in the normal course of business.

☒ Yes. ☐ No. If not, please explain:

- h) *Training.* Users complete annual privacy training which has been approved by Component Privacy Officer (or Privacy Point of Contact) based upon training materials provided by the DHS Privacy Office. Training must include, at minimum: legal authorities, acceptable operational uses of social media, access requirements, and requirements for documenting operational uses of social media.

☒ Yes. ☐ No. If not, please explain:

Mechanisms are (or will be) in place to verify that users have completed training.

☒ Yes, employees self-certify that they have read and understood their Component Rules of Behavior.



Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202 (b) (7)(E)@dhs.gov
www.dhs.gov/privacy

Version date: July 24, 2012
Page 8 of
10

☒ Yes, Component Privacy Officers or PPOCs maintain a record of employee attendance at privacy training that includes training on the Rules of Behavior.

☐ No. If not, please explain:



DHS SOCIAL MEDIA DOCUMENTATION

(To be Completed by the DHS Privacy Office)

DATE reviewed by the DHS Privacy Office: 04/26/2019

NAME of the DHS Privacy Office Reviewer: (b) (6), (b) (7)(C)

DHS Privacy Office Determination

☒ Program has met requirements to use social media for the stated authorized operational purposes, and must continue compliance with the requirements above.

☐ Program has not yet met requirements to utilize social media for operational purposes.

☐ Program authorities do not authorize operational use of social media.

☐ Rules of Behavior do not comply. <Please explain analysis.>

☐ Training required.

Additional Privacy compliance documentation is required:

☐ A PIA is required.

☒ Covered by existing PIA. DHS/ALL/PIA-056 DHS and Component Network IT Security Operations and Privacy and IT Security Incident Response; DHS/CBP/PIA-010(a) Analytical Framework for Intelligence

☐ New.

☐ Updated. <Please include the name and number of PIA to be updated here.>

☒ A SORN is required:

☒ Covered by existing SORN. DHS/CBP/PIA-010(a) Analytical Framework for Intelligence

☐ New.

☐ Updated. <Please include the name and number of SORN to be updated here.>

DHS PRIVACY OFFICE COMMENTS



CBP is submitting this PTA to discuss OIT use of social media in support of protection and cybersecurity of CBP information systems and networks. (b) (7)(E)

(b) (7)(E)
(b) (7)(E)

If OIT identifies an issue of concern in which PII of an individual that posted it is not necessary, the PII will be redacted from any notifications or products that are produced or stored. If PII is deemed relevant, the notifications and work products containing the PII will be retained in AFI.

The DHS Privacy Office finds this is a privacy sensitive use of social media, and requires PIA coverage. Coverage for instances where CBP would identify an issue of concern on social media in which PII is not relevant or necessary is provided by DHS/ALL/PIA-056 DHS and Component Network IT Security Operations and Privacy and IT Security Incident Response, which outlines the Department's efforts to protect the confidentiality, integrity, and availability of DHS information and information assets. In the event that PII is relevant and would be included in notifications and work products, coverage is provided by DHS/CBP/PIA-010(a) Analytical Framework for Intelligence, which discusses information collected as part of CBP's efforts to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk, and aids in the enforcement of customs, immigration, and other laws enforced by DHS.

SORN coverage is also required, and is provided by DHS/CBP-024 CIRS, which covers information collected to identify, apprehend, or prosecute individuals who pose a potential law enforcement or security risk.

DHS OPERATIONAL USE OF SOCIAL MEDIA

This template is used to assess the Department's Operational Use of Social Media, consistent with Management Directive 110-01.

The DHS Privacy Office has created this template to determine privacy compliance with Management Directive 110-01, *Privacy Policy for Operational Use of Social Media*. For the purposes of the Management Directive and this template, "Operational Use" means authorized use of social media to collect personally identifiable information for the purpose of enhancing situational awareness, investigating an individual in a criminal, civil, or administrative context, making a benefit determination about a person, making a personnel determination about a Department employee, making a suitability determination about a prospective Department employee, or for any other official Department purpose that has the potential to affect the rights, privileges, or benefits of an individual. Operational use does not include the use of search engines for general Internet research, nor does it include the use of social media for professional development such as training and continuing education or for facilitating internal meetings. The following uses of social media are exempt from the Management Directive and are not subject to this requirement¹:

- a) Communications and outreach with the public authorized by the Office of Public Affairs (covered by the existing PIAs: [DHS/ALL/PIA-031 - Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue](#) and [DHS/ALL/PIA-036 - Use of Unidirectional Social Media Applications](#));
- b) The conduct of authorized intelligence activities carried out by the Office of Intelligence and Analysis, the intelligence and counterintelligence elements of the United States Coast Guard, or any other Component performing authorized foreign intelligence or counterintelligence functions, in accordance with the provisions of Executive Order 12333, as amended.

This template shall be used to document the process to be followed by all programs engaging in operational uses of social media; to identify information technology systems, technologies, rulemakings, programs, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer; and to assess whether there is a need for additional Privacy Compliance Documentation. Components may appeal to the Deputy Secretary for Homeland Security if there is disagreement over the DHS Privacy Office determination of privacy compliance for the operational use of social media.

¹Gathering information by the Office of Operations Coordination and Planning (OPS) to enhance situational awareness is exempt from this requirement and is covered by the existing PIA: [DHS/OPS/PIA-004\(d\) - Publicly Available Social Media Monitoring and Situational Awareness Initiative Update](#).

DHS OPERATIONAL USE OF SOCIAL MEDIA

Please complete this form and send it to your Component Privacy Officer.
Upon receipt, your Component Privacy Officer and the DHS Privacy Office will review this form and may request additional information.

SUMMARY INFORMATION

Date submitted for review: 07/19/2017

Name of Component: U.S. Customs and Border Protection

Contact Information: (b) (6), (b) (7)(C) Senior Special Agent, (b) (6), (b) (7)(C)

Counsel²Contact Information: (b) (6), (b) (7)(C) Associate Chief Counsel, Enforcement and Operations

IT System(s) where social media data is stored:

- Joint Integrity Case Management System (JICMS),

Applicable Privacy Impact Assessment(s) (PIA):

- DHS/CBP/PIA-044, [Joint Integrity Case Management System \(JICMS\)](#), July 18, 2017

Applicable System of Records Notice(s) (SORN):

- [DHS/ALL-020 - Department of Homeland Security Internal Affairs](#), April 28, 2014, 79 FR 23361

²Counsel listed here must certify that appropriate authority exists to engage in particular operational activities involving social media.

DHS OPERATIONAL USE OF SOCIAL MEDIA

SPECIFIC QUESTIONS

1. Describe the category of use for collecting personally identifiable information from social media sources. Examples include: law enforcement intelligence, criminal investigations, background investigations, administrative investigations, professional responsibility investigations, benefit or employment determinations, or situational awareness. If use does not fit into one of these categories, please describe in full below. If your component has multiple categories of use, please submit separate template for each category.

