DHS-001-02632-00007405/02/2022

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, 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-001-02632-00007405/02/2022

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy



# 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. Immigration and Customs Enforcement

**Contact Information:** (b)(6); (b)(7c) Deputy Privacy Officer, (202) 732-(b)(6); (b)(7c)

**Counsel[2] Contact Information:** Jennifer Fenton, Chief, Enforcement and Removal Operations Division, OPLA; (b)(6); (b)(7c) Chief, Immigration Law and Practice Division, OPLA.

**IT System(s) where social media data is stored:** (b) (7)(E)
(b) (7)(E)

**Applicable Privacy Impact Assessment(s) (PIA):**

(b) (7)(E)

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

DHS/ICE-009 – External Investigations

(b) (7)(E)

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

DHS-001-02632-00007605/02/2022



(b) (7)(E)

DHS-001-02632-00007605/02/2022

DHS-001-02632-00007705/02/2022



# 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.**

As the definition of social media in the DHS Instruction 110-01-001 *Privacy Policy for the Operational Use of Social Media* (Privacy Policy) is drafted broadly so as to likely include general use of the Internet and as social media technology is ever changing and evolving, this template addresses ICE's use of the Internet, to include social media as defined in the Privacy Policy.

ICE uses the Internet, including social media as defined in the Privacy Policy, for criminal and administrative immigration law enforcement purposes. (b) (7)(E) (b) (7)(E) (b) (7)(E) This immigration law enforcement use of the Internet including social media, falls into the following three categories: (1) using the Internet, including social media, to assist in locating, arresting, and adjudicating individuals who may be amenable to removal under the Immigration and Nationality Act or are otherwise suspected of violations of U.S. immigration law and assisting other law enforcement agencies with investigations and adjudications related to individuals, (2) pre-operational, operational, and situational awareness uses related to officer safety or threats to the public at-large, and (3) to obtain information to assist in determining whether to exercise prosecutorial discretion.

**Category One: Basic Criminal and Administrative Enforcement of the Immigration and Nationality Act**

With regard to the use of the Internet, including social media, to locate and arrest individuals, ICE officers, agents, attorneys, and support personnel routinely use a variety of government and commercial databases to identify, locate, and arrest individuals who may be amenable to removal and meet ICE's current enforcement priorities. However, additional information not available in these databases is available on the Internet, including social media. The use of the Internet, including social media, will allow ICE to gather information that assists in identifying, locating, and arresting individuals wanted for crimes and/or who may be amenable to removal, and assisting other law enforcement agencies with investigations related to individuals where necessary and appropriate. It will also allow ICE attorneys who represent the agency in civil immigration proceedings before the Executive Office for Immigration Review to conduct general and specific case research and preparation.

DHS-001-02632-00007705/02/2022

Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy



**Category Two: Officer and Public Safety**

ICE also uses the Internet, including social media, for pre-operational/operational/situational awareness uses relating to officer safety or threats to the public at-large. (b) (7)(E)

(b) (7)(E)

**Category Three: Prosecutorial Discretion**

Finally, ICE also uses the Internet, including social media, to gather information related to the possible exercise of prosecutorial discretion. Pursuant to Director Morton's June 17, 2011 memorandum relating to the exercising of prosecutorial discretion, ICE law enforcement personnel are expected to consider a number of factors when deciding whether to exercise prosecutorial discretion in various situations. Some of these factors include: whether the subject is a danger to the community or to national security, whether the subject is the primary caregiver to a minor, or a person with a physical or mental disability, a subject's educational and military background, a subject's ties and contributions to the community, whether the subject (or the subject's spouse) is pregnant or nursing, whether the subject or subject's spouse suffers from severe mental or physical illness. These factors can be difficult to ascertain using routine government and commercial databases and the use of the Internet including social media serves as another tool to attempt to identify these unique factors. Similarly, some of these same factors may also apply when setting conditions of release from ICE custody. The Internet, including social media, provides a source of information that can be used to help determine when it is appropriate to release an individual from ICE custody.

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

- Homeland Security Act of 2002, as amended, Pub. L. No. 107-296, 116 Stat. 2135 (2002)
- Immigration and Nationality Act of 1952, as amended, U.S. Code Title 8
- DHS Delegation No. 7030.2, Delegation of Authority to the Assistant Secretary of U.S Immigration and Customs Enforcement
- ICE Delegation No. 0001, Delegation of Authority to the Directors, Detention and Removal and Investigations, and to Field Office Directors, Special Agents in Charge and Certain Other Officers of the Bureau of Immigration and Customs Enforcement
- 8 C.F.R. § 2.1, Authority of the Secretary of Homeland Security

Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy



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: Unknown.

The Internet has been in use at ICE's legacy agencies since it was publicly available. However, the use of certain specific social media websites such as (b) (7)(E) (b) (7)(E) have not yet been implemented but will be after adjudication of this Template by the DHS Privacy Office.

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

*See* Memorandum from John Morton, Use of Public and Non-Public Online Information, June 28, 2012.

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:

The nature of immigration law enforcement investigations may require investigators to use non-government-issued equipment when engaging in investigations. Investigators at times find themselves in rapidly evolving situations in the field that call for the use of adaptive measures. In situations where government-issued equipment is either not available, or is technologically insufficient to perform the required task at hand, investigators may need to rely on non-government-issued equipment. However, ICE is currently working to provide government-issued equipment to all personnel so as to not require the use of non-government-issued equipment in these circumstances.

b) (b) (7)(E)

Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy



(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;

☒ Yes. ☐ No. If not, please explain:

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

☒ Yes. ☐ No. If not, please explain:

Law enforcement personnel may not access restricted online sources or facilities absent legal authority permitting entry into private space.

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:

The applicable SORNs cited above are all exempted by Final Rules from the Privacy Act (e)(1) requirement (5 U.S.C. § 552a(e)(1)), which normally limits agencies to collecting only information about individuals that is relevant and necessary to accomplish a purpose of the agency required by statute or Executive Order. The exemption from the (e)(1) requirement is necessary to ensure the integrity of law enforcement investigations, as more fully detailed in the Final Rules.

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:

DHS-001-02632-00008105/02/2022



ICE's rules of behavior stated that law enforcement personnel should retain the information they access on the Internet, including social media, if they would have retained that content had it been written on paper. These contents should be preserved in a manner authorized by ICE procedures governing the preservation of electronic communications.

**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:

All ICE users will complete the necessary training when it is available.

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-001-02632-00008105/02/2022

DHS-001-02632-00008205/02/2022

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy



# DHS SOCIAL MEDIA DOCUMENTATION

**(To be Completed by the DHS Privacy Office)**

**DATE reviewed by the DHS Privacy Office: November 6, 2012**

**NAME of the DHS Privacy Office Reviewer:** (b) (6)

**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/ICE/PIA-009 – Fugitive Case Management System (FCMS)

DHS/ICE/PIA-015 – Enforcement Integrated Database (EID)

DHS/ICE/PIA-020 – Alien Criminal Response Information Management System (ACRIMe)

☐ New.

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

☐ A SORN is required:

☒ Covered by existing SORN:

DHS/ICE-009 – External Investigations

DHS-001-02632-00008205/02/2022

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy



DHS/ICE-007 – Alien Criminal Response Information Management (ACRIMe) SORN

DHS/ICE-011 – Immigration and Enforcement Operational Records System (ENFORCE) SORN

DHS/USCIS-ICE-CBP-001 – Alien File, Index, and National File Tracking System SORN

☐ New.

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

## DHS PRIVACY OFFICE COMMENTS

The DHS Privacy Office determines that ICE has provided sufficient documentation to demonstrate compliance with the MD 110-01. The rules of behavior reference that Law Enforcement personnel shall follow ICE guidelines and procedures whether the activities are online or offline. ICE did not provide the "offline policy" that is referenced in the Rules of Behavior because it is very close hold and distribution is limited. (b) (7)(E) (b) (7)(E) CE PRIV has reviewed the document.

(b) (7)(E)

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy



- (b) (7)(E)

DHS PRIV also requested additional guidance on how the requirements to retain records were covered. ICE PRIV advised that Section 5 of the ICE principles covers the retention of records. DHS PRIV concurs.

