The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

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 requirement[1]:

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: September 25, 2019

Name of Component: Cybersecurity and Infrastructure Security Agency

Contact Information: (b)(6)

Counsel[2] Contact Information: (b)(6)

Counsel Contact information: (b)(6)

IT System(s) where social media data is stored: Social media data will be stored on the contractor's system. Resulting products will be stored on DHS analyst's hard drive and shared with the CFI TF on an access controlled DHSConnect page. Information will not be filed or retrieved by personal identifier.

Applicable Privacy Impact Assessment(s) (PIA): No Privacy Impact Assessment is required at this time. During this initial pilot phase, data collected as part of this project will either not include personally identifiable information (PII) or will consist of social media information (username, handle, social media post content) attributed to a foreign source. Should CISA decide to move the pilot into the next stage, the CISA Office of Privacy will consider developing a PIA.

Applicable System of Records Notice(s) (SORN): No SORN is required for this pilot at this time. Information collected during this pilot will not be filed or retrieved by personal identifier.

[2] Counsel 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.

DHS formed a Countering Foreign Influence (CFI) Task Force to understand and counter the impacts of malign foreign influence operations on the United States. For the purposes of the CFI Task Force, foreign influence operations are actions taken by foreign governments designed to influence policy, shape public discourse, sow discord, and advance that government's national self-interests. Ultimately, the CFI Task Force seeks to leverage its legal authorities to examine how foreign adversaries leverage social media platforms to disseminate misinformation, malinformation, and disinformation[3] in ways that threaten homeland security. To do this, the CFI Task Force is initiating a pilot, the initial stage of which will consist of testing the ability of certain analytical capabilities to provide outputs of value related to the impact of disinformation.

During the initial stage of the pilot, the CFI Task Force will rely on TRUSTED Partners consulting group, a contracted entity, to test their capabilities against existing data sets to understand the likely impact of historic disinformation, target audiences of that disinformation, and the likely reaction of those audiences to the disinformation. Specifically, TRUSTED Partners will utilize publicly-available social media data released by Facebook and Twitter in connection to the U.S. House of Representatives Permanent Select Committee on Intelligence's (HPSCI) investigation into 2016 election-related foreign influence campaigns. Disinformation social media data utilized during the initial stage of the pilot will include foreign social media posts published by HPSCI as part of that investigation.[4] The pilot will also include social media posted between June 19, 2015 an December 31, 2017 and collected and analyzed as part of a Clemson University research project[5] on understanding the Russian Internet Agency's (IRA) efforts to influence the United States political landscape using Twitter handles that HPSCI has associated[6] with the IRA. The capability will compare homeland security-related trends from those datasets to historical advertising content

[3] **Disinformation**: Information that is deliberately false or misleading and distributed with malicious intent. Malicious intent distinguishes disinformation from other deliberately false information including satire, parody, and hoax. **Malinformation**: Information that is verifiable but is disseminated with malicious intent. **Misinformation**: Information whose inaccuracy is unintentional, including information reported in error.

[4] https://intelligence.house.gov/social-media-content/social-media-advertisements.htm.

[5] http://pwarren.people.clemson.edu/Linvill_Warren_TrollFactory.pdf.

[6] https://intelligence.house.gov/uploadedfiles/ira_handles_june_2018.pdf.

and engagement metadata, using their capabilities to identify likely impact of the disinformation, likely audience targeted and likely reactions related to the specific disinformation narratives that threaten homeland security. The impact of the disinformation will be measured using binary user reactions (e.g., likes, clicks, etc.) and will not utilize content or any other social media user information for impact context.

Social media information collected by the TRUSTED Partners on behalf of the CFI Task Force may be retained in the form of aggregated data as well as in written products developed using the aggregated data. Products will be used internally by the CFI Task Force to determine the utility of the capability. Ultimately, the goal is to use the vendor reporting to inform future CISA education and awareness materials and allow for more targeted and effective outreach to stakeholders most likely to be affected by particular foreign influence campaigns. During the initial phase of the pilot, products will be shared with DHS's Office of Intelligence and Analysis (I&A), DHS Policy, and the Secretary's Office to determine the utility of the products to these offices.

Depending on funding requirements, legal and privacy constraints, and the success of the initial phase of the pilot, future phases of the pilot might address foreign influence in other contexts not discussed here. This SMOUT will be updated to provide additional specifics of the future phases of the pilot. In addition, the CISA Office of Privacy will continue to monitor this pilot to ensure any future privacy compliance documentation is completed, as appropriate.

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

- The Homeland Security Act of 2002, as amended by the Cybersecurity and Infrastructure Security Act of 2018

a) **Has Counsel listed above reviewed these authorities for privacy issues and determined that they permit the Program to use social media for the listed operational use?**

☒ Yes. ☐ No.

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: Contractor systems will analyze social media data, but no new data is being retrieved from social media. For the purposes of testing the capability, CISA is asking the contractor to utilize existing publicly-available social media datasets

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;

☐ Yes. ☒ No. If not, please explain: Not applicable. Neither CISA nor the contractor will directly access social media accounts to accomplish the initial stage of the pilot.

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

☐ Yes. ☒ No. If not, please explain: Not applicable. CISA and the contractor will not access the information through social media.

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

☐ Yes. ☒ No. If not, please explain: CISA and the contractor will not access social media sites for the purposes of the initial phase of the pilot.

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: No PII of U.S. Persons will be collected as part of the pilot.

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: Not applicable. CISA and the contractor will not access social media to perform the pilot.

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: Rules of Behavior and Training are not required because CISA and contractor employees will not access social media to perform the work required in the pilot.

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: Not applicable.

DHS SOCIAL MEDIA DOCUMENTATION

(To be Completed by the DHS Privacy Office)

DATE reviewed by the DHS Privacy Office: 9/30/2019

NAME of the DHS Privacy Office Reviewer: Jamie Huang

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. <Please include the name and number of PIA here.>
  - ☐ New.
  - ☐ Updated. <Please include the name and number of PIA to be updated here.>
- ☐ A SORN is required:
  - ☐ Covered by existing SORN. <Please include the name and number of SORN here.>
  - ☐ New.
  - ☐ Updated. <Please include the name and number of SORN to be updated here.>

DHS PRIVACY OFFICE COMMENTS

DHS CISA's Countering Foreign Influence (CFI) Task Force is contracting out a pilot with Trusted Partners consulting group for them to use existing data sets to understand/study the

likely impact of historic disinformation, target audiences of that disinformation, and the likely reaction of those audiences to the disinformation. This disinformation obtained for this initial stage of the pilot will include social media posts collected from HSPIC foreign social media posts published by HPSCI as part of that investigation. The pilot will also include social media posted between June 19, 2015 an December 31, 2017 and collected and analyzed as part of a Clemson University research project on understanding the Russian Internet Agency's (IRA) efforts to influence the United States political landscape using Twitter handles that HPSCI has associated with the IRA.

As described on page 4 of the SMOUT, this initial pilot has been narrowly scoped, focusing on disinformation measured by binary user reactions (e.g., likes, dislikes, number of clicks, etc.) and most importantly, will not utilize content or any other social media user information (e.g. consumer sentiments) for impact context. No PII will be retained. CISA Privacy estimates this initial data set to be around three million posts. The testing capability should last only for a couple days. CISA has also explained that the results will be aggregated.

This SMOUT will be updated to provide additional specifics regarding future phases of the pilot to include, but not limited to, adding additional data sets, etc. Should CISA CFI decide to operationalize this feature, it will require CISA to first publish a PIA. SORN coverage determination will be conducted during the writing process of the PIA.