This SMOUT addresses the operational use of social media for administrative investigations in a professional responsibility context. The personnel anticipated to use social media under this SMOUT are assigned to the Office of Professional Responsibility (OPR) Investigative Operations Division (IOD). All allegations against CBP employees are entered through the Joint Intake Center (JIC) process. The CBP OPR JIC and IOD vet the allegations to determine whether any allegation of corruption or misconduct rise to the level of criminal activity. If an allegation is determined to rise to the level of criminal activity, the investigation will proceed under the CBP OPR SMOUT for criminal investigations. If an allegation does not rise to the level of criminal activity, or if a prosecutor determines that a case cannot viably be criminally prosecuted, then OPR IOD will treat it as an administrative investigation. OPR IOD conducts administrative investigations for employee misconduct (improper fraternization, neglect of duty, mismanagement, etc.) in order to ensure compliance with CBP rules and prevent against corruption. In the process of these investigations OPR IOD will use the internet, including social media, to investigate, gather evidence, and gather information on activities by CBP employees or contractors that is pertinent to allegations of misconduct by an employee or contractor. (b) (7)(E)

OPR IOD will not be involved in the gratuitous gathering of personal social media information or PII. OPR IOD's focus is solely on identifying information that is germane to either proving or disproving allegations of misconduct. All OPR IOD investigations are predicated on specific allegations or articulable facts that are prima facie indicators of misconduct.

Once an individual is the subject of an investigation, OPR IOD will use the Internet, including social media as defined in DHS Instruction 110-01-001, Privacy Policy for the Operational Use of Social Media (Privacy Policy), for administrative investigations in a professional responsibility context that do not rise to the level of criminal misconduct or where prosecution is declined to gather evidence and relevant information related to misconduct. (b) (7)(E)

(b) (7)(E)

The information is stored in the Joint Integrity Case Management System (JICMS), which is covered under the DHS/ALL-20- Internal Affairs SORN and the JICMS PIA.

This use of the Internet, including social media, involves activities to gather information pertinent to allegations of misconduct by an employee or contractor, such as (b) (7)(E)

(b) (7)(E) This information is gathered and used by CBP OPR IOD personnel in the same manner as information gathered from non-Internet and non-social media sources such as information gathered in person, on the phone, or through

research of hard copy documents. Information gathered in this fashion may be used in administrative investigations of employees or contractors of CBP.

2. Based on the operational use of social media listed above, please provide the appropriate authorities.

- Homeland Security Act of 2002 § 411(c) & (j), Pub. L. No. 107-296, 116 Stat. 2135 (2002) as amended by section 802 of the Trade Enforcement and Trade Facilitation Act of 2015, Pub. L. No. 114-25 (2016) (codified at 6 U.S.C. § 211(c) & (j))
- Inspector General Act of 1978, Pub. L. 95-452, 92 Stat. 1101 (1978), as amended (codified at 5 U.S.C. App.)
- DHS Delegation No. 7010.3, Delegation of Authority to the Commissioner of U.S. Customs and Border Protection
- DHS Management Directive 0810.1, The Office of Inspector General
- CBP Directive No. 2130-016, Roles and Responsibilities for Internal Affairs Activities and Functions (December 23, 2008)

(b) (5)

3. Is this use of social media in development or operational?

☐ In development. ☒ Operational. Date first launched: July 18, 2017

4. Please attach a copy of the Rules of Behavior that outline the requirements below.

Attached. Also attached is the CBP Directive for Operational Use of Social Media, Section 5

5. Please describe the Rules of Behavior in effect for the listed operational use of social media. If users do NOT follow a particular Rule, please detail reasoning for not following that Rule:

- a) *Equipment.* Use only government-issued equipment when engaging in the operational use of social media;

☒ Yes. ☐ No. If not, please explain:

- b) *Email and accounts.* Use online screen names or identities that indicate an official DHS affiliation and use DHS email addresses to open accounts used when engaging in social media in the performance of their duties;

(b) (7)(E)

(b) (7)(E)

- c) *Public interaction.* Access publicly available information through social media only by reviewing posted information without interacting with any individual who posted the information;

(b) (7)(E)

- d) *Privacy settings.* Respect individuals' privacy settings and access only information that is publicly available;

(b) (7)(E)

- e) *PII collection:* Collect the minimum PII necessary for the proper performance of their authorized duties except for systems subject to Final Rules for Exemption from certain aspects of the Privacy Act;

☒ Yes. ☐ No. If not, please explain:

- f) *PII safeguards.* Protect PII as required by the Privacy Act (if applicable) and DHS privacy policy;

☒ Yes. ☐ No. If not, please explain:

- g) *Documentation.* Document operational use of social media, including date, site(s) accessed, information collected and how it was used.

☒ Yes. ☐ No. If not, please explain:

- h) *Training.* Users complete annual privacy training which has been approved by Component Privacy Officer (or Privacy Point of Contact) based upon training materials provided by the DHS Privacy Office. Training must include, at minimum: legal authorities, acceptable operational uses of social media, access requirements, and requirements for documenting operational uses of social media.

☒ Yes. ☐ No. If not, please explain:

Mechanisms are (or will be) in place to verify that users have completed training.

☒ Yes, employees self-certify that they have read and understood their Component Rules of Behavior.

☒ Yes, Component Privacy Officers or PPOCs maintain a record of employee attendance at privacy training that includes training on the Rules of Behavior.

☐ No. If not, please explain:

H
S

DHS SOCIAL MEDIA DOCUMENTATION

(To be Completed by the DHS Privacy Office)

DATE reviewed by the DHS Privacy Office: 2/12/2018

NAME of the DHS Privacy Office Reviewer (b) (6), (b) (7)(C)

DESIGNATION

This program is covered by the following Privacy Impact Assessment and Privacy Act System of Records Notice:

PIA: DHS/CBP/PIA-044 Joint Integrity Case Management System (JICMS)

SORN: DHS/ALL-020 Department of Homeland Security Internal Affairs, April 28, 2014, 79 FR 23361

1. Category of Use:

- ☐ Law Enforcement Intelligence;
- ☐ Criminal law enforcement investigations;
- ☐ Background investigations;
- ☒ Professional responsibility investigations;
- ☒ Administrative or benefit determinations (including fraud detection);
- ☐ Situational awareness; and
- ☐ Other. <Please explain "other" category of use here.>

(b) (5)

3. Rules of Behavior Content: (Check all items that apply.)

a. Equipment.

(b) (7)(E) Users must use government-issued equipment. Equipment may be non-attributable and may not resolve back to DHS/US IP address.

(b) (7)(E) Users must use government-issued equipment. Equipment must resolve back to DHS/US IP address.

b. Email and accounts.

USCBP000102

(b) (7)(E) Users do not have to use government email addresses or official DHS accounts online.

(b) (7)(E) Users must use government email addresses or official DHS accounts online.

c. *Public interaction.*

(b) (7)(E) Users may interact with individuals online in relation to a specific law enforcement investigation.

(b) (7)(E) Users may NOT interact with individuals online.

d. *Privacy settings.*

☐ Users may disregard privacy settings.

☒ Users must respect individual privacy settings.

e. *PII storage:*

☒ PII is maintained in an exempted Privacy Act System of Records.

Please list applicable SORN here: DHS/ALL-020 Department of Homeland Security Internal Affairs, April 28, 2014, 79 FR 23361

☐ PII is maintained in a Privacy Act Systems of Records.

Please list applicable SORN here:

f. *PII safeguards.*

☒ PII is protected as required by the Privacy Act and DHS privacy policy.

