Exhibit K

Privacy Impact Assessment
for the

Publicly Available Social Media Monitoring and Situational Awareness Initiative

DHS/CBP/PIA-058

March 25, 2019

Contact Point
David Bates
Office of Intelligence
U.S. Customs and Border Protection
(202) 344-2548

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The U.S. Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) takes steps to ensure the safety of its facilities and personnel from natural disasters, threats of violence, and other harmful events and activities. In support of these efforts, designated CBP personnel monitor publicly available, open source social media to provide situational awareness and to monitor potential threats or dangers to CBP personnel and facility operators. Authorized CBP personnel may collect publicly available information posted on social media sites to create reports and disseminate information related to personnel and facility safety. CBP is conducting this Privacy Impact Assessment (PIA) because, as part of this initiative, CBP may incidentally collect, maintain, and disseminate personally identifiable information (PII) over the course of these activities.

Introduction

Certain CBP personnel are responsible for providing around-the-clock monitoring and reporting to the CBP Commissioner, facility operators, and field offices in order to provide situational awareness[1] that can be used to shape the agency's operational picture and facilitate decision making regarding threats to CBP facilities and employees. These CBP personnel may use publicly available information,[2] including information obtained from social media sites, to provide greater situational awareness and in turn greater security throughout CBP. As part of this initiative, CBP uses Internet-based platforms, as well as government and commercially developed tools that provide a variety of methods for monitoring social media sites.[3] Through the use of publicly available search engines and content aggregators,[4] CBP monitors content on social media sites for information that informs Agency situational awareness while respecting individual users' privacy

[1] *See* Section 515 of the Homeland Security Act (6 U.S.C. § 321d(b)(1)). The law defines the term "situational awareness" as "information gathered from a variety of sources that, when communicated to emergency managers and decision-makers, can form the basis for incident management decision-making and steady-state activity." 6 U.S.C. § 321d(a).

[2] For purposes of this PIA, the term "publicly available information" means unclassified information that has been published, posted, disseminated, broadcast, or otherwise made available to the general public, is available to a significant portion of the public, is available to any interested individual who opts to receive the information, is available to members of the public by subscription or purchase, could lawfully be seen or heard by a casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public.

[3] Social media, for the purposes of this PIA, means 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 take 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 Department intranets or applications.

[4] Content aggregators generally provide a consolidated view of web content in a single browser display or desktop application.

settings. Many of these tools use keywords to search across platforms and pull publicly available posts made in public forums that match those keywords. If necessary, CBP may create accounts on social media sites in order to view publicly available information. CBP employees then review the posts captured by the monitoring tools in order to determine whether they are relevant for situational awareness and threat monitoring. CBP also uses tools that allow for the creation of a geo-fence,[5] in which authorized CBP employees can view publicly available social media posts that contain certain words and are posted from certain locations, and are from users who have opted to make their location public. Generally, designated CBP employees will use information collected from publicly available social media postings that is deemed relevant to draft reports designed to shape the agency's situational awareness. CBP will generally redact PII in reports. However, there are certain instances, including when a posting is deemed threatening, when it may be necessary to include PII in a report. Unless otherwise authorized by law, CBP does not store or disseminate information related to First Amendment[6] protected speech or activities, unless those activities evolve into dangerous or threatening events impacting the operations or safety of CBP facilities and personnel.

Under this initiative, CBP will not: 1) post any information on social media sites; 2) connect or engage with other social media platform users; 3) accept invitations to connect; or 4) interact on social media sites. CBP is permitted by policy to establish user names and passwords to create profiles and follow relevant government, media, and subject matter experts on social media sites in order to use search tools under established criteria and search terms for monitoring that supports providing situational awareness.[7]