DHS-001-02632-00008505/02/2022

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, 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-001-02632-00008505/02/2022

DHS-001-02632-00008605/02/2022

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy



# 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. Immigration and Customs Enforcement

**Contact Information:** (b6)(b7c) Deputy Privacy Officer, (202) 732 (b6)(b7c)

**Counsel[2] Contact Information** (b6)(b7c) Chief, Homeland Security Investigations Division, (202) 732 (b6)(b7c) ennifer Fenton, Chief, Enforcement and Removal Operations Division, (202) 732- (b6)(b7c)

**IT System(s) where social media data is stored:** (b) (7)(E)

(b) (7)(E)

**Applicable Privacy Impact Assessment(s) (PIA):**

(b) (7)(E)

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

DHS-001-02632-00008605/02/2022

DHS-001-02632-00008705/02/2022

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy



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

(b) (7)(E)

DHS/ICE 008 – Search, Arrest, and Seizure Records

DHS/ICE-009 – External Investigations

(b) (7)(E)

DHS/ALL-020 – DHS Internal Affairs Records

DHS-001-02632-00008705/02/2022

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy



# 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.**

As the definition of social media in the DHS Instruction 110-01-001 *Privacy Policy for the Operational Use of Social Media* (Privacy Policy) is drafted broadly so as to likely include general use of the Internet and as social media technology is ever changing and evolving, this submission addresses ICE's use of the Internet, to include social media as defined in the Privacy Policy.

ICE uses the Internet, including social media as defined in the Privacy Policy, for criminal law enforcement purposes. (b) (7)(E)

(b) (7)(E)

This criminal law enforcement use of the Internet, including social media, falls into the following three categories: (1) using the Internet, including social media, to assist in locating, arresting, and adjudicating fugitives and assisting other law enforcement agencies with investigations and adjudications related to the fugitive, (2) using the Internet, including social media, to assist in investigating, gathering evidence, and gathering criminal intelligence on criminal and potential criminal activity, and (3) pre-operational, operational, and situational awareness uses related to officer safety or threats to the public at-large.

**Category One: Locating, Arresting, and Adjudicating Fugitives**

With regard to the use of the Internet, including social media, to locate and arrest fugitives and criminals, ICE officers, agents, attorneys, and support personnel routinely use a variety of government and commercial databases to identify, locate, and arrest fugitives. These individuals could include members of the public or employees or contractors of ICE and CBP suspected of committing crimes or other forms of misconduct. However, additional information not available in these databases is available on the Internet, including social media. The use of the Internet, including social media, will allow ICE to gather information that assists in identifying, locating, and arresting fugitives wanted for crimes and assisting other law enforcement agencies with identifying, locating, and arresting fugitives.

**Category Two: Criminal Investigations and Law Enforcement Intelligence**

ICE also uses the Internet, including social media, to assist in investigating, gathering evidence, and gathering law enforcement intelligence on criminal and potential criminal

Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy



activity. This use of the Internet, including social media, involves activities to gather information such as Internet searches, reviewing social media sites, (b) (7)(E) and reviewing comments posted on websites. This information is gathered and used by ICE officers, agents, attorneys, and support 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 criminal investigations of members of the public or employees or contractors of ICE and CBP.

**Category Three: Officer and Public Safety**

ICE also uses the Internet, including social media, for pre-operational/operational/situational awareness uses relating to officer safety or threats to the public at-large. (b) (7)(E)

(b) (7)(E)

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

- Homeland Security Act of 2002, as amended, Pub. L. No. 107-296, 116 Stat. 2135 (2002)
- DHS Delegation No. 7030.2, Delegation of Authority to the Assistant Secretary of U.S Immigration and Customs Enforcement
- 19 U.S.C. § 1589a, Enforcement authority of customs officers
- 8 U.S.C. § 1357, Powers of immigration officers and employees

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: Unknown.

The Internet has been in use at ICE's legacy agencies since it was publicly available.

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

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy



*See* Memorandum from John Morton, Use of Public and Non-Public Online Information, June 28, 2012.

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:

The nature of criminal investigations may require investigators to use non-government-issued equipment when engaging in criminal investigations. Investigators at times find themselves in rapidly evolving situations in the field that call for the use of adaptive measures. In situations where government-issued equipment is either not available, or is technologically insufficient to perform the required task at hand, investigators may need to rely on non-government-issued equipment. However, ICE is currently working to provide government-issued equipment so as to not require the use of non-government-issued equipment in these circumstances.

b) (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;

☒ Yes. ☐ No. If not, please explain:

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

☐ Yes. ☒ No. If not, please explain:

DHS-001-02632-00009105/02/2022



Law enforcement personnel may not access restricted online sources or facilities absent legal authority permitting entry into private space. Where legal authority exists, law enforcement personnel may access restricted online information.

**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:

The applicable SORNs cited above are all exempted by Final Rules from the Privacy Act (e)(1) requirement (5 U.S.C. § 552a(e)(1)), which normally limits agencies to collecting only information about individuals that is relevant and necessary to accomplish a purpose of the agency required by statute or Executive Order. The exemption from the (e)(1) requirement is necessary to ensure the integrity of law enforcement investigations, as more fully detailed in the Final Rules.

**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:

ICE's rules of behavior state that law enforcement personnel should retain the information they access on the Internet, including social media, if they would have retained that content had it been written on paper. These contents should be preserved in a manner authorized by ICE procedures governing the preservation of electronic communications.

**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:

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

DHS-001-02632-00009105/02/2022

DHS-001-02632-00009205/02/2022



The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy



☒ 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-001-02632-00009205/02/2022

DHS-001-02632-00009305/02/2022

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy



# DHS SOCIAL MEDIA DOCUMENTATION

**(To be Completed by the DHS Privacy Office)**

**DATE reviewed by the DHS Privacy Office: 11/6/2012**

**NAME of the DHS Privacy Office Reviewer:** (b) (6)

**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.

(b) (7)(E)

☐ New.

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

DHS-001-02632-00009305/02/2022

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy



☒ A SORN is required:

☒ Covered by existing SORN.

(b) (7)(E)

DHS/ICE 008 – Search, Arrest, and Seizure Records

DHS/ICE-009 – External Investigations

(b) (7)(E)

DHS/ALL-020 – DHS Internal Affairs Records

☐ New.

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

## DHS PRIVACY OFFICE COMMENTS

The DHS Privacy Office determines that ICE has provided sufficient documentation to demonstrate compliance with the MD 110-01. The rules of behavior reference that Law Enforcement personnel shall follow ICE guidelines and procedures whether the activities are online or offline. ICE did not provide the "offline policy" that is referenced in the Rules of Behavior because it is very close hold and distribution is limited. (b) (7)(E)

(b) (7)(E) ICE PRIV has reviewed the document.

(b) (7)(E)

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy



- (b) (7)(E)

DHS PRIV also requested additional guidance on how the requirements to retain records were covered. ICE PRIV advised that Section 5 of the ICE principles covers the retention of records. DHS PRIV concurs.

(b) (5)

DHS-001-02632-00009605/02/2022

DHS-001-02632-00009605/02/2022

(b) (5)

DHS-001-02632-00009705/02/2022

DHS-001-02632-00009705/02/2022

(b) (5)

DHS-001-02632-00009805/02/2022

DHS-001-02632-00009805/02/2022

(b) (5)

DHS-001-02632-00009905/02/2022

DHS-001-02632-00009905/02/2022

(b) (5)

DHS-001-02632-00010005/02/2022

DHS-001-02632-00010005/02/2022

(b) (5)

DHS-001-02632-00010105/02/2022

DHS-001-02632-00010105/02/2022


Homeland Security

# DHS 4300A
# Sensitive Systems Handbook

## Attachment X
## Social Media

Version 14
July 24, 2018

DHS-001-02632-00010305/02/2022


# Document Change History

| Version | Date | Description |
|---|---|---|
| 0.6 | March 25, 2010 | Final Draft for Comment |
| 0.7 | May 12, 2011 | Final Draft for Review; Includes Component Comments |
| 8.0 | May 23, 2011 | Final |
| 9.1 | July 24, 2012 | Stylistic and formatting changes throughout the document |
| 11.0 | August 5, 2014 | Additional stylistic changes throughout. |
| 14.0 | July 24, 2018 | Thoroughly revised to conform to current standards and best practices.<br>Thoroughly updated with regard to Privacy issues.<br>Version numbered to coincide with current 4300A Policy edition (No version 11, 12, nor 13 of this Attachment was published. |


DHS-001-02632-00010305/02/2022

DHS-001-02632-00010405/02/2022


# Contents




DHS-001-02632-00010405/02/2022

DHS-001-02632-00010505/02/2022




.


DHS-001-02632-00010505/02/2022

DHS-001-02632-00010605/02/2022


# 1.0 INTRODUCTION

***Social media*** such as Facebook, Twitter, and Instagram have become ubiquitous in our daily life. According to a study by the Pew Research Center, nearly two-thirds (65%) of all American adults use social network sites—a nearly tenfold jump in the past decade[1]. Due to extensive casual Internet use, it comes as no surprise that Federal employees and contractors may have difficulty deciding what constitutes acceptable and security-conscious behavior in using social media.

Even as Government organizations consider how best to leverage the interactivity enabled by social media, they must also ensure a common understanding of how employees are expected to use those media.