☐ Only a minimal amount of PII is collected and safeguarded, consistent with [DHS/OPS-004 – Publicly Available Social Media Monitoring and Situational Awareness Initiative](#).

g. *Documentation.*

☒ Users must appropriately document their use of social media, and collection of information from social media website.

☐ Documentation is not expressly required.

h. *Training.*

☒ All users must complete annual privacy training that has been approved by Component Privacy Officer. Training includes:

☒ Legal authorities;

☒ Acceptable operational uses of social media;

☒ Access requirements;

☒ Applicable Rules of Behavior; and

☒ Requirements for documenting operational uses of social media.

☒ Mechanisms are (or will be) in place to verify that users have completed training.

☒ Yes, employees self-certify that they have read and understood their Component Rules of Behavior.

☒ Yes, Component Privacy Officers or PPOCs maintain a record of employee attendance at privacy training that includes training on the Rules of Behavior.

☐ No, certification of training completion cannot be verified.

DHS Privacy Office Determination

☒ Program has met requirements to use social media for the stated authorized operational purposes, and must continue compliance with the requirements above.

☐ Program has not yet met requirements to utilize social media for operational purposes.

☐ Program

a ational use of social media.

u

t

h

o

r

i

t

i

e

s

d

o

n

o

t

a

u

t

h

o

r

i

z

e

o

p

e

r

☐ Rules of Behavior do not comply. <Please explain analysis.>

☐ Training required.

Additional Privacy compliance documentation is required:

☒ A PIA is required.

☒ Covered by existing PIA. DHS/CBP/PIA-044 Joint Integrity Case Management System (JICMS)

☐ New.

☐ Updated. <Please include the name and number of PIA to be updated here.>

☒ A SORN is required:

☒ Covered by existing SORN. DHS/ALL-020 Department of Homeland Security Internal Affairs, April 28, 2014, 79 FR 23361

☐ New.

☐ Updated. <Please include the name and number of SORN to be updated here.>

DHS PRIVACY OFFICE COMMENTS

CBP is submitting this SMOUT to discuss the operational use of social media for administrative investigations in a professional responsibility context. Office of Professional Responsibility (OPR) Investigative Operations Division (IOD) personnel will use social media to investigate allegations against CBP employees to vet the allegations to determine whether any allegation of corruption or misconduct rise to the level of criminal activity. If an allegation does not rise to the level of criminal activity, or if a prosecutor determines that a case cannot viably be criminally prosecuted, then OPR IOD will treat it as an administrative investigation. OPR IOD conducts administrative investigations for employee misconduct (improper fraternization, neglect of duty, mismanagement, etc.) in order to ensure compliance with CBP rules and prevent against corruption.

CBP OPR IOD will use social media to gather evidence directly relevant to the activity that predicates its investigation. OPR IOD will not gather PII that is not relevant to the investigation pursuant to OPR IOD investigation training standards and guidelines, the CBP Directive for Operational Use of Social Media, the CBP Rules of Behavior, and the DHS Privacy Policy for the Operational Use of Social Media. OPR IOD's focus is solely on identifying information that is germane to either proving or disproving allegations of administrative violations or misconduct. (b) (7)(E)

(b) (7)(E)

The information is stored in the Joint Integrity Case Management System (JICMS).

While some investigations are clearly administrative, some criminal investigations may become administrative in nature. Once a prosecuting authority declines prosecution of an investigation, it may become an administrative matter. This change in the character of the investigation is a function of prosecutorial discretion, and not an arbitrary decision on the part of OPR.

The DHS Privacy Office finds that CBP's operational use of social media for internal affairs administrative investigations purposes is consistent with their internal affairs investigatory authorities. PIA coverage is provided by DHS/CBP/PIA-044 Joint Integrity Case Management System (JICMS). SORN coverage is provided by DHS/ALL-020 Department of Homeland Security Internal Affairs.



DHS OPERATIONAL USE OF SOCIAL MEDIA

This template is used to assess the Department's Operational Use of Social Media, consistent with Management Directive 110-01.

The DHS Privacy Office has created this template to determine privacy compliance with Management Directive 110-01, *Privacy Policy for Operational Use of Social Media*. For the purposes of the Management Directive and this template, "Operational Use" means authorized use of social media to collect personally identifiable information for the purpose of enhancing situational awareness, investigating an individual in a criminal, civil, or administrative context, making a benefit determination about a person, making a personnel determination about a Department employee, making a suitability determination about a prospective Department employee, or for any other official Department purpose that has the potential to affect the rights, privileges, or benefits of an individual. Operational use does not include the use of search engines for general Internet research, nor does it include the use of social media for professional development such as training and continuing education or for facilitating internal meetings. The following uses of social media are exempt from the Management Directive and are not subject to this requirement¹:

- a) Communications and outreach with the public authorized by the Office of Public Affairs (covered by the existing PIAs: [DHS/ALL/PIA-031 - Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue](#) and [DHS/ALL/PIA-036 - Use of Unidirectional Social Media Applications](#));
- b) The conduct of authorized intelligence activities carried out by the Office of Intelligence and Analysis, the intelligence and counterintelligence elements of the United States Coast Guard, or any other Component performing authorized foreign intelligence or counterintelligence functions, in accordance with the provisions of Executive Order 12333, as amended.

This template shall be used to document the process to be followed by all programs engaging in operational uses of social media; to identify information technology systems, technologies, rulemakings, programs, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer; and to assess whether there is a need for additional Privacy Compliance Documentation. Components may appeal to the Deputy Secretary for Homeland Security if there is disagreement over the DHS Privacy Office determination of privacy compliance for the operational use of social media.

¹ Gathering information by the Office of Operations Coordination and Planning (OPS) to enhance situational awareness is exempt from this requirement and is covered by the existing PIA: [DHS/OPS/PIA-004\(d\) - Publicly Available Social Media Monitoring and Situational Awareness Initiative Update](#).



DHS OPERATIONAL USE OF SOCIAL MEDIA

Please complete this form and send it to your Component Privacy Officer.
Upon receipt, your Component Privacy Officer and the DHS Privacy Office will review this form and may request additional information.

SUMMARY INFORMATION

Date submitted for review: 6/12/18

Name of Component: Customs and Border Protection

Contact Information: (b) (6), (b) (7)(C) International Trade Specialist, Office of Trade,
(b) (6), (b) (7)(C) International Trade Specialist, Office of Trade (b) (6), (b) (7)(C)
(b) (6), (b) (7)(C) International Trade Specialist, Office of Trade (b) (6), (b) (7)(C)
(b) (6), (b) (7)(C) International Trade Specialist, Office of Trade, (b) (6), (b) (7)(C) Management and
Program Analyst, Office of Trade (b) (6), (b) (7)(C)

Counsel² Contact Information: (b) (6), (b) (7)(C) Director Forced Labor Division (b) (6), (b) (7)(C)
(b) (6), (b) (7)(C)

IT System(s) where social media data is stored: Information will be stored in users shared drive

Applicable Privacy Impact Assessment(s) (PIA):

- The CBP Privacy Office finds that overarching PIA coverage for this effort is provided by the DHS/CBP/PIA-010(a) Analytical Framework for Intelligence, which outlines CBPs efforts to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk, and aids in the enforcement of customs, immigration, and other laws enforced by DHS. The CBP Privacy Office is working to develop more specific coverage in the future, however AFI covers all aspects of this effort, including the collection and use of social media.