The majority of CBP personnel using social media for situational awareness will not collect, store, or disseminate PII. CBP primarily uses social media to monitor events that may impact the operational readiness or security of CBP facilities (such as natural disasters in the area of a Port of Entry or an active shooter near CBP headquarters). The collection and dissemination of PII is not necessary in order to report on these events. However, there may be times when reporting on PII collected from social media will provide a greater operating picture that will allow CBP to protect lives and facilities as well as to ensure efficient functioning of CBP field locations. For example, CBP officials working at Los Angeles International Airport may use social media to monitor postings and reporting related to nearby forest fires to determine if they will have an effect on the airport itself, or on local CBP personnel supporting operations. CBP could provide that

[5] A geo-fence is a virtual geographic boundary, defined by CBP personnel, that limits tools to search for information from inside or outside a designated area or location.
[6] 5 U.S.C. § 552a(e)(7) requires that agencies "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity."
[7] CBP Directive 5410-003 "Operational Use of Social Media" (Jan. 2, 2015); DHS Instruction 110-01-001 "Privacy Policy for Operational Use of Social Media" (June 8, 2012); DHS Directive 110-01 "Privacy Policy For Operational Use Of Social Media" (June 8, 2012).

information to employees warning them of potential dangers, and helping to manage potential impacts on staffing. Such situations may not involve an imminent loss of life but may impact operations. Awareness of these events enables the development of a better operating picture for CBP decision makers.

Given the unpredictable nature of disasters or other events, coupled with the voluntary and unrestricted nature of the content that people post, it is possible during *in extremis* situations for CBP to collect a limited amount of PII from the public through its monitoring of social media. An *in extremis* situation is one which there is an imminent threat of loss of life, serious bodily harm, or credible threats to facilities or systems. Any storage and dissemination of PII is limited to what is necessary to investigate an incident or threat, respond and provide assistance to an individual, or to ensure the safety of CBP personnel. For example, CBP may collect an individual's: name; social media user name, handle, or alias; address or approximate location; phone number, email address or other contact information that is made publicly available on social media; and when relevant, details that may relate to a potential active threat, such as for an active shooter. CBP may disseminate relevant information to the CBP Commissioner, CBP personnel, CBP facility operators, the National Targeting Center (NTC), the National Operations Center (NOC), and with other authorized authorities consistent with applicable laws and policies via email and other emergency notification mechanisms.[8]

Collection and Use of PII

As previously noted, CBP personnel who access publicly available social media for situational awareness purposes do not routinely store and disseminate PII. However, it may be necessary, particularly when social media is used to identify or monitor credible threats against CBP personnel, to both collect and use PII.[9] For example, CBP may create keyword lists that are processed by various tools to identify postings containing information related to threats against CBP employees. Keyword lists may be developed for high interest events (e.g., trials or conferences where there may be an increased threat risk). There may be cases in which PII may be included as keywords in order to identify the target or perpetrator of threats. This PII would be limited to biographic information on CBP employees and the names of individuals known to represent a threat or have been involved in events that could lead to credible threats. For example, a keyword may be the name and home address of CBP leadership. Posting the name and address

[8] In addition to being stored in Outlook, information used to create a finished intelligence product (such as an Officer Safety Alert) for publication in Analytical Framework for Intelligence (AFI). These finished intelligence products may include general intelligence information about potential threats that are not directed at specific individuals. For example, a threat of violence to agents at a specific office would go into AFI, whereas a threat to a specific agent at a specific office would be put into the Joint Integrity Case Management System (JICMS).

[9] A number of federal laws describe punishment for threats or offenses against federal personnel and their family members. *See, e.g.*, 18 U.S.C. §§ 115, 351, 1114.

of a specific individual may heighten the credibility of a threat by demonstrating a potential ability to carry it out.