Issued under the authority of the Department of Homeland Security (DHS) Chief Information Officer (CIO), through the Office of the Chief Information Security Officer (OCISO), this document expands on existing DHS policy as provided in Section 3.16, "Social Media," of *DHS Sensitive Systems Policy Directive 4300A*, and in DHS Management Directive (MD) 4400.1, "Web (Internet, Intranet, and Extranet Information) and Information Systems."

This document is applicable under the following guidelines:

- Whether or not the use is official (work-related) or unofficial (personal)
- Whether or not the use occurs on sanctioned "official" social media sites or on commercially managed sites
- Whether or not use is accomplished using Government-issued equipment or on electronic devices owned by the employee or other third-party.

## 1.1 Background

Cyber attacks on and via social media are rapidly increasing because of the abundance of personal information available on social media sites that is of interest to cybercriminals such as home address, family names, friends' names, and current employer. Due to the high threat of ***malware*** infiltration and the sensitive nature of the information maintained at DHS, social media host sites are blocked at the Department's Trusted Internet Connections (TIC).[2] The Assistant Secretary, Office of Public Affairs (OPA), as well as Component public or external affairs offices, however, do permit limited social media use "by exception," through sanctioned Government and commercial social media sites and social networking services. These limited uses of social media make information and services more widely available. Sanctioned social media can:

- Provide additional sources that the public can use to obtain supplemental information about the Department's activities

[1] "Social Media Usage: 2005-2015", Pew Research Center, October 6, 2016, http://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/

[2] Section 3.16, *DHS Sensitive Systems Policy Directive 4300A*.


DHS-001-02632-00010605/02/2022

DHS-001-02632-00010705/02/2022


- Provide opportunities for participation and collaboration on Department activities
- Reach a wider audience more efficiently through the use of social media capabilities
- Showcase the Department's work and integration
- Support Department and Component missions

Unofficial (personal) social media usage can easily make DHS personnel and the Department victims of ***social engineering*** or other forms of cyber-attack. Employees need guidance to help minimize the risks their social media use poses to the Department and its missions.

### 1.2 Purpose and Scope

This document provides guidance regarding official (work-related) and unofficial (personal) social media use whether occurring within or outside the Department network, the risks and attack techniques associated with social media, and best practices for social media use.

### 1.3 Application

This document applies to all DHS Federal employees and contractors, describes the governance of social media sites across DHS, and addresses the use and associated risks of social media technologies in three scenarios:

- Required work-related use
- Unofficial or personal use on Government equipment
- Unofficial or personal use on non-Government equipment

The term *equipment* includes both non-portable devices such as desktop computers as well as mobile devices such as laptop computers smartphones and tablets.

Commonly used social media terms are in bold italics throughout this attachment and are defined in the Glossary.


DHS-001-02632-00010705/02/2022

DHS-001-02632-00010805/02/2022


# 2.0 USE OF SOCIAL MEDIA

## 2.1 Official Public Affairs Use of Social Media

Many Federal Departments and agencies are required to publish Government information for public engagement or external affairs purposes. Component offices of public or external affairs publish materials on dhs.gov, which is the official website and presence of DHS. In addition, some Components maintain their own websites, subject to departmental oversight.

Instructions for using dhs.gov and commercial or third party social media are provided at the DHS Web Center (see www.dhs.gov/webcenter).

As a result of these technological relationships between the Department and the public, it is imperative that DHS engage the public in a manner that complies with Federal accessibility, privacy, information security, and records requirements.

### 2.1.1 Governance

The DHS Office of Public Affairs (OPA) serves as the primary account holder for all DHS and Component social media websites, approves and manages all content posted, and when necessary acts as the final authority on comment acceptability. OPA will ensure that posted content meets the requirements for publicly available information and materials.

### 2.1.2 Privacy Issues

To protect Personally Identifiable Information (PII) internally and when engaging the public, DHS employees must comply with Federal privacy laws, Office of Management and Budget (OMB) guidance, and DHS privacy policies when using social media in an official capacity. The Privacy Office is responsible for ensuring that DHS use of social media sustains and does not erode privacy protections concerning the use, collection, and disclosure of ***PII.***

It is imperative that the Department be transparent about its use of social media to avoid concerns about unauthorized surveillance. Therefore, DHS must engage social media websites in a manner that protects privacy and respects users' intent. The public user fully expects privacy protections while interacting with the Department. In order to address these and other concerns, the DHS Privacy Office has set forth specific requirements for using social media in a privacy- sensitive manner.

Each social media website provides its own privacy policy, and while users are typically required to submit some PII during the registration process, the Department will neither solicit nor collect such PII. The Department will examine the social media website or application privacy policy and evaluate the risks to determine whether or not the website is appropriate for the Department's use. If an agency posts a link that leads to a social media website, the agency will provide an alert to the visitor, either a statement adjacent to the link or a "pop-up," explaining that visitors are being directed to a non-government website that may have different privacy policies from those of the agency's official website.

The Department will only collect the minimum information necessary for the performance of official functions. Official DHS accounts on social media websites will be identified by the Department or Component seal and an easily identifiable account user name indicating DHS presence, such as "DHS Jane Q. Employee."


DHS-001-02632-00010805/02/2022

DHS-001-02632-00010905/02/2022


As part of the Department's privacy compliance process, the DHS Privacy Office has developed two Department-wide Privacy Impact Assessments (PIA), both found at www.dhs.gov/privacy, to identify and mitigate privacy risks for the Department's use of social media for public engagement or external affairs:

- "Use of Social Networking Interactions and Applications (Communications/Outreach/Public Dialogue)," September 16, 2010
- "Use of Unidirectional Social Media Applications," March 8, 2011

These two PIAs and the DHS privacy policies, including those that are social media specific, govern the Department's use of social media from a privacy standpoint. The DHS privacy policy as well as privacy policies specific to social media can be found at www.dhs.gov.

PIA determination is made on a case by case basis through the social media privacy threshold analysis (SMPTA). Components should work with their Component Privacy Office to ensure compliance with privacy requirements. DHS Headquarters should contact the DHS Privacy Office directly at PIA@hq.dhs.gov.

Approved PIAs are published on the Department's Privacy Impact Assessment Web page (see www.dhs.gov/topic/privacy) unless they are classified. DHS has issued a PIA detailing the PII to which the Department may have access because of its use of social networking applications, how it will use the information, what information is retained and shared, and how individuals can gain access to and correct their information.

If PII is posted on a social media site, the Department will attempt to delete it. If that is not possible, the Department will disregard the PII and it will not be maintained in agency files. It should be noted, however, that PII posted on a social media website or sent to the Department in connection with the transaction of public business may become part of a Federal record and will have to be maintained in accordance with appropriate records retention policies.

Note that this privacy compliance framework does not apply to the Department's "operational use of social media." See section 2.2 for details.

### 2.1.3 Standards of Conduct

DHS employees and contractors are responsible for knowing and following the guidelines in DHS Directive) 262-04, "DHS Web (Internet and Extranet Information)" (Revision 00) and Executive Branch conduct guidelines, such as "Standards of Ethical Conduct for Employees of the Executive Branch," when using social media in an official capacity. These standards cover topics of prohibited activities such as:

- Engaging in vulgar or abusive language, personal attacks of any kind, or offensive terms targeting individuals or groups
- Endorsement of commercial products, services, or entities
- Endorsement of political parties, candidates, or groups
- Lobbying members of Congress using DHS or any other appropriated resource
- Use of Government resources to foster commercial interests or individual profit


DHS-001-02632-00010905/02/2022

DHS-001-02632-00011005/02/2022


Federal employees often inadvertently fail to comply with the stringent requirements of the Hatch Act of 1939, which governs political speech by Federal employees. The U.S. Office of Special Counsel (OSC) issued "Hatch Act Social Media and Email Guidance" regarding the applicability of the Hatch Act to social media engagement in the workplace by Federal employees[3]. The Hatch Act's restrictions may determine whether or not Federal employees are allowed to post content that could be interpreted in a political light. Employees should understand the Hatch Act, and Sections 4 and 5 of this document, before posting on social media or revealing professional titles or political affiliations.

### 2.2 Operational Use of Social Media

As part of the Department's homeland security missions, DHS personnel may engage in the operational use social media to meet their mission requirements, consistent with their existing authorities and subject to the approval of the Chief Privacy Officer.

Pursuant to the DHS Management Directive 110-01, "Privacy Policy for Operational Use of Social Media" (June 8, 2012), "operational use" means the 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.

#### 2.2.1 Authority

Program Managers and System Managers must consult with counsel to ensure that appropriate authority exists to engage in categories of operational use of social media before Component employees engage in those activities.