Applicable System of Records Notice(s) (SORN):

- The CBP Privacy Office finds that SORN coverage for this effort is provided by DHS/CBP-017 – Analytical Framework for Intelligence System (June 7, 2012 77 FR 13813), which describes CBP's collection, maintenance, and use of records in order to identify, apprehend, and/or prosecute individuals who pose a potential law enforcement risk and aid in the enforcement of the customs laws.
- The CBP Privacy Office finds that SORN coverage for this effort is provided by DHS/CBP-001 Import Information System (July 26, 2016, 81 FR 48826), which describes

² Counsel listed here must certify that appropriate authority exists to engage in particular operational activities involving social media.



CBP's collection, maintenance, and use of records on all commercial goods imported into the United States, along with carrier, broker, importer, as well as other information that facilitates the flow of legitimate shipments, and assists DHS/CBP in securing U.S. borders and targeting illicit goods.

DHS OPERATIONAL USE OF SOCIAL MEDIA

SPECIFIC QUESTIONS

1. Describe the category of use for collecting personally identifiable information from social media sources. Examples include: law enforcement intelligence, criminal investigations, background investigations, administrative investigations, professional responsibility investigations, benefit or employment determinations, or situational awareness. If use does not fit into one of these categories, please describe in full below. If your component has multiple categories of use, please submit separate template for each category.

CBP is submitting this SMOUT to outline the Office of Trade, Forced Labor Division's (FLD) operational use of social media, including (b) (7)(E) capabilities to identify and support FLD cases. The Commissioner of CBP established the Forced Labor Division in 2018 to focus solely on developing forced labor enforcement cases. These cases are (b) (7)(E)

(b) (7)(E)

The cases are developed through open source searches (b) (7)(E)

(b) (7)(E)

FLD may take notes containing PII from the social media that is reviewed, but it will not be retrievable by a personal identifier. All notes would be stored in password protected files on a shared drive. Because FLD investigates entities, this information will be stored for the length of the investigation.

2. Based on the operational use of social media listed above, please provide the appropriate authorities.

Under the authority of 19 CFR § 12.42 Findings of Commissioner of Customs.

(a) If any port director or other principal Customs officer has reason to believe that any class of merchandise that is being, or is likely to be, imported into the United States is being produced, whether by mining, manufacture, or other means, in any foreign locality with the use of convict labor, forced labor, or indentured labor under penal sanctions, including forced child labor or indentured child labor under penal sanctions, so as to come within the purview of section 307, Tariff Act of 1930, he shall communicate his belief to the Commissioner of Customs. Every such communication shall contain or be accompanied by a statement of substantially the same information as is required in paragraph (b) of this



section, if in the possession of the port director or other officer or readily available to him. Also, under 19 U.S. Code § 1307 - Convict-made goods; importation prohibited. All goods, wares, articles, and merchandise mined, produced, or manufactured wholly or in part in any foreign country by convict labor or/and forced labor or/and indentured labor under penal sanctions shall not be entitled to entry at any of the ports of the United States, and the importation thereof is hereby prohibited, and the Secretary of the Treasury is authorized and directed to prescribe such regulations as may be necessary for the enforcement of this provision.

"Forced labor", as herein used, shall mean all work or service which is exacted from any person under the menace of any penalty for its nonperformance and for which the worker does not offer himself voluntarily. For purposes of this section, the term "forced labor or/and indentured labor" includes forced or indentured child labor.

(b) (5)

3. Is this use of social media in development or operational?

☒ In development. ☐ Operational. Date first launched:

4. Please attach a copy of the Rules of Behavior that outline the requirements below.

- See attached Rules of Behavior (RoB)

5. Please describe the Rules of Behavior in effect for the listed operational use of social media. If users do NOT follow a particular Rule, please detail reasoning for not following that Rule:

- a) *Equipment*. Use only government-issued equipment when engaging in the operational use of social media;

☒ Yes. ☐ No. If not, please explain:

- b) *Email and accounts*. Use online screen names or identities that indicate an official DHS affiliation and use DHS email addresses to open accounts used when engaging in social media in the performance of their duties;

(b) (7)(E)



(b) (7)(E)

- c) *Public interaction.* Access publicly available information through social media only by reviewing posted information without interacting with any individual who posted the information;

(b) (7)(E)

- d) *Privacy settings.* Respect individuals' privacy settings and access only information that is publicly available;

(b) (7)(E)

- e) *PII collection:* Collect the minimum PII necessary for the proper performance of their authorized duties except for systems subject to Final Rules for Exemption from certain aspects of the Privacy Act;

☒ Yes. ☐ No. If not, please explain:

- f) *PII safeguards.* Protect PII as required by the Privacy Act (if applicable) and DHS privacy policy;

☒ Yes. ☐ No. If not, please explain:

- g) *Documentation.* Document operational use of social media, including date, site(s) accessed, information collected and how it was used in the same manner as the component would document information collected from any source in the normal course of business.

☒ Yes. ☐ No. If not, please explain:

- h) *Training.* Users complete annual privacy training which has been approved by Component Privacy Officer (or Privacy Point of Contact) based upon training materials provided by the DHS Privacy Office. Training must include, at minimum: legal authorities, acceptable operational uses of social media, access requirements, and requirements for documenting operational uses of social media.

☒ Yes. ☐ No. If not, please explain:



Version date: July 24, 2012

Page 6 of 9

Mechanisms are (or will be) in place to verify that users have completed training.

☒ Yes, employees self-certify that they have read and understood their Component Rules of Behavior.

☒ Yes, Component Privacy Officers or PPOCs maintain a record of employee attendance at privacy training that includes training on the Rules of Behavior.

☐ No. If not, please explain:



DHS SOCIAL MEDIA DOCUMENTATION

(To be Completed by the DHS Privacy Office)

DATE reviewed by the DHS Privacy Office: 9/24/18

NAME of the DHS Privacy Office Reviewer: (b) (6), (b) (7)(C)

DHS Privacy Office Determination

- ☒ Program has met requirements to use social media for the stated authorized operational purposes, and must continue compliance with the requirements above.
- ☐ Program has not yet met requirements to utilize social media for operational purposes.
- ☐ Program authorities do not authorize operational use of social media.
 - ☐ Rules of Behavior do not comply. <Please explain analysis.>
 - ☐ Training required.

Additional Privacy compliance documentation is required:

- ☒ A PIA is required.
- ☒ Covered by existing PIA. DHS/CBP/PIA-010(a) Analytical Framework for Intelligence
 - ☐ New.
 - ☐ Updated. <Please include the name and number of PIA to be updated here.>
- ☒ A SORN is required:
- ☒ Covered by existing SORN. DHS/CBP-001 Import Information System, July 26, 2016, 81 FR 48826; DHS/CBP-017 Analytical Framework for Intelligence System, June 7, 2012, 77 FR 13813
 - ☐ New.
 - ☐ Updated. <Please include the name and number of SORN to be updated here.>

DHS PRIVACY OFFICE COMMENTS



CBP Office of Trade, Forced Labor Division's (FLD) is submitting this SMOUT to discuss the request for access to social media for certain instances to use (b) (7)(E)

(b) (7)(E)

CBP's definition of (b) (7)(E)

(b) (7)(E)

The cases are developed through open source searches to (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

Under no circumstance will DHS/CBP violate any social media privacy settings (b) (7)(E)

PIA coverage for this collection is provided by the DHS/CBP/PIA-010(a) Analytical Framework for Intelligence, which outlines CBPs efforts to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk, and aids in the enforcement of customs, immigration, and other laws enforced by DHS. The DHS Privacy Office agrees with CBP Privacy that they should work to develop more specific coverage in the future.