First Amendment Protections

Prior to collecting information from social media, CBP employees will determine whether a posting is protected by the First Amendment to the U.S. Constitution[10] and whether the collection of information is permissible under the Privacy Act.[11] CBP personnel receive training to distinguish between First Amendment protected activities and credible threats. This training reinforces First Amendment protections and requires that CBP personnel use a balancing test when assessing whether or not speech is deemed a threat. CBP personnel gauge the weight of a First Amendment claim, the severity of the threat, and the credibility of the threat. For example, a threat to harm a CBP employee, without additional information, might be considered First Amendment protected speech. A threat that was accompanied by additional information that indicated the threat was actionable and credible (e.g., if the person posted pictures of a weapon and stated they were going to a specific CBP location to inflict harm), might be designated a credible threat and CBP would investigate further.

In addition, the Privacy Act generally prohibits the Agency collection of records describing how an individual (defined in the Act as a U.S. citizen or Lawful Permanent Resident) exercises rights guaranteed by the First Amendment.[12] There are exceptions, however, if the record is "pertinent to and within the scope of an authorized law enforcement activity," or if either a statute or the individual about whom the record is maintained expressly authorizes such maintenance.[13] CBP personnel receive social media training, where they are given instruction from the Office of Chief Counsel and the CBP Privacy and Diversity Office on how to identify First Amendment activity and determine if social media posts discuss protected activities, such as protests, or if they are credible threats for which CBP personnel should take action. CBP personnel manually review all posts identified by the tools employed as part of situational awareness activities to determine the accuracy of information and whether it is protected speech.[14]

---

[10] "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances." U.S. CONST. amend. I.

[11] 5 U.S.C. § 552a(e)(7).

[12] *Id.*

[13] *Id.*

[14] CBP will store and process collected information on a secure enclave operated under CBP Security Operations - Digital Guardian. DHS/ALL/PIA-056 DHS and Component Network IT Security Operations and Privacy and IT Security Incident Response provides PIA coverage; and DHS/ALL-020 DHS Internal Affairs, April 28, 2014, 79 FR 23361; and DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), November 27, 2012, 77 FR 70792 provide SORN coverage, *available at* www.dhs.gov/privacy.

Data Accuracy and Credible Threats

In order to determine accuracy, CBP personnel attempt to match information collected through Social Media against other CBP datasets. For example, if a person makes a threat, CBP may use CBP travel records to determine if the person is even in the United States and able to act on that threat. If the information that is evaluated contains a threat, it is reported through the Joint Integrity Case Management System (JICMS)[15] for possible referral for criminal investigation by CBP's Office of Professional Responsibility (OPR).[16]

Once entered into JICMS, OPR determines whether the activity involves criminal activity or warrants further investigation. Based on the threat information, OPR may generate Protective Intelligence, Threat Bulletins, or Travel Assessments[17] for distribution to CBP Protective Detail Personnel, CBP's Situation Room,[18] facility managers, the National Targeting Center (NTC), National Intelligence Watch, and the DHS National Operations Center (NOC) for dissemination to the respective wider CBP, Departmental, or other law enforcement audience. For direct threats to a named CBP individual, the reporting is restricted to official investigative and leadership channels.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the Federal Government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. The FIPPs account for the nature

---

[15] DHS/CBP/PIA-044 Joint Integrity Case Management System (JICMS) July 2017, *available at* https://www.dhs.gov/publication/dhscbppia-044-joint-integrity-case-management-system-jicms.

[16] Through the national headquarters in Washington, D.C., and strategically located regional field offices, OPR screens potential CBP employees for suitability; educates employees concerning ethical standards and integrity responsibilities; conducts inquiries into employee misconduct allegations; evaluates physical security threats to CBP employees, facilities, and sensitive information; and inspects CBP operations and processes for managerial effectiveness and improvements.

[17] Travel assessments are reports on threat activity in areas where CBP Commissioner is traveling and contains information on areas of concern.

[18] DHS/CBP/PIA-039 CBP Situation Room, March 2017, *available at* https://www.dhs.gov/publication/dhscbppia-039-cbp-situation-room.

and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002 Section 208 and the Homeland Security Act of 2002 Section 222. This PIA examines the privacy impact of the use of social media for situational awareness as it relates to the Fair Information Principles.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.