#### 2.2.2 Privacy Compliance Documentation

Before engaging in, or contracting for, new or modified categories of operational use of social media (which as defined includes investigatory purposes), Program Managers and System Managers, in consultation with Component Privacy Officers or Privacy Points Of Contact and counsel must complete a Social Media Operational Use Template (SMOUT) to document the authority and purpose(s) of those uses as well as a description of those uses, and to determine whether all of the Rules of Behavior discussed below will apply to the particular uses(s) covered by the SMOUT.

Please contact the DHS Privacy Office at PIA@hq.dhs.gov for a blank SMOUT form.

SMOUTs are submitted to the Chief Privacy Officer for a prompt review and determination as to whether a new or updated PIA or SORN is required. SMOUTs are also completed to document

[3] Official of Special Counsel, "Hatch Act Social Media and Email Guidance", https://osc.gov/Pages/Hatch-Act-Social-Media-and-Email-Guidance.aspx


DHS-001-02632-00011005/02/2022

DHS-001-02632-00011105/02/2022


categories of operational use of social media in existence prior to this Instruction to ensure compliance with this Instruction. Once a SMOUT is approved for a category of operational use, a new SMOUT is not required for additional use of social media within that category unless there is a material modification of the Rules of Behavior applicable to that category. Components may appeal to the Deputy Secretary of Homeland Security if there is a disagreement over the DHS Privacy Office determination of privacy compliance for the operational use of social media.

### 2.2.3 Access

DHS employees who are authorized to use social media by their Component heads renew their access authority annually, consistent with annual training requirements. Access is contingent upon an employee's successfully completing privacy training for operational use of social media.

### 2.2.4 Rules of Behavior

Component Privacy Officers or PPOCs, in coordination with counsel and Program Managers, or System Managers as appropriate, draft Rules of Behavior for operational use of social media (either separately or as part of a broader policy document) and submit them with the Template to the Chief Privacy Officer for review and approval. Personnel granted access to use social media certify annually that they have read and understand the Component Rules of Behavior. Where certification is not practicable, Component Privacy Officers and PPOCs maintain records of employee attendance at privacy training that includes training on Rules of Behavior.

Rules of Behavior must include requirements for operational use of social media and the consequences of failure to adhere to those requirements. Where a federal policy establishes guidelines that apply to a Component's operational use of social media, the Component's Rules of Behavior incorporate that policy and that fact is noted in the Template.

Unless otherwise noted in the Template adjudication process, the Rules of Behavior provide, at a minimum, that DHS employees:

1. Use social media for operational purposes only when activities are authorized by statute, executive order, regulation, or policy.
2. Use only government-issued equipment, government accounts, and only government email addresses when engaging in the operational use of social media.
3. 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.
4. Access publicly available information through social media only by reviewing posted information without interacting with any individual who posted the information.
5. Respect individuals' privacy settings and access only information that is publicly available unless the individual whose information the employee seeks to access has given consent to access it.
6. Collect the minimum PII necessary for the proper performance of their authorized duties;
7. Protect PII as required by the Privacy Act and DHS privacy policy.


DHS-001-02632-00011105/02/2022

DHS-001-02632-00011205/02/2022


8. Document operational use of social media, including date, site(s) accessed, information collected, and how it was used in the same manner that the Department would document information collected from any source in the normal course of business. For instance, where information obtained through authorized operational use of social media is used in whole or in part to make decisions regarding an individual's rights, benefits or privileges, employees document that fact in relevant records.
9. When use of the social media site is completed, always log out of the site.

### 2.2.5 Privacy Training

Component Privacy Officers or PPOCs tailor privacy training for the operational use of social media to Component-specific needs, based upon training materials provided by the Chief Privacy Officer. Completion of this privacy training is a prerequisite for obtaining access to social media for operational use. Upon completion of this training, employees will certify that they have read and understand their Component's Rules of Behavior. Where certification is not practicable, Component Privacy Officers and PPOCs maintain records of employee attendance at privacy training that includes training on Rules of Behavior. Employees also complete refresher training and recertify they have read and understand their Component's Rules of Behavior annually thereafter. Privacy training content includes, at a minimum, legal authorities, acceptable operational uses of social media, access requirements, applicable Rules of Behavior, and requirements for documenting operational uses of social media.

### 2.2.6 Retention of PII

Component Program Managers or System Managers where appropriate, maintain PII collected through authorized operational uses of social media in the applicable Privacy Act system of records in accordance with approved records retention schedules.

## 2.3 Unofficial or Personal Use of Social Media on Government Equipment

Social media is an attack vector routinely exploited by cybercriminals, whose activities may expose the Department to unacceptable risk. Additionally, social network activity consumes bandwidth and can negatively impact employee productivity. DHS prohibits personal access to social media from Government equipment unless an exception to policy has been granted.

Although DHS employees are authorized limited personal use of DHS office equipment in accordance with DHS Management Directive (MD) No. 4600.1, "Personal Use of Government Office Equipment," such authorization does not apply to the use of DHS equipment for personal use of social media. This restriction also applies to contractors and other individuals using DHS equipment.

## 2.4 Unofficial or Personal Use of Social Media on Non-Government Equipment

Employee activities potentially affect DHS job performance, the performance of others, and DHS business interests. Any information posted on the Internet incurs a level of risk, because that information is exposed indefinitely with no reliable methods for deletion or retraction. In addition, because of the connected nature of the Internet, even information presumed to be posted in a venue with restricted access is potentially accessible to anyone.


DHS-001-02632-00011205/02/2022

DHS-001-02632-00011305/02/2022


"Unofficial Internet posts" result when DHS personnel express DHS-related thoughts, ideas, knowledge, experience, and opinions on any Internet site, whether or not the site is DHS-controlled. Unofficial Internet posts are personal expressions developed and released by an employee or contractor that have not been initiated by any official part of the DHS organization or reviewed through an official DHS approval process. Employees must remember that any information about another individual is almost surely protected by the Privacy Act and should not be shared.

Social networks are of particular concern because of the potential for users to disseminate personal information about themselves and others. Unless strict privacy controls are applied to online profiles, the information posted is viewable by a wide range of strangers. Normally adversaries would have to engage in determined information gathering in order to collect sensitive information, but social networks can easily provide them an opportunity to gather sensitive information with relative ease. Even seemingly harmless facts can be collected and used by adversaries to assemble profiles and select targets. Even with privacy controls in place, DHS employees and contractors should not post any content that they would not be comfortable disclosing to the public.

Employees must remember that any information that is work-related is sensitive and cannot be repeated outside the workplace without appropriate approval. In addition, further limits are in place if you identify yourself, whether directly or indirectly, as a DHS employee.

Consistent with the risks detailed above, the recent guidance issued by the U.S. Office of Special Counsel (OSC) regarding social media outside the workplace does not differ substantially from guidance for the workplace, although more latitude is given for employees to express political thoughts and candidate advocacy and support on their personal websites. See Sections 4 and 5 of this document for additional best practices and guidelines applicable to social media use.


DHS-001-02632-00011305/02/2022

DHS-001-02632-00011405/02/2022


## 3.0 RISKS AND ATTACK TECHNIQUES ASSOCIATED WITH SOCIAL MEDIA

Adversaries look for opportunities to easily target persons of interest on the Internet in order to develop footholds for long-term surveillance and exploitation. Social media sites are attractive to hackers since the same technologies that invite user participation make user systems easy to corrupt with ***malware*** such as ***worms*** that can shut down networks, ***spyware,*** or ***keystroke loggers*** that can steal sensitive data. For example, the availability of ***widgets*** makes it easier for social networkers to share links, insert pictures, etc., but it also makes it easier for an attacker to slip in malicious code or to link to off-site content that contains ***malware***.

### 3.1 Common Risks of Cyber Attacks

The risks associated with social networking fall into a few broad categories:

- Accidentally releasing sensitive information
- Hackers gaining information through a social networking site that will allow the hacker to attack the ***enterprise network***
- Having the social networking account itself hacked
- Identity theft
- Users picking up ***malware*** through the social networking site

Government use of social media also poses potential privacy risks. Social media users voluntarily provide PII in their user profiles (examples are hometown and employer), making such information available to other registered users, including DHS. The availability of this PII does not give the Department the authority or right to collect, use, or disclose that information absent a separate authority to do so.

The emergence of ***Location-Based Services (LBS)*** (geo-location) poses additional privacy concerns. Research undertaken by Carnegie Mellon University in 2009 and 2010[4] found that "currently available location-sharing services do not, for the most part, do a good job of informing [users] about how their location information will be used or provide users with expressive location privacy controls and privacy-protective default settings." Furthermore, although Section 222(f) of the Communications Act[5] generally prohibits wireless carriers from using location-based information for commercial purposes without the express prior consent of the consumer, these prohibitions do not currently apply to LBS providers even though their applications are being downloaded on the devices of wireless carriers.