SORN coverage for collection, maintenance, and sharing of information by FLD is provided by DHS/CBP-017 Analytical Framework for Intelligence System (June 7, 2012 77 FR 13813), which describes CBP's collection, maintenance, and use of records in order to identify, apprehend, and/or prosecute individuals who pose a potential law enforcement risk and aid in the enforcement of the customs laws.



Homeland Security

The Privacy Office
U S Department of Homeland Security
Washington, DC 20528
202 (b) (7)(E) @dhs.gov
www.dhs.gov/privacy

Version date: July 24, 2012
Page 9 of 9

Additional SORN coverage is provided by DHS/CBP-001 Import Information System (July 26, 2016, 81 FR 48826), which describes CBP's collection, maintenance, and use of records on all commercial goods imported into the United States, along with carrier, broker, importer, as well as other information that facilitates the flow of legitimate shipments, and assists DHS/CBP in securing U.S. borders and targeting illicit goods.

DHS OPERATIONAL USE OF SOCIAL MEDIA

This template is used to assess the Department's Operational Use of Social Media, consistent with Management Directive 110-01.

The DHS Privacy Office has created this template to determine privacy compliance with Management Directive 110-01, *Privacy Policy for Operational Use of Social Media*. For the purposes of the Management Directive and this template, "Operational Use" means authorized use of social media to collect personally identifiable information for the purpose of enhancing situational awareness, investigating an individual in a criminal, civil, or administrative context, making a benefit determination about a person, making a personnel determination about a Department employee, making a suitability determination about a prospective Department employee, or for any other official Department purpose that has the potential to affect the rights, privileges, or benefits of an individual. Operational use does not include the use of search engines for general Internet research, nor does it include the use of social media for professional development such as training and continuing education or for facilitating internal meetings. The following uses of social media are exempt from the Management Directive and are not subject to this requirement¹:

- a) Communications and outreach with the public authorized by the Office of Public Affairs (covered by the existing PIAs: [DHS/ALL/PIA-031 - Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue](#) and [DHS/ALL/PIA-036 - Use of Unidirectional Social Media Applications](#));
- b) The conduct of authorized intelligence activities carried out by the Office of Intelligence and Analysis, the intelligence and counterintelligence elements of the United States Coast Guard, or any other Component performing authorized foreign intelligence or counterintelligence functions, in accordance with the provisions of Executive Order 12333, as amended.

This template shall be used to document the process to be followed by all programs engaging in operational uses of social media; to identify information technology systems, technologies, rulemakings, programs, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer; and to assess whether there is a need for additional Privacy Compliance Documentation. Components may appeal to the Deputy Secretary for Homeland Security if there is disagreement over the DHS Privacy Office determination of privacy compliance for the operational use of social media.

¹Gathering information by the Office of Operations Coordination and Planning (OPS) to enhance situational awareness is exempt from this requirement and is covered by the existing PIA: [DHS/OPS/PIA-004\(d\) - Publicly Available Social Media Monitoring and Situational Awareness Initiative Update](#).

DHS OPERATIONAL USE OF SOCIAL MEDIA

Please complete this form and send it to your Component Privacy Officer.
Upon receipt, your Component Privacy Officer and the DHS Privacy Office will review this form and may request additional information.

SUMMARY INFORMATION

Date submitted for review:

Name of Component: U.S. Customs and Border Protection

Contact Information: (b) (6), (b) (7)(C) Director, Personnel Security Division (b) (6), (b) (7)(C)

Counsel²Contact Information: (b) (6), (b) (7)(C) Associate Chief Counsel, Ethics, Labor & Employment

IT System(s) where social media data is stored:

- Integrated Security Management System (ISMS)

Applicable Privacy Impact Assessment(s) (PIA):

- DHS/ALL/PIA-038(c) [Integrated Security Management System \(ISMS\)](#), June 26, 2017
- Forthcoming Background Investigations PIA

Applicable System of Records Notice(s) (SORN):

- [DHS/ALL-023 - Department of Homeland Security Personnel Security Management](#), February 23, 2010, 75 FR 8088

²Counsel listed here must certify that appropriate authority exists to engage in particular operational activities involving social media.

DHS OPERATIONAL USE OF SOCIAL MEDIA

SPECIFIC QUESTIONS

1. Describe the category of use for collecting personally identifiable information from social media sources. Examples include: law enforcement intelligence, criminal investigations, background investigations, administrative investigations, professional responsibility investigations, benefit or employment determinations, or situational awareness. If use does not fit into one of these categories, please describe in full below. If your component has multiple categories of use, please submit separate template for each category.

This SMOUT addresses the operational use of social media during background investigations and adjudications for determining initial or continued suitability for employment, eligibility to occupy a national security position, eligibility for access to classified information, eligibility for unescorted access to DHS/CBP facilities, or access to DHS/CBP information technology systems. The personnel using social media under this SMOUT are Office of Professional Responsibility (OPR), Personnel Security Division (PSD), employees and persons contracted by OPR PSD to support the background investigation, periodic reinvestigation, and continuous evaluation process.

This SMOUT encompasses both

(b) (7)(E) _ _

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

In addition to sharing information with OPR IOD, OPR PSD may also share information with other entities as required by regulation.

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

will be stored in the Integrated Security Management System (ISMS), which is covered under the DHS/ALL-023 Department of Homeland Security Personnel Security Management SORN. OPR PSD is not involved in the gratuitous gathering of personal social media information or PII. In addition, OPR does not collect or store as evidence any social media information that is solely an exercise of rights protected by the First Amendment (b) (7)(E)

(b) (7)(E)

2. Based on the operational use of social media listed above, please provide the appropriate authorities.

- Executive Order (E.O.) 10450; E.O. 12968; E.O. 13467; E.O. 13488; E.O. 13764
- 5 CFR Parts 731, 732, 736, and 1400; 32 CFR Part 147
- Security Executive Agent Directive 4, National Security Adjudicative Guidelines
- Security Executive Agent Directive 5, Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications
- Director of Central Intelligence Directive 6/4
- DHS Delegation No. 12000, Delegation for Security Operations Within the Department of Homeland Security
- DHS Directive 110-01, Privacy Policy for Operational Use of Social Media (June 8, 2012), and Instruction 110-01-001, Privacy Policy for Operational Use of Social Media (June 8, 2012).
- CBP Directive No. 2130-016, Roles and Responsibilities for Internal Affairs Activities and Functions (December 23, 2008)
- CBP Directive No. 5410-003, Operational Use of Social Media (January 2, 2015)

(b) (5)

3. Is this use of social media in development or operational?

☒ In development. ☐ Operational.

4. Please attach a copy of the Rules of Behavior that outline the requirements below.

Attached. Also attached is the CBP Directive for Operational Use of Social Media.