This PIA functions as the primary form of notice to individuals that CBP monitors publicly available social media. CBP may publicize its use of social media to respond to disasters or other *in extremis* events. CBP does not, however, individually provide notice when collecting publicly available information from specific users who voluntarily post information on publicly accessible social media sites. Authorized CBP employees may retrieve public information from the social media sites, but do not interact with individual users. CBP's use of social media to enhance its ability to identify, apprehend, or prosecute individuals who pose a law enforcement or security risk as discussed in the CBP Intelligence Records System SORN.[19] Some CBP personnel, consistent with CBP policy and procedures,[20] may conceal their identity when viewing social media for operational security purposes.

Privacy Risk: There is a risk that individuals whose data is collected by CBP while using social media for situational awareness will not receive notice prior to the collection.

Mitigation: This risk is partially mitigated. While CBP does not provide individual social media users notice prior to viewing or collecting publicly available information, CBP only collects information that users have proactively contributed to publicly available websites. Users that post content to publicly available social media platforms make that information available to the all members of the public, including law enforcement. CBP provides notice of its collection of publicly available social media information for situational awareness via this PIA, as well as through the publication of SORNs for the relevant systems where such information is stored.

[19] *See* DHS/CBP-024 Intelligence Records System (CIRS) System of Records, 82 Fed. Reg. 44198 (Sept. 21, 2017).
[20] CBP Directive 5410-003 "Operational Use of Social Media" (Jan. 2, 2015).

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

Individuals voluntarily post publicly available information on social media sites or otherwise make information publicly available online, in the same way that they make information available in any kind of public forum. Individuals retain the right and ability to refrain from making information public or, in most cases, to remove previously posted information from their respective social media accounts. In addition, individual users of social media may use the sites' privacy settings to choose to keep private or limit the availability of the information they share through their respective accounts. In many cases this information is voluntarily generated and individuals make the decision when to post or not post information.

Privacy Risk: There is a risk that individuals may be unaware that someone has publicly posted information about them that may be available to CBP for situational awareness purposes.

Mitigation: This risk is partially mitigated. This PIA provides notice to everyone that CBP is viewing social media for situational awareness, as well as to monitor for credible threats. As part of this initiative, CBP only collects information that is publicly available; however, CBP does not have the ability to determine if a user received consent to publicly post information about someone else.

Privacy Risk: There is a risk that individuals may not be aware that their posts are public and CBP may view and collect information from their posts.

Mitigation: CBP is unable to mitigate this risk. The privacy policy and terms of service of social media sites inform users that information they post is publicly accessible. Many sites offer users the ability to change their privacy settings and control who can see what they post.

Privacy Risk: There is a risk that users will be unable to correct information already collected by CBP.

Mitigation: This risk is partially mitigated. The tools CBP uses continuously monitor social media sites. This means that if a post is made in error and then later corrected or deleted, the social media aggregation tools and CBP personnel would correct CBP's records. CBP would then be able to edit any information that is stored and disseminated. However, it is possible that the tools will miss some corrections and CBP will not be able to make edits to the information. Due to the real-time nature of social media monitoring, CBP tries to confirm all information it receives with information found across various platforms from various users. For the majority of information stored and disseminated, CBP only stores content of posts and not the handle of the

poster, reducing the potential for harm posed by inaccurate information. Whenever possible, CBP limits the amount of PII to include only the information necessary for the usefulness of the report. CBP personnel update or correct any reports they create once they become aware of errors or if the operational security scenarios of the situation change.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and the purpose or purposes for which the PII is intended to be used.