Consumers may mistakenly conclude that application providers are subject to the same prohibitions as wireless carriers and that no action by consumers is necessary to ensure that their

[4] "Location-Sharing Technologies: Privacy Risks and Controls", Carnegie Mellon University, February 1010. http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf

[5] "Communications Act of 1934", Federal Communications Commission, https://transition.fcc.gov/Reports/1934new.pdf


DHS-001-02632-00011405/02/2022

DHS-001-02632-00011505/02/2022


privacy is protected.[6] The DHS Privacy Office requires all projects, programs, or systems contemplating the use of LBS to submit a PTA.

## 3.2 Common Cyber Attack Techniques

According to the *Guidelines for Secure Use of Social Media by Federal Departments and Agencies*[7], social media technologies such as *wikis, blogs*, and *social networks* are especially vulnerable to the following cyber-attack techniques:

- Spear phishing
- Social engineering
- Web application attacks

### 3.2.1 Spear Phishing

***Spear phishing*** is an attack targeting a specific user or group of users, attempting to deceive the user into performing an action that launches an attack, such as opening a document or clicking a link. Spear phishers rely on knowing some personal piece of information about their target, such as an event, interest, travel plans, or current issues. Sometimes this information is gathered by hacking into the targeted network, but often it is easier to look up the target on a social media network.

In April 2009, the Federal Bureau of Investigation (FBI) released a Headline Alert citing social networking sites as a mechanism for attackers to gather information on their targets by harvesting information from publically accessible networks and using the information as an attack vector[8]. Spear phishers use social media as an alternative way to send phishing messages, as the social media platform bypasses traditional email security controls. Security teams have already observed multiple social media websites used as a propagation mechanism to trick users into opening a document or clicking a link. DHS daily receives many specific attacks via email targeting specific employees by name and position.

### 3.2.2 Social Engineering

The second concern regarding social media use by Federal employees is ***social engineering***, which relies on exploiting the human tendency to trust. The attacker's first step in any social engineering attack is to collect information about the target. Social networking websites can reveal many details of personal information, including resumes, home addresses, phone numbers, employment information, work locations, family members, education, and photos. Social media websites may share more personal information than users expect, need, or realize. For example, a study by the University of Virginia cites that out of the top 150 Facebook applications, all of which are externally hosted, over 90% needed nothing more than publicly available information

---

[6] Joint Hearing on "The Collection and Use of Location Information for Commercial Purposes", February 24, 2010.

[7] "Guidelines for Secure Use of Social Media by Federal Departments and Agencies," Version 1.0, Federal CIO Council, September 2009.

[8] "Spear Phishers: Angling to Steal Your Financial Info", FBI, April 2009, https://archives.fbi.gov/archives/news/stories/2009/april/spearphishing_040109


DHS-001-02632-00011505/02/2022

DHS-001-02632-00011605/02/2022


from members in order to operate. In every case, however, users needlessly granted the applications total access to their account and therefore full access to all personal information.

When DHS employees join a social media website, they may identify themselves as DHS employees. Their self-identification creates a DHS ***Internet footprint,*** which is valuable information to adversaries. As more Federal employees self-identify on social media websites, the Federal footprint on social networking will grow, creating a target-rich environment to help adversaries target specific individuals to launch various social engineering attacks.

To learn personal information about an individual, an attacker can express a common interest in a topic and build a trust relationship with the victim. This positions the attacker to influence the victim's friends and co-workers or even to collect sufficient information to pose as the victim, providing an easy avenue for penetrating the trust of the Department or of other DHS personnel.

High-profile Federal employees with greater name recognition are an especially prime target for a social engineer seeking to exploit trust relationships in social networks.

### 3.2.3 Web Application Attacks

Malicious content on social networking sites is easy to disguise as valid content. Developers of user-generated games and applications on some sites have the option of going through an approval process, but the application's code is not always locked in the state in which it was submitted for approval. This creates a situation in which apparently vetted software can be injected with malicious code at a later time.

Finally, while a hijacked personal social media account may be annoying and personally costly or embarrassing, the hijacked account of a Federal user or a hijacked Federal account can have more serious implications. Unauthorized posts, tweets or messages may be seen by the public as official messages, or may be used to spread malware by encouraging users to click links or download malware and unwanted applications.


DHS-001-02632-00011605/02/2022

DHS-001-02632-00011705/02/2022


## 4.0 BEST PRACTICES FOR SOCIAL MEDIA USE

Online activities often blur the line between individuals' personal and professional lives. Real-world social and business rules have counterparts in digital environments. DHS employees or contractors, in or outside of the workplace, may affect their job performance, the performance of others, or DHS business interests, so they are a proper audience for best practice guidance. The following guidelines are intended to assist DHS employees and contractors in protecting their personal information and reputation while interacting online. These best practices are based on guidelines established by other Federal and commercial organizations.

### 4.1 Personal Use of Social Media

Use social media only on personal time using your personal computer and email account. You should not be logged onto external social networking sites while at work.

### 4.2 Never Post Classified or Sensitive Information

Posting classified or sensitive information on a social media site will lead to significant adverse action and penalties. DHS Management Directive No. 11042.1, "Safeguarding Sensitive But Unclassified (For Official use Only) Information" establishes DHS policy regarding the identification and safeguarding of sensitive but unclassified information originated within DHS, and other sensitive but unclassified information received by DHS from other Government and nongovernment activities. Do Not Communicate DHS Policies

### 4.3 Never Speak for the Department without Authorization

Never answer questions or make statements about or on behalf of DHS on a social networking site without explicit authorization from the DHS Office of Public Affairs, the DHS Office of General Counsel, or their Component equivalent.

### 4.4 Avoid Posting Personal Information

Limit the amount of personal information you post to social networks. Avoid posting personal information such as your home address, personal phone numbers, or details about your schedule or routine. This type of information gives cybercriminals the baseline they need for more targeted activities. Assume that anything you post to a social network can be seen by anyone and act accordingly. Also be wary of the type of information — including photographs — that you post about your friends and family, since that information can put them at risk.

### 4.5 Use Privacy and Security Settings

When accessing social networking sites, you can limit disclosure by using the site's Privacy settings. The default settings for some sites may allow anyone to see your profile. You can customize your settings to restrict access to only certain people. Also be aware of any changes to the site's privacy or security options. For example, Facebook is constantly improving user privacy settings that users should be aware of and implement as soon as possible[9]. Users should

[9] "Facebook Privacy: 10 Settings to Check", Information Week, June 5, 2014, http://www.informationweek.com/software/social/facebook-privacy-10-settings-to-check/d/d-id/1269438


DHS-001-02632-00011705/02/2022

DHS-001-02632-00011805/02/2022


monitor the privacy policies for social networking sites as they change often and without warning. Remember though, there is a risk that even private information can be exposed, so do not post anything that you would not want the public to see.

### 4.6 Be Wary of Location-Based Services

Be aware of privacy and security issues when using location-based services (LBS). LBS offers many conveniences such as keeping track of family and friends, getting directions, finding restaurants, and assisting in law enforcement. But LBS may make information about your location accessible to unintended recipients. Employees should understand that use of LBS introduces significant privacy and personal security risks with their use. The most common example is using a location check-in service (for example, Foursquare). If you check in from your couch at home, the precise Global Positioning System (GPS) coordinates of your couch are published. If you later check in from your office, it can be seen that you are no longer at your home, which is now an excellent target, and your own personal security can be compromised.

Carefully consider any request by any application to allow use of your location or any other personal information. In Snapchat and in other applications that can show your location or that of your contacts, always use a "ghost" mode that disallows showing your location. You should also be aware that this information may leak unintentionally. For example, smartphones can attach GPS coordinates to pictures you take. Posts made to social media sites such as Facebook or Twitter may also contain this detailed geo-location data that could also compromise your personal security and possibly your workplace security. The location attached to the picture may be metadata that is uploaded without your knowledge.

Be sure to examine your phone's privacy, security, and location settings to ensure that GPS coordinates are not automatically associated with LBS. Be sure never to check in from sensitive locations and avoid establishing patterns when possible.

### 4.7 Use Strong Passwords

Protect your account with passwords that cannot be easily guessed. Avoid using passwords such as your dog's name, the word "password" plus a digit, or your favorite sports team name.

A strong password resists guessing. Hackers and computer intruders use automated software as a way to submit hundreds of guesses per minute to access your account. These software tools are called 'dictionary' or 'brute force repetition' tools, because they will use English dictionaries to sequentially guess your password. These password-guessing tools can submit up to 1000 attempts per minute. The less that your password resembles regular word patterns, the longer it will take for a repetition tool to guess it.

These password variations below purposely avoid using complete English word patterns. Passwords that use combinations of characters that include numerals, symbols, and capital letters as well as lower case letters will create an exponentially longer task for attackers using dictionary programs and brute force.