5. Please describe the Rules of Behavior in effect for the listed operational use of social media. If users do NOT follow a particular Rule, please detail reasoning for not following that Rule:

(b) (7)(E)

- b) *Email and accounts.* Use online screen names or identities that indicate an official DHS affiliation and use DHS email addresses to open accounts used when engaging in social media in the performance of their duties;

(b) (7)(E)

- c) *Public interaction.* Access publicly available information through social media only by reviewing posted information without interacting with any individual who posted the information;

- d) (b) (7)(E) *Privacy settings.* Respect individuals' privacy settings and access only information that is publicly available;

(b) (7)(E)

- e) *PII collection:* Collect the minimum PII necessary for the proper performance of authorized duties except for systems subject to Final Rules for Exemption from certain aspects of the Privacy Act;

☒ Yes. ☐ No. If not, please explain:

- f) *PII safeguards.* Protect PII as required by the Privacy Act (if applicable) and DHS privacy policy;

☒ Yes. ☐ No. If not, please explain:

- g) *Documentation.* Document operational use of social media, including date, site(s) accessed, information collected and how it was used.

☒ Yes. ☐ No. If not, please explain:

- h) *Training.* Users complete annual privacy training which has been approved by Component Privacy Officer (or Privacy Point of Contact) based upon training materials provided by the DHS Privacy Office. Training must include, at minimum: legal authorities, acceptable operational uses of social media, access requirements, and requirements for documenting operational uses of social media.

☒ Yes. ☐ No. If not, please explain:

Mechanisms are (or will be) in place to verify that users have completed training.

☒ Yes, employees self-certify that they have read and understood their Component Rules of Behavior.

☒ Yes, Component Privacy Officers or PPOCs maintain a record of employee attendance at privacy training that includes training on the Rules of Behavior.

☐ No. If not, please explain:

DHS SOCIAL MEDIA DOCUMENTATION

(To be Completed by the DHS Privacy Office)

DATE reviewed by the DHS Privacy Office: 5/16/2018

NAME of the DHS Privacy Office Reviewer: (b) (6), (b) (7)(C)

DESIGNATION

This program is covered by the following Privacy Impact Assessment and Privacy Act System of Records Notice:

PIA: New CBP Background Investigations PIA

SORN: Update to DHS/ALL-023 Department of Homeland Security Personnel Security Management, February 23, 2010, 75 FR 8088

1. Category of Use:

- ☐ Law Enforcement Intelligence;
- ☐ Criminal law enforcement investigations;
- ☒ Background investigations;
- ☒ Professional responsibility investigations;
- ☐ Administrative or benefit determinations (including fraud detection);
- ☐ Situational awareness; and
- ☐ Other. <Please explain "other" category of use here.>

(b) (5)


3. Rules of Behavior Content: (Check all items that apply.)

a. *Equipment.*

(b) (7)(E)

b. *Email and accounts.*

(b) (7)(E)

A large black rectangular redaction box covering the content of section b.

c. *Public interaction.*

(b) (7)(E)

A large black rectangular redaction box covering the content of section c.

d. *Privacy settings.*

☐ Users may disregard privacy settings.

☒ Users must respect individual privacy settings.

e. *PII storage:*

☐ PII is maintained in an exempted Privacy Act System of Records.

Please list applicable SORN here:

☒ PII is maintained in a Privacy Act Systems of Records.

Please list applicable SORN here: DHS/ALL-023 Department of Homeland Security Personnel Security Management, February 23, 2010, 75 FR 8088 - SORN must be updated with social media information as a Category of Record.

f. *PII safeguards.*

☒ PII is protected as required by the Privacy Act and DHS privacy policy.

☐ Only a minimal amount of PII is collected and safeguarded, consistent with [DHS/OPS-004 – Publicly Available Social Media Monitoring and Situational Awareness Initiative](#).

g. *Documentation.*

☒ Users must appropriately document their use of social media, and collection of information from social media website.

☐ Documentation is not expressly required.

h. *Training.*

☒ All users must complete annual privacy training that has been approved by Component Privacy Officer. Training includes:

☒ Legal authorities;

☒ Acceptable operational uses of social media;

☒ Access requirements;

☒ Applicable Rules of Behavior; and

☒ Requirements for documenting operational uses of social media.

☒ Mechanisms are (or will be) in place to verify that users have completed training.

☒ Yes, employees self-certify that they have read and understood their Component Rules of Behavior.

☒ Yes, Component Privacy Officers or PPOCs maintain a record of employee attendance at privacy training that includes training on the Rules of Behavior.

☐ No, certification of training completion cannot be verified.

DHS Privacy Office Determination

☒ Program has met requirements to use social media for the stated authorized operational purposes, and must continue compliance with the requirements above.

☐ Program has not yet met requirements to utilize social media for operational purposes.

☐ Program authorities do not authorize operational use of social media.

☐ Rules of Behavior do not comply.<Please explain analysis.>

☐ Training required.

Additional Privacy compliance documentation is required:

☒ A PIA is required.

☒ New. CBP Background Investigations PIA

☐ Updated.

☒ A SORN is required:

☐ New.

☒ Updated. DHS/ALL-023 Department of Homeland Security Personnel Security Management, February 23, 2010, 75 FR 8088

DHS PRIVACY OFFICE COMMENTS

CBP Privacy is submitting this SMOUT to discuss the operational use of social media during background investigations and adjudications for determining initial or continued suitability for employment, eligibility to occupy a national security position, eligibility for access to classified information, eligibility for unescorted access to DHS/CBP facilities, or access to DHS/CBP information technology systems.

The personnel using social media under this SMOUT are Office of Professional Responsibility (OPR), Personnel Security Division (PSD), employees and persons contracted by OPR PSD to support the background investigation, periodic reinvestigation, and continuous evaluation process.

This SMOUT encompasses both (b) (7)(E), (b) (5) OPR PSD's use of social media for (b) (7)(E), (b) (5)

(b) (7)(E), (b) (5)

OPR PSD will use the (b) (7)(E), (b) (5)

(b) (7)(E), (b) (5)

The DHS Privacy Office finds that CBP's operational use of social media by OPR PSD is consistent with its background investigation responsibilities and authorities.

A new CBP Background Investigations PIA will be required to discuss the collection of social media information by OPR PSD to support the background investigation, periodic reinvestigation, and continuous evaluation process. SORN coverage is provided by the DHS/ALL-023 Department of Homeland Security Personnel Security Management SORN, which will need to be updated to include social media information as a Category of Records.

DHS OPERATIONAL USE OF SOCIAL MEDIA

This template is used to assess the Department's Operational Use of Social Media, consistent with Management Directive 110-01.

The DHS Privacy Office has created this template to determine privacy compliance with Management Directive 110-01, *Privacy Policy for Operational Use of Social Media*. For the purposes of the Management Directive and this template, "Operational Use" means authorized use of social media to collect personally identifiable information for the purpose of enhancing situational awareness, investigating an individual in a criminal, civil, or administrative context, making a benefit determination about a person, making a personnel determination about a Department employee, making a suitability determination about a prospective Department employee, or for any other official Department purpose that has the potential to affect the rights, privileges, or benefits of an individual. Operational use does not include the use of search engines for general Internet research, nor does it include the use of social media for professional development such as training and continuing education or for facilitating internal meetings. The following uses of social media are exempt from the Management Directive and are not subject to this requirement¹:

- a) Communications and outreach with the public authorized by the Office of Public Affairs (covered by the existing PIAs: [DHS/ALL/PIA-031 - Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue](#) and [DHS/ALL/PIA-036 - Use of Unidirectional Social Media Applications](#));
- b) The conduct of authorized intelligence activities carried out by the Office of Intelligence and Analysis, the intelligence and counterintelligence elements of the United States Coast Guard, or any other Component performing authorized foreign intelligence or counterintelligence functions, in accordance with the provisions of Executive Order 12333, as amended.