CBP's general authority for this initiative falls under various criminal and civil provisions. Specifically, CBP is authorized to collect data pursuant to the Homeland Security Act of 2002, as amended, Pub. L. No. 107-296, 116 Stat. 2135 (2002), as amended, 6 U.S.C. § 101 et seq.; 29 U.S.C § 654(a)(1), Duties of employers and employees; and 41 C.F.R. § 102-74, Facility Management. Additionally, the rules of behavior and appropriate uses of social media is authorized by DHS and CBP directives.[21] CBP is responsible for ensuring the safety of America's borders while enabling legitimate trade and travel. The purpose of this initiative is to expand the sources of information available to CBP to maintain the safety and security of employees, facilities, and operations, ensuring legitimate trade and travel. Access to publicly available information assists CBP personnel in providing a complete and accurate operating picture to decision makers. The real-time information that CBP can gather from social media assists CBP in handling quickly evolving events for situational awareness. For example, eyewitnesses may post on social media concerning active shooter situations in areas at or near CBP facilities. Additionally, the use of social media allows CBP to gather information on credible threats that may endanger CBP personnel and facilities. These authorities permit investigative personnel to protect CBP personnel against credible threats.

Privacy Risk: There is a risk that CBP personnel may access social media to conduct investigations rather than just to view information for situational awareness.

Mitigation: This risk is mitigated by CBP policies[22] that determine who can use social media for investigative purposes, and under what circumstances. If CBP personnel do not follow those policies, then the policies preclude the use of such information for investigative purposes. Authorized users must abide by the CBP directive allowing them to conduct investigations. CBP personnel who do not abide by the rules of behavior and other policies may lose access to social media or are subject to disciplinary action.

---

[21] CBP Directive 5410-003 "Operational Use of Social Media" (January 2, 2015), implementing the 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).

[22] CBP Directive 5410-003 "Operational Use of Social Media" (January 2, 2015).

Privacy Risk: There is a risk that CBP personnel may misuse their access to social media tools and platforms in order to view publicly available information in a manner that is not consistent with situational awareness operations.

Mitigation: This risk is mitigated by CBP policies governing the use of social media for situational awareness purposes. Additionally, CBP employs a tool to provide personnel with access to website and social media platforms, not generally accessible through the CBP network, which generates audit logs of the sites visited and platforms used. The ability to monitor the sites visited by CBP employees helps to ensure that social media tools are not being used for purposes other than those prescribed.

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

Generally, CBP does not require PII for situational awareness. CBP only collects and disseminates PII if it determines that the PII is necessary for a complete understanding of the operational security aspects of the situation. In the event of an *in extremis* situation, CBP will share certain PII with the responding authority, which may be a federal agency, such as FEMA, or local law enforcement, in order for them to take the actions necessary to save a life or secure a threat. CBP will share this information verbally or electronically through email and other CBP-operated reporting systems.

First Amendment Protections

Prior to collecting information from social media, CBP employees will determine whether the posting is protected by the First Amendment of the U.S. Constitution, and whether the collection of information is permissible under the Privacy Act, as applicable. CBP personnel receive training to distinguish between First Amendment protected activities and credible threats. This training reinforces First Amendment protections and requires that CBP personnel use a balancing test when assessing whether or not speech is deemed a threat. CBP personnel gauge the weight of a First Amendment claim, the severity of the threat, and the credibility of the threat. Information related to First Amendment protected speech and activities will not be collected, unless those activities evolve into dangerous or threatening events. For example, a threat to harm a CBP employee, without additional information, might be considered First Amendment protected speech. A threat that was accompanied by additional information that indicated the threat was actionable and credible (e.g., if the person posted pictures of a weapon and stated they were going

to a specific CBP location to inflict harm), might be designated a credible threat and CBP would investigate further.

In addition, the Privacy Act expressly prohibits the Agency collection of records describing how an individual (defined in the Act as a U.S. citizen or Lawful Permanent Resident) exercises rights guaranteed by the First Amendment. There are exceptions, however, if the record is "pertinent to and within the scope of an authorized law enforcement activity," or if either a statute or the individual about whom the record is maintained expressly authorizes such maintenance.[23] CBP personnel receive social media training in which they are given instruction from the Office of Chief Counsel and the CBP Privacy and Diversity Office on how to identify First Amendment activity and determine if social media posts involve protected activities, such as protests, or if they are actually credible threats for which CBP personnel should take action. CBP personnel manually review all posts identified by tools to determine the accuracy of information and whether it is protected speech.