Do not use the same password for multiple applications.

Even strongly constructed passwords are vulnerable to keystroke loggers and password cracking tools. In the final analysis, passwords do little to deter a determined attacker.


DHS-001-02632-00011805/02/2022

DHS-001-02632-00011905/02/2022


According to NIST (National Institute of Standards and Technology), a strong password should contain no fewer than 12 characters, a rule adopted by the U.S. government in 2007 and further defined in the U.S. Government Configuration Baseline. Admin passwords should be 15 characters. Readers may sigh at those lengths, but they have been the recommended minimum for half a decade. Anything shorter is not considered secure.

### 4.8 Be Suspicious about Installing Applications

Applications from social media sites are very often given complete access to your account—not just to what is necessary for the application to run. "Quizzes" are also problematic. For example, Facebook users taking quizzes can reveal far more personal information to the applications than they realize. This is mostly due to the fact that Facebook's default privacy settings allow access to all your profile information whether or not your profile is set to "private."

Even if you do not take quizzes yourself, your profile information may be revealed when one of your friends takes a social media or Internet quiz. Almost everything on your profile, even if you use privacy settings to limit access, is available to the quiz.

### 4.9 Be Wary of All Links

Vigilance is the best defense against phishing. Phishing scams can arrive in e-mails that look as though they come from real companies or trusted individuals. For example, you may receive an e-mail message announcing that your bank account will be closed unless you confirm your personal identification number, or that you need to provide your credit card information to confirm an order, or requesting verification of your social security number for billing purposes. Legitimate companies do not ask for your account or personal information via e-mail. To find out whether the message is legitimate, contact the company directly by telephone or letter using contact information from a trusted source, such as your account statements.

Never reply to suspect emails or click on any links they contain. This could expose you to clickjacking, in which a web page will trick you into performing undesired actions by clicking on concealed buttons or links that are on a web page hidden by the visible one. For example, the page may list what appears to be a valid DHS web page address, such as www.dhs.gov; however it hides the link to a web site set up by a cybercriminal. To find out whether the message is legitimate, contact the sending company directly by telephone or letter using data from a trusted source, such as your account statements or the back of your credit/debit card. Another way to verify the validity of the web page is, instead of clicking on an embedded link, manually enter the URL into the navigation bar of your web browser to avoid clickjacking.

Phishing attempts can also come in Twitter "tweets", Facebook wall postings, videos, or pictures sent via email. Get into the habit of not clicking on hyperlinks, especially those for videos or news-related events from unfamiliar sources and senders. In many cases, these are linked to phishing and social engineering attacks.

### 4.10 Have No Expectation of Privacy

Assume that your thoughts are in the public domain. Remember that social networking sites are generally public and permanent, even if you delete the information you posted. You should understand the security and privacy features available for the social networking sites you use,


DHS-001-02632-00011905/02/2022

DHS-001-02632-00012005/02/2022


and exercise discretion and common sense. Most social networks offer settings to keep profiles private and restrict access to personal photographs or other personally identifiable details; however, opting for privacy does not guarantee that others will not see your content. Content can be forwarded or hacked.

Facebook has found itself at the center of privacy breakdown controversies numerous times, and confusing Twitter interfaces have resulted in private messages being inadvertently posted to public feeds. Hackers can force access and friends can forward your content to others. In short, do not post anything that you do not want the public to see.

### 4.11 Protect Your Privacy

Do not share personal or contact information about your family, friends, co-workers, clients, or businesses without their explicit consent. Do not post or tag pictures of family, friends, co-workers, clients, or business without their consent. Respect the privacy of others at all times. Always protect your PII.

### 4.12 Be Professional

If you identify yourself as a DHS employee or have a public-facing position so that your DHS association is known to the general public, ensure that your profile and related content are consistent with how you wish to present yourself as a DHS professional, even if the information is of a personal and unofficial nature. Ensure that all your posts and interactions are consistent with the public trust associated with your position, and conform to existing standards such as "Standards of Ethical Conduct for Employees of the Executive Branch."

If you establish online profiles, you may provide your DHS title and contact information. You may also indicate that DHS is your employer, and you may describe your past and present job responsibilities (as you would on your resume) if you do not disclose any DHS sensitive information or the personal information of others.

### 4.13 Use Disclaimers

Be aware of your DHS association in online social networks. If your profile reveals your employment relationship with DHS, you should include a disclaimer stating that your activity and posts represent your personal opinions and do not represent those of DHS. An example of an appropriate disclaimer is "The postings on this site are my own and do not represent the positions, strategies, or opinions of the Department of Homeland Security."

### 4.14 Be the First to Respond to Your Own Mistakes

If you make an error, be up front about your mistake and correct it quickly. In a blog, if you choose to modify an earlier post, make it clear that you have done so.

### 4.15 Be Yourself

Do not forge or manipulate identities in your posts in an attempt to disguise, impersonate, or misrepresent your identity or affiliation with any other person or entity.


DHS-001-02632-00012005/02/2022

DHS-001-02632-00012105/02/2022


### 4.16 Avoid Being Offensive

Do not post defamatory, libelous, vulgar, obscene, abusive, profane, threatening, racially and ethnically hateful, or otherwise offensive or illegal information or material.

### 4.17 Do Not Breach Trademarks

Do not use any word, logo, or other mark that would infringe on a trademark, service mark, certification mark, or other intellectual property rights of the owners of such marks without the permission of such owners.

### 4.18 Respect Copyright, Fair Use, and Financial Disclosure Laws

Do not post any information or other material protected by copyright without the permission of the copyright owner. Also, consider using a Creative Commons license to protect your own work. Creative Commons offers a flexible copyright model through a collection of free copyright licenses written in plain language. Creators can select several of these licenses to communicate which rights they reserve, and which they waive, when their intellectual property is used by others. Wikipedia is one of the most notable web-based projects using a Creative Commons license. See www.creativecommons.org for additional details.

### 4.19 If in Doubt, Seek Guidance

Seek guidance from the DHS Office of Public Affairs or the DHS Office of General Counsel, or Component equivalent, prior to publicly sharing any personal opinions or statements based on your role within DHS. Those with leadership responsibilities, by virtue of their position, especially must understand that personal thoughts they publish, even in clearly personal venues, inadvertently may be interpreted as expressions of official DHS positions. They should assume that their co-workers, employees, and those outside of DHS will read what they have written.


DHS-001-02632-00012105/02/2022

DHS-001-02632-00012205/02/2022


## 5.0 UNOFFICIAL INTERNET POSTING GUIDELINES[10]

Department of Homeland Security (DHS) personnel who post content about DHS on the Internet are responsible for ensuring that any information disclosed (including personal comments) is accurate and appropriate. DHS personnel should keep in mind how their posts will reflect upon themselves and their organization, and also be aware that some individuals and groups use public networking forums to gain information that will help them advance their own causes or agendas at the expense of others. DHS personnel who engage in unofficial posting on the Internet should observe the following guidelines:

(1) You may not release DHS e-mail addresses, telephone numbers, or fax n umbers not already publicly released. You may not release the content manager's or content provider's work contact information.

(2) You may not post or disclose the existence of internal DHS documents or information that DHS has not officially released to the public. This policy applies no matter you obtained the information. Examples include, but are not limited to, the following: memos, e-mails, meeting notes, articles for publications, white papers, Public Affairs guidance, and all pre-decisional materials. Do not release any For Official Use Only (FOUO) information or PII in unofficial Internet posts.

(3) You, as a DHS Federal employee or contractor, are always responsible for adhering to DHS policies concerning information security, physical security, and to the Privacy Act in all forms of communication. Unauthorized disclosure of protected information, including sensitive but unclassified (SBU) information may result in disciplinary action.

(4) You may not release information about or pertaining to another DHS employee. Release of classified, operational, proprietary, law enforcement sensitive, or investigatory information is not authorized.

(5) Any photo, video, or sound recording made by DHS personnel of an official DHS function is considered official DHS media. Newsworthy items should be released officially to news organizations and other media with the knowledge and approval of OPA or the Component office of public or external affairs before being posting unofficially.

(6) DHS-related media made by DHS personnel while they are in a non-working status in public areas, (e.g., photo of a U.S. Coast Guard cutter taken from a public pier while on liberty) is considered private imagery and is not subject to these guidelines.

(7) Use of official or protected DHS statements or symbols (for example, the DHS logo) must be approved OPA. This prevents the impression of official or implied endorsements.

(8) You may not release, intentionally or unintentionally, location-based (geospatial) information related to a DHS mission. This prohibition includes, for example, disclosing the location of the employee and/or DHS assets at a particular point in time. ***Auto-***

[10] Based on US DHS, ALCOAST 548/08, COMDTNOTE 5700. SUBJ: SOCIAL MEDIA - UNOFFICIAL INTERNET POSTS.