This template shall be used to document the process to be followed by all programs engaging in operational uses of social media; to identify information technology systems, technologies, rulemakings, programs, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer; and to assess whether there is a need for additional Privacy Compliance Documentation. Components may appeal to the Deputy Secretary for Homeland Security if there is disagreement over the DHS Privacy Office determination of privacy compliance for the operational use of social media.

¹Gathering information by the Office of Operations Coordination and Planning (OPS) to enhance situational awareness is exempt from this requirement and is covered by the existing PIA: [DHS/OPS/PIA-004\(d\) - Publicly Available Social Media Monitoring and Situational Awareness Initiative Update](#).

DHS OPERATIONAL USE OF SOCIAL MEDIA

Please complete this form and send it to your Component Privacy Officer.
Upon receipt, your Component Privacy Officer and the DHS Privacy Office will review this form and may request additional information.

SUMMARY INFORMATION

Date submitted for review: 07/19/2017

Name of Component: U.S. Customs and Border Protection

Contact Information: (b) (6), (b) (7)(C)

Counsel²Contact Information: (b) (6), (b) (7)(C) Associate Chief Counsel, Enforcement and Operations

IT System(s) where social media data is stored:

- Joint Integrity Case Management System (JICMS),

Applicable Privacy Impact Assessment(s) (PIA):

- DHS/CBP/PIA-044, [Joint Integrity Case Management System \(JICMS\)](#), July 18, 2017

Applicable System of Records Notice(s) (SORN):

- [DHS/ALL-020 - Department of Homeland Security Internal Affairs](#), April 28, 2014, 79 FR 23361

²Counsel listed here must certify that appropriate authority exists to engage in particular operational activities involving social media.

DHS OPERATIONAL USE OF SOCIAL MEDIA

SPECIFIC QUESTIONS

1. Describe the category of use for collecting personally identifiable information from social media sources. Examples include: law enforcement intelligence, criminal investigations, background investigations, administrative investigations, professional responsibility investigations, benefit or employment determinations, or situational awareness. If use does not fit into one of these categories, please describe in full below. If your component has multiple categories of use, please submit separate template for each category.

This SMOUT addresses the operational use of social media for criminal investigations in a professional responsibility context. The personnel anticipated to use social media under this SMOUT are assigned to the Office of Professional Responsibility (OPR) Investigative Operations Division (IOD). This SMOUT encompasses using (b) (7)(E)

(b) (7)(E) All allegations against CBP employees are entered through the Joint Intake Center (JIC) process. The CBP OPR JIC and IOD vet the allegations to determine whether any allegation of corruption or misconduct rise to the level of criminal activity. For those allegations determined to be criminal in nature, OPR requires the use of cutting edge investigative methodologies to collect evidence that may be unavailable through traditional investigative means. CBP OPR IOD investigators are aware that targets of criminal investigations may place information, (b) (7)(E)

(b) (7)(E) in publicly accessible/non-privacy restricted social media forums. This publicly accessible/non-privacy restricted information has the potential to serve as evidence germane to the criminal activity under investigation. (b) (7)(E)

(b) (7)(E) The evidentiary potential of this publicly accessible/non-privacy restricted social media information may be derogatory or mitigating, depending the investigation.

CBP OPR IOD will use social media to gather evidence directly relevant to the criminal activity that predicates their investigations. OPR IOD will not gather PII that is not relevant to the investigation pursuant to OPR IOD investigation training standards and guidelines, the CBP Directive for Operational Use of Social Media, the CBP Rules of Behavior, and the DHS Privacy Policy for the Operational Use of Social Media. OPR IOD's focus is solely on identifying information that is germane to either proving or disproving allegations of criminal violations or misconduct. All OPR IOD investigations are predicated on specific allegations or articulable facts that are prima facie indicators of misconduct or criminal violations.

Once an individual is the subject of an investigation, OPR IOD will use social media to gather evidence and relevant information related to the criminal conduct. (b) (7)(E)

(b) (7)(E)

(b) (7)(E). The information is stored in the Joint Integrity Case Management System (JICMS), which is covered under the DHS/ALL-20- Internal Affairs SORN and the JICMS PIA.

(Note: While some OPR IOD investigations are clearly administrative, based on a lack of correlation between activity and criminal statutes, some criminal investigations may become administrative in nature. Once a competent prosecuting authority (i.e., the U.S. Attorney's Office) declines prosecution of an investigation, it may become an administrative matter. This change in the character of the investigation is a function of prosecutorial discretion, and not an arbitrary decision on the part of OPR. Once prosecution of the matter is declined, OPR IOD will conduct any further investigation of the matter pursuant to the Office of Professional Responsibility Administrative Investigation SMOUT.

2. Based on the operational use of social media listed above, please provide the appropriate authorities.

- Homeland Security Act of 2002 § 411(c) & (j), Pub. L. No. 107-296, 116 Stat. 2135 (2002) as amended by section 802 of the Trade Enforcement and Trade Facilitation Act of 2015, Pub. L. No. 114-25 (2016) (codified at 6 U.S.C. § 211(c) & (j))
- 19 U.S.C. § 1589a, Enforcement authority of customs officers
- 8 U.S.C. § 1357, Powers of immigration officers and employees
- 8 C.F.R. § 287.2, Disposition of criminal cases
- DHS Delegation 7010.3, Delegation of Authority to the Commissioner of U.S. Customs and Border Protection
- Memorandum, Authorization to the Commissioner of CBP to Investigate Allegations of Criminal Misconduct by CBP Employees and to Convert CBP Internal Affairs GS-1801 Employees to GS-1811 Series to Conduct such Investigations (Aug. 29, 2014)
- CBP Directive No. 2130-016, Roles and Responsibilities for Internal Affairs Activities and Functions (December 23, 2008)
- CBP Office of Internal Affairs Order 14-001, Designation Order, Immigration Officer and Customs Officer Authority (Sept. 25, 2014)
- 8 C.F.R. § 2.1, Authority of the Secretary of Homeland Security

(b) (5)

3. Is this use of social media in development or operational?

☐ In development. ☒ Operational. Date first launched: July 18, 2017

4. Please attach a copy of the Rules of Behavior that outline the requirements below.

Attached. Also attached is the CBP Directive for Operational Use of Social Media, Section 5

5. Please describe the Rules of Behavior in effect for the listed operational use of social media. If users do NOT follow a particular Rule, please detail reasoning for not following that Rule:

- a) *Equipment.* Use only government-issued equipment when engaging in the operational use of social media;

(b) (7)(E)

- b) *Email and accounts.* Use online screen names or identities that indicate an official DHS affiliation and use DHS email addresses to open accounts used when engaging in social media in the performance of their duties;

(b) (7)(E)

- c) *Public interaction.* Access publicly available information through social media only by reviewing posted information without interacting with any individual who posted the information;

(b) (7)(E)

- d) *Privacy settings.* Respect individuals' privacy settings and access only information that is publicly available;

(b) (7)(E)

- e) *PII collection:* Collect the minimum PII necessary for the proper performance of their authorized duties except for systems subject to Final Rules for Exemption from certain aspects of the Privacy Act;

☒ Yes. ☐ No. If not, please explain:

- f) *PII safeguards.* Protect PII as required by the Privacy Act (if applicable) and DHS privacy policy;

☒ Yes. ☐ No. If not, please explain:

- g) Documentation.** Document operational use of social media, including date, site(s) accessed, information collected and how it was used.