Credible Threats

CBP will collect PII and report any information about individuals expressing credible threats against CBP persons, events, and facilities to the Joint Intake Center.[24] Threatening posts are those that infer an intent, or incite others, to do physical harm or cause damage, injury, or destruction. CBP uses tools that identify social media posts based on keywords, but will manually review all posts removed from the tools to determine if they rise to the level of a threat and are relevant for the mission of protecting CBP personnel and facilities. PII collected by the CBP from publicly available social media postings that are deemed to involve a credible threat will be stored in JICMS for 25 years.[25]

Privacy Risk: There is a risk that CBP will receive PII or other identifiable information that is not relevant to its investigative and monitoring activities.

Mitigation: This risk is partially mitigated. Under this initiative, CBP will not: 1) post any information on social media; 2) connect with the personal accounts of social media users; 3) accept invitations from other personal social media accounts; and 4) interact on social media sites. For general situational awareness use, PII is of little value and its addition would not provide greater situational awareness. All information collected, disseminated, used, and maintained as part of this Initiative is publicly available. The tools used for this initiative may retrieve PII that is not

[23] 5 U.S.C. § 552a(e)(7).
[24] The Joint Intake Center (JIC) serves as the central "clearinghouse" for receiving, processing and tracking allegations of misconduct involving personnel and contractors employed by CBP and Immigration and Customs Enforcement (ICE). The JIC provides CBP and ICE with a centralized and uniform system for processing reports of alleged misconduct. All reports of misconduct are coordinated with DHS Office of Inspector General (OIG) and referred to the appropriate office for investigation, fact-finding or immediate management action.
[25] *See* DHS/CBP/PIA-044 Joint Integrity Case Management System (JICMS) July 2017, available at https://www.dhs.gov/publication/dhscbppia-044-joint-integrity-case-management-system-jicms.

necessary for either general situational awareness use for threat monitoring and assessment. This information will be deleted and will not be stored or disseminated.

Privacy Risk: There is a risk that any PII collected will be retained for longer than necessary.

Mitigation: This risk is mitigated. Case files created for investigating threats are kept only as long as needed to determine if there is a credible threat or to use in a case file if someone acts on their threat. Any PII collected for general situational awareness will only be stored so long as necessary to act on an *in extremis* event. However, that information may be stored on email servers until those are regularly deleted. Regardless, any information that is collected will be maintained in accordance with established retention periods as outlined in the applicable SORNs.

Privacy Risk: There is a risk that CBP will monitor First Amendment activities including protests and speeches.

Mitigation: This risk is fully mitigated. Unless otherwise authorized by law, CBP does not store or disseminate information related to First Amendment protected speech or activities, unless those activities evolve into dangerous or threatening events impacting the operations or safety of CBP facilities and personnel. CBP oversight personnel offer in-person training for social media users that includes a section on identify and handling First Amendment protected activity. Part of this training involves teaching personnel a balancing test where the nature of the threat, ability to carry out the threat, and weight of First Amendment claim are analyzed to determine if a post is a true threat or not. Additionally, CBP specifically selects keywords so as to minimize collecting information related to First Amendment activities.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

CBP relies on publicly available information – from social media and other sources to ensure a comprehensive understanding of CBP's entire operating picture and monitor events that may impact the security of CBP personnel, facilities, and operations. As such, CBP's monitoring of publicly available social media postings is specifically scoped to the identification of issues and incidents that may have a detrimental impact on the agency. Information garnered from social media will only be used to support the identification of threats and to provide CBP leadership with a more defined operational picture.

CBP will only share information it collects as part of this initiative with state, local, and Federal Government agencies if CBP determines that the information would allow those agencies

to respond to *in extremis* events, or to the extent otherwise authorized or required by law or policy. Any information shared will be anonymized unless PII is needed to respond to an event, for example identifying information associated with someone in danger, or that of an individual whom represents an active threat.