DHS-001-02632-00012205/02/2022

DHS-001-02632-00012305/02/2022


***tweeting,*** geospatial coordinates while driving, or reporting via a location-based social media tool such as ***Foursquare*** are examples of violations of this guideline.

(9) As with other forums of personal public engagement, DHS personnel shall avoid off-duty behavior that negatively impacts, or conflicts with, their ability to execute their duties for DHS, such as the prohibited personal conduct described in Standards of Ethical Conduct for Employees of the Executive Branch.


DHS-001-02632-00012305/02/2022

DHS-001-02632-00012405/02/2022


## GLOSSARY

Terms commonly used in relation to social media are defined below.

| Term | Explanation |
|---|---|
| Blog | An abbreviation of "weblog." A blog is a web-based forum where individual content providers contribute regular entries or "posts" in the form of commentary, descriptions of events, or other materials on the website. Visitors to the blog may add their own comments to posts. Blogs may be "moderated" with the blog owner overseeing removal of any objectionable material, or they may be "unmoderated," in which case there is no control over the posted material. |
| Clickjacking | A malicious technique of tricking a user into revealing confidential information or of taking control of their computer when they click links on seemingly harmless web pages. On a clickjacked page, the attacker shows a set of dummy buttons or links, then loads another page over it in a transparent layer. Users think they are clicking on the visible page while they are actually performing actions on the hidden page which the users never intended, such as changing privacy settings on a social networking site or following someone on Twitter. |
| Commercial/Third Party Social Media | Social media hosted on servers over which DHS has no control. This includes proprietary social networking sites such as Facebook and MySpace, as well as collaboration services such as Wikipedia, BlogSpot, and Delicious. |
| Content Manager | Any individual designated to manage web content for DHS or a Component. The duties of the Web Content Manager include ensuring compliance with accessibility standards for persons with disabilities. This individual is the organization's primary point of contact for Web issues.[11] |
| Content Provider | Any individual who creates content for publication to DHS websites.[12] |
| Enterprise Network | The communications backbone that interconnects every computer and associated device at every location under the jurisdiction of an organization, such as DHS. |
| External Hosting | Provision by an external organization or company of access, on a fee-per-service basis, to the equipment, technology and support to needed to establish and run a website, as opposed to an organization's using its own in-house resources. |
| Farming | See Pharming |
| Fishing | See Phishing |

[11] DHS 4300A, IV Definitions, J

[12] DHS 4300A, IV Definitions, K


DHS-001-02632-00012405/02/2022

DHS-001-02632-00012505/02/2022


| Term | Explanation |
|---|---|
| Foursquare | A location-based social networking website and application for mobile devices. Users "check in" or report their location by accessing a mobile website, text messaging or a device-specific application, so that their whereabouts can be discovered by others. Foursquare also incorporates elements of a game by awarding users points for being the first to visit a new place, and for adding new information about the locations they visit. |
| Hacker | A person who uses their proficiency with electronics, computers and/or programming skills to gain illegal access to others' digital resources, including personal handheld devices, files, computers and networks. |
| Internet footprint | The collective activities and behaviors recorded as an individual interacts in a digital environment, including device usage, system logins and logouts, website visits, files, transmitted emails, and posted messages. "Passive footprints" are created when data are collected about individuals' activities without any deliberate action on their part, such as tracking which products customers are visiting on a vendor's website regardless of whether purchases occur. "Active footprints" are created when personal data is released intentionally by individuals for the purpose of sharing information with others online. Footprints are sometimes used as a rough measure of an individual's "web presence." |
| Keystroke loggers | Also called a "keylogger," It it is can be a hardware device or a program that monitors and records each keystroke a user types on a computing device's keyboard. Although sometimes used for legitimate purposes, such as diagnostics or monitoring a child's Internet activity, a more typical use of keystroke loggers is for the unauthorized capture of security credentials such as passwords and personal identification numbers. |
| Malware | Derived from the phrase "malicious software," this term is a generic term for any program whose purpose is to cause harm to a computer system. Typically, malware is installed without the user's knowledge or consent, although it is often packaged with other software the user does in fact choose to install or download. Viruses and worms are examples of malware. |
| Mashup | A web page or application that enables the fast, easy combination of data and/or functionality from multiple sources to create a new, enriched result that was not necessarily the reason for producing the original sources. Most mashups use publicly-accessible resources. For example, a mashup might superimpose on a Google map of a neighborhood the average housing prices drawn from a city assessor's online database. |
| Metadata | Information about the meaning of other information. Metadata can describe or summarize key attributes of a piece of information to facilitate finding that information when needed. An example of metadata is a time stamp that specifies when a piece of information was created. |
| Micro-Blog | Extremely short blog posts similar to text messaging. The messages can either be viewed by anyone or by a restricted group that is chosen by the user. Twitter, a popular micro-blog client, allows posts of up to 140 characters to be uploaded and read using instant messaging or mobile devices via text messaging. |


DHS-001-02632-00012505/02/2022

DHS-001-02632-00012605/02/2022


| Term | Explanation |
|---|---|
| Operational Use | The 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. |
| Password Attack | An attempt to obtain a legitimate user's password. Hackers can use common password lists, dictionaries, cracking programs, and password sniffers in password attacks. |
| Personally Identifiable Information (PII) | Any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual regardless of whether the individual is a United States citizen, legal permanent resident, or a visitor to the United States. Examples of PII include, but are not limited to name, date of birth, mailing address, telephone number, Social Security Number, email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), IP addresses, biometric identifiers (e.g., fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic), and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual. Also, Sensitive Personally Identifiable Information (SPII) that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual.[13] |
| Pharming | An action whereby a hacker subverts a user's attempt to visit a legitimate website by instead redirecting themr to a counterfeit or "spoofed" website. The spoofed site is designed to trick users into revealing personal information such as usernames, passwords, and account information. |
| Phishing | An attempt to fraudulently acquire a user's personal information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication. Phishing is common in e-mail and instant messaging. For example, you might receive an e-mail that appears to come from an official at your bank that instructs you to "confirm" your Internet banking credential by clicking on a link. The "spoofed" website to which you would be directed would capture your credentials in order to enable a third party to access and withdraw all funds from your bank account. |

[13] DHS 4300A, IV Definitions, H


DHS-001-02632-00012605/02/2022

DHS-001-02632-00012705/02/2022


| Term | Explanation |
|---|---|
| Sensitive Personally Identifiable Information (SPII) | Sensitive PII is personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII requires stricter handling guidelines because of the increased risk to an individual if the data are compromised. SPII includes Social Security Number, driver's license or State ID number, passport number, Alien Registration Number, fiancial acocunt number, and biometric identifisers. |
| Social Bookmarking | A Web-based service where users create and store links to information on topics of particular interest to them. Although web browsers have the ability to bookmark links to "favorite" pages, those links are tied to an individual browser on a single computer. Social bookmarking, by contrast, stores links in an online account which can be made public. These bookmarks can be shared and discovered by others who are interested in finding information on similar topics. Examples of social bookmarking sites include Delicious, Digg, and Reddit. |
| Social Engineering | The act of deceiving or tricking people into performing actions or divulging confidential information, rather than obtaining such information by breaking in or using technical means. For example, someone posing as a help desk representative might telephone you and claim to be diagnosing a connection problem; the caller requests that you verify your login ID and password or other personal information so it can be checked against the items on file. |
| Social Media | Internet-based applications that build on the foundations of Web 2.0 to allow the creation and exchange of user-generated content. Social media can take many different forms, including but not limited to Web-based communities and hosted services, social networking sites, video and photo sharing sites, wikis, blogs, podcasts, virtual worlds, social bookmarking, and many emergent technologies. |
| Social Networking Services | Web-based services that connect people who share the same interests and/or activities, or who are interested in exploring the interests and activities of others. Social networking services provide a variety of ways for users to interact. For example, Facebook is used as a place to socialize with friends, whereas LinkedIn caters to those who wish to make professional connections. |
| Spam | Unsolicited or undesired electronic messages. Spam includes legitimate advertisements, misleading advertisements, and phishing messages— any unsolicited message can be spam. |
| Spear Fishing | See Spear Phishing |
| Spear Phishing | A technique by which the attacker generates an e-mail message or prompts linking to a website. The attack's target is a specific individual or small group. The goal is to convince the targets to take action, which gives the attacker access to their system by presenting them with text, images, or URLs that they could actually expect and therefore mistake for legitimate. |


DHS-001-02632-00012705/02/2022

DHS-001-02632-00012805/02/2022


| Term | Explanation |
|---|---|
| Spoofed Website | An impostor website that mimics a real company's website in order to steal personal information from site visitors. Victims are often directed to these spoofed sites through phishing e-mails. Spoofed sites can look extremely convincing, but often contain small flaws such as spelling errors or "slightly wrong" logos. |
| Spyware | Any software that covertly gathers users' information through their computing devices and/or their Internet connection without their knowledge for unauthorized use. Spyware applications are typically hidden components that users inadvertently download together with legitimate material. Spyware may gather information such as e-mail addresses for advertising purposes, or even passwords and credit card data. |
| Trusted Internet Connections (TIC) | A DHS initiative implementing OMB Memorandum M-08-05, to optimize and standardize the security of individual external network connections including connections to the Internet that are currently in use by the Federal Government. A "TIC" is a physical location an agency uses to meet the objectives of the TIC Initiative. |
| Twitter | A social networking micro-blogging service that enables its users to send and read other users' messages, called "tweets." Users ("followers") may subscribe to ("follow") other users' tweets. Twitter is sometimes called the "Short Message Service of the Internet" because of the compatibility of its interface with smart phones. Tweets are limited to 140 characters. |
| Uniform Resource Locator (URL) | In computing, the identifier that specifies where a resource is located and the mechanism for retrieving it. The best-known example of the use of URLs is for the addresses of web pages on the Internet, such as www.dhs.gov. |
| Video Sharing | Websites on which users post video they have taken for others to view and comment on. Such sites allow viewers to "embed" or display others' video on their own sites. YouTube is probably the most widely known video sharing site. |
| Virtual world | Online communities where users or their digital representations (called "avatars") can socialize, connect, and interact with one another using text and voice chat. The term is used more specifically to refer to an online community such as Second Life that features a computer-based simulated three-dimensional environment where users can not only interact but also create and use virtual objects. |
| Virus | A form of malware that can copy itself and spread from one computer to another in the form of executable code when its host is taken to a target computer. For example, a user might send an infected file over a network, or carry it on a removable medium such as a CD or thumb drive, or the virus might send an instant message to all the contacts on the infected machine which, when opened by the addressee, infects the recipient's computer. While some viruses are benign, often a virus will cause a computer to "hang," rendering it inoperable by corrupting and/or disabling key operating system files and tools. |


DHS-001-02632-00012805/02/2022

DHS-001-02632-00012905/02/2022


| Term | Explanation |
|---|---|
| Web 2.0 | Although there is no agreed-upon definition of the term *Web 2.0*, it term generally refers to the move toward a more social, interactive, collaborative, and responsible Web. It can be characterized by capabilities and tools facilitating social media dialog. |
| Whaling | Phishing attacks targeted at high-ranking personnel in an organizational hierarchy, such as Chief Executive Officers (CEO) and other top executives. |
| Widget | A self-contained tool that can be embedded in a website or program to deliver a single-purpose service, such as displaying the latest news and weather, maps, or photos, or allowing a user to play interactive games with other website visitors. Users of social networking sites often take advantage of widgets as an easy way to make their sites more interesting to visitors; care must be taken, however, since hackers often use widgets as malware entry points. |
| Wiki | A technology for creating collaborative websites. From the Hawaiian word meaning "quick," a wiki is a collection of Web pages that encourages users to contribute or modify the content. By using a simple Web interface, a community can collaborate to develop a document or Web page, no matter where the members of the community are located. By far the best-known wiki is Wikipedia, a multilingual, web-based, free content encyclopedia project. |
| Worm | Self-replicating malware that uses a computer network to send copies of itself from one computer system to another. Worms can cause excessive network traffic and other malicious disruptions such as file deletion and sending junk mail to every e-mail address it discovers on every computer system as it spreads throughout a network. |


DHS-001-02632-00012905/02/2022

DHS-001-02632-00013005/02/2022


# REFERENCES


### Federal Regulations

"Standards of Ethical Conduct for Employees of the Executive Branch," 5 CFR 2635

### DHS Directives)

Directive 110-01, "Privacy Policy for the Operational Use of Social Media," June 8, 2012

MD No. 11042.1, "Safeguarding Sensitive But Unclassified (For Official Use Only) Information," January 6, 2005

Directive 139-05, "Office of Accessible Systems and Technology," January 29, 2016

MD 262-04, "DHS Web (Internet, and Extranet Information)" (Revision 00), April 13, 2015

MD 4600.1, "Personal Use of Government Office Equipment," April 14, 2003

MD 4900, "Individual Use and Operation of DHS Information Systems/Computers," undated DHS Privacy Office Publications

MD 110-01, "Privacy Policy for the Operational Use of Social Media," June 8, 2012

Instruction 110-01-001, "Privacy Policy for Operational Use of Social Media," June 8, 2012

### DHS Privacy Office Publications

"DHS Privacy Impact Assessment for Use of Social Networking Interactions and Applications," DHS Privacy Office, April 2010

"Government 2.0: Privacy and Best Practices: Report on the DHS Privacy Office Public Workshop, DHS Privacy Office, November 2009

### Congressional Proceedings

Joint Hearing, "Collection and Use of Location Information for Commercial Purposes," U.S. House of Representatives, Energy and Commerce Committee, Subcommittee on Communications, Technology and the Internet, and Subcommittee on Commerce, Trade, and Consumer Protection, February 24, 2010

### Other Government Sources

"CIO Council Guidelines for Secure Use of Social Media by Federal Departments and Agencies," Federal CIO Council, Version 1.0, September 2009

"Communications Act of 1934", Federal Communications Commission, https://transition.fcc.gov/Reports/1934new.pdf

"GSA Social Media Policy and Handbook," CIO 2106.1, General Services Administration, July 17, 2009

"Hatch Act Social Media and Email Guidance," Office of Special Counsel, https://osc.gov/Pages/Hatch-Act-Social-Media-and-Email-Guidance.aspx

"New Media and the Air Force," U.S. Air Force Public Affairs Agency, Emerging Technology Division, April 6, 2009

"Social Media and the Federal Government: Perceived and Real Barriers and Potential Solutions," Federal Web Managers Council," December 23, 2008

"Social Media Security Mitigations," Version 1.1, U.S. Centers for Disease Control and Prevention, December 3, 2009

### Articles and White Papers

"Security Threat Report: 2010," Sophos Group, 2010



DHS-001-02632-00013005/02/2022

DHS-001-02632-00013105/02/2022


"The Application Usage and Risk Report: An Analysis of End User Application Trends in the Enterprise," Palo Alto Networks, Fall 2009

"Location-based Social Media Has Legal Implications for Employers & Employees," www.thesocialworkplace.com, April 16, 2010

"Location-Sharing Technologies: Privacy Risks and Controls", Carnegie Mellon University, February 1010, http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf

"Spear Phishers: Angling to Steal Your Financial Info", FBI, April 2009, https://archives.fbi.gov/archives/news/stories/2009/april/spearphishing_040109


DHS-001-02632-00013105/02/2022

DHS-001-02632-00013205/02/2022

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



# PRIVACY THRESHOLD ANALYSIS (PTA)

**This form is used to determine whether a Privacy Impact Assessment is required.**

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSConnect and directly from the DHS Privacy Office via email: pia@hq.dhs.gov, phone: 202-343-1717.

DHS-001-02632-00013205/02/2022

DHS-001-02632-00013305/02/2022

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



# PRIVACY THRESHOLD ANALYSIS (PTA)

## SUMMARY INFORMATION

| | | | |
|---|---|---|---|
| **Project or Program Name:** | **ClearView AI** | | |
| **Component:** | Immigration and Customs Enforcement (ICE) | **Office or Program:** | Homeland Security Investigations (HSI) Child Exploitation Investigations Unit (CEIU) |
| **Xacta FISMA Name (if applicable):** | **N/A** | **Xacta FISMA Number (if applicable):** | **N/A** |
| **Type of Project or Program:** | **Pilot** | **Project or program status:** | **Pilot** |
| **Date first developed:** | Click here to enter a date. | **Pilot launch date:** | **June 18, 2019** |
| **Date of last PTA update** | **N/A** | **Pilot end date:** | **June 18, 2020** |
| **ATO Status (if applicable)** | **Not started** | **ATO expiration date (if applicable):** | **N/A** |

## PROJECT OR PROGRAM MANAGER

| | | | |
|---|---|---|---|
| **Name:** | (b6)(b7c) | | |
| **Office:** | **Child Exploitation Investigations Unit** | **Title:** | Section Chief |
| **Phone:** | **503-209-**(b6)(b7c) | **Email:** | (b6)(b7c)e.dhs.gov |

## INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

| | | | |
|---|---|---|---|
| **Name:** | (b6)(b7c) | | |
| **Phone:** | **703-407-**(b6)(b7c) | **Email:** | (b6)(b7c)@associates.ice.dhs.