☒ Yes. ☐ No. If not, please explain:

As described in Section 1, all documentation of the operational use of social media for OPR IOD's criminal investigations is done (and stored) within the individual JICMS case file. JICMS has privacy compliance coverage under the DHS/ALL-20- Internal Affairs SORN and the JICMS PIA (DHS/CBP/PIA-044).

- h) Training.** Users complete annual privacy training which has been approved by Component Privacy Officer (or Privacy Point of Contact) based upon training materials provided by the DHS Privacy Office. Training must include, at minimum: legal authorities, acceptable operational uses of social media, access requirements, and requirements for documenting operational uses of social media.

☒ Yes. ☐ No. If not, please explain:

Mechanisms are (or will be) in place to verify that users have completed training.

☒ Yes, employees self-certify that they have read and understood their Component Rules of Behavior.

☒ Yes, Component Privacy Officers or PPOCs maintain a record of employee attendance at privacy training that includes training on the Rules of Behavior.

☐ No. If not, please explain:

DHS SOCIAL MEDIA DOCUMENTATION

(To be Completed by the DHS Privacy Office)

DATE reviewed by the DHS Privacy Office: 2/21/2018

NAME of the DHS Privacy Office Reviewer (b) (6), (b) (7)(C)

DESIGNATION

This program is covered by the following Privacy Impact Assessment and Privacy Act System of Records Notice:

PIA: DHS/CBP/PIA-044 Joint Integrity Case Management System (JICMS)

SORN: DHS/ALL-020 Department of Homeland Security Internal Affairs, April 28, 2014, 79 FR 23361

1. Category of Use:

- ☐ Law Enforcement Intelligence;
- ☒ Criminal law enforcement investigations;
- ☐ Background investigations;
- ☒ Professional responsibility investigations;
- ☐ Administrative or benefit determinations (including fraud detection);
- ☐ Situational awareness; and
- ☐ Other. <Please explain "other" category of use here.>

(b) (5)

3. Rules of Behavior Content: (Check all items that apply.)

a. Equipment.

(b) (7)(E) Users must use government-issued equipment. Equipment may be non-attributable and may not resolve back to DHS/US IP address.

(b) (7)(E) Users must use government-issued equipment. Equipment must resolve back to DHS/US IP address.

b. Email and accounts.

(b) (7)(E) Users do not have to use government email addresses or official DHS accounts online.

(b) (7)(E) Users must use government email addresses or official DHS accounts online.

c. *Public interaction.*

(b) (7)(E) Users may interact with individuals online in relation to a specific law enforcement investigation.

(b) (7)(E) Users may NOT interact with individuals online.

d. *Privacy settings.*

☐ Users may disregard privacy settings.

☒ Users must respect individual privacy settings.

e. *PII storage:*

☒ PII is maintained in an exempted Privacy Act System of Records.

Please list applicable SORN here: DHS/ALL-020 Department of Homeland Security Internal Affairs, April 28, 2014, 79 FR 23361

☐ PII is maintained in a Privacy Act Systems of Records.

Please list applicable SORN here:

f. *PII safeguards.*

☒ PII is protected as required by the Privacy Act and DHS privacy policy.

☐ Only a minimal amount of PII is collected and safeguarded, consistent with [DHS/OPS-004 – Publicly Available Social Media Monitoring and Situational Awareness Initiative](#).

g. *Documentation.*

☒ Users must appropriately document their use of social media, and collection of information from social media website.

☐ Documentation is not expressly required.

h. *Training.*

☒ All users must complete annual privacy training that has been approved by Component Privacy Officer. Training includes:

☒ Legal authorities;

☒ Acceptable operational uses of social media;

☒ Access requirements;

☒ Applicable Rules of Behavior; and

☒ Requirements for documenting operational uses of social media.

☒ Mechanisms are (or will be) in place to verify that users have completed training.

☒ Yes, employees self-certify that they have read and understood their Component Rules of Behavior.

☒ Yes, Component Privacy Officers or PPOCs maintain a record of employee attendance at privacy training that includes training on the Rules of Behavior.

☐ No, certification of training completion cannot be verified.

DHS Privacy Office Determination

☒ Program has met requirements to use social media for the stated authorized operational purposes, and must continue compliance with the requirements above.

☐ Program has not yet met requirements to utilize social media for operational purposes.

☐ Program authorities do not authorize operational use of social media.

☐ Rules of Behavior do not comply. <Please explain analysis.>

☐ Training required.

Additional Privacy compliance documentation is required:

☒ A PIA is required.

☒ Covered by existing PIA. DHS/CBP/PIA-044 Joint Integrity Case Management System (JICMS)

☐ New.

☐ Updated. <Please include the name and number of PIA to be updated here.>

☒ A SORN is required:

☒ Covered by existing SORN. DHS/ALL-020 Department of Homeland Security Internal Affairs, April 28, 2014, 79 FR 23361

☐ New.

☐ Updated. <Please include the name and number of SORN to be updated here.>

DHS PRIVACY OFFICE COMMENTS:

CBP is submitting this SMOUT to discuss the operational use of social media for criminal investigations in a professional responsibility context. Office of Professional Responsibility (OPR) Investigative Operations Division (IOD) personnel will use social media to investigate allegations against CBP employees to vet the allegations to determine whether any allegation of corruption or misconduct rise to the level of criminal activity. CBP OPR IOD will use social media to gather evidence directly relevant to the criminal activity that predicates their investigations. OPR IOD will not gather PII that is not relevant to the investigation pursuant to OPR IOD investigation training standards and guidelines, the CBP Directive for Operational Use of Social Media, the CBP Rules of Behavior, and the DHS Privacy Policy for the Operational Use of Social Media. OPR IOD's focus is solely on identifying information that is germane to either proving or disproving allegations of criminal violations or misconduct.

(b) (7)(E)
(b) (7)(E)

The information

is stored in the Joint Integrity Case Management System (JICMS).

While investigations are clearly administrative, some criminal investigations may become administrative in nature. Once a prosecuting authority declines prosecution of an investigation, it may become an administrative matter. This change in the character of the investigation is a function of prosecutorial discretion, and not an arbitrary decision on the part of OPR. Once prosecution of the matter is declined, OPR IOD will conduct any further investigation of the matter pursuant to the Office of Professional Responsibility Administrative Investigation SMOUT.

The DHS Privacy Office finds that CBP's operational use of social media for internal affairs criminal investigations purposes is consistent with their internal affairs investigatory authorities. PIA coverage is provided by DHS/CBP/PIA-044 Joint Integrity Case Management System (JICMS). SORN coverage is provided by DHS/ALL-020 Department of Homeland Security Internal Affairs.