In order to effectively monitor social media, CBP employs tools that search social media sites for certain keywords. CBP selects these keywords to limit the number of results returned and to make sure the results are specifically focused and relevant to the task of identifying and mitigating potential threats to the agency and its personnel. CBP maintains a keyword list for broad threat indicators and separate lists depending on upcoming or current events. These lists are updated based on new intelligence.

Privacy Risk: There is a risk that CBP will inappropriately use or share information gathered from social media sites under this effort.

Mitigation: This risk is fully mitigated. The information collected as part of this initiative is publicly available and has little to no use outside of the purpose for the collection. CBP personnel with access to social media are required to complete training and acknowledge rules of behavior for appropriate use of social media and publicly available information. CBP collects this information to inform decision makers on threats to CBP personnel and facilities, and because of this limited and specific scope, CBP would not be able to share the information for a different purpose, except to the extent otherwise authorized or required by law or policy.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

CBP relies on information from third-party Internet social media services submitted voluntarily by users of those sites and compares it with information available through other open source reporting, as well as a variety of other public and government sources. Individuals posting on social media are also able to edit and delete any incorrect information. CBP personnel reviewing information use their training to determine what information is credible and accurate in order to provide decision makers with a more complete situational awareness picture. Because of the nature of social media information, CBP may not be able to verify the information's accuracy. CBP generally attempts to corroborate social media information with credible news reports, information available in CBP databases, or information obtained from other governmental partners, rather than making operational decisions based solely on social media.

Privacy Risk: There is a risk that because information is being collected in real-time it may be difficult to determine the accuracy of individual posts.

Mitigation: CBP partially mitigates this risk by reviewing information from multiple sources using tools across multiple platforms to determine if information is corroborated by others. Additionally, CBP social media users participate in extensive training to help them analyze information. However, due to the real-time nature of collection, CBP is unable to always verify the accuracy of the information. The impacts of this risk are mitigated by the fact that CBP always assesses the totality of circumstances and available evidence and generally does not make operational decisions solely based on social media posts.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

CBP limits access to social media to users who have completed annual social media training, show a need to access social media for their work, have agreed to specific rules of behavior associated with access to social media tools, and are approved to use it by a supervisor. All information stored through this initiative will be stored in JICMS, a system with built in audit controls. Users are granted access on a "need to know" basis. CBP operates JICMS in compliance with the information security requirements of the Federal Information Security Modernization Act of 2014. Social media sites have their own security that CBP is unable to control. Individuals agree to the terms of social media sites when they post on the platforms and many of these sites provide privacy settings that allow individuals to determine the extent to which their posts are available to the public.

Privacy Risk: There is a risk that an unauthorized individual without a legitimate need to know may access information maintained in CBP systems that CBP obtained from social media.

Mitigation: This risk is mitigated. Only authorized CBP personnel, with a need to know, will have access to social media data stored as part of this initiative. Additionally, because the information is publicly available, anyone would be capable of accessing the information on the social media sites where it is posted.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

In accordance with the CBP Social Media Directive, all CBP employees who use social media in the course of their official duties are required to take annual privacy training and annual

social media training. Additionally, all users must certify that they have read and will abide by the rules of behavior and recertify their need to access social media at least annually. Additionally, the technology and tools used to access social media contain audit controls that track the activity of all users. This allows CBP to monitor what sites and information users are viewing and storing. CBP Office of Information Technology personnel are able to access audit logs that detail the social media searches being conducted by users.

Responsible Officials

Donald Torrence
Executive Director, Mission Readiness Directorate
Office of Intelligence
U.S. Customs and Border Protection

Debra L. Danisek
Privacy Officer
Office of the Commissioner
U.S. Customs and Border Protection

Approval Signature Page

[Original signed and on file with the DHS Privacy Office]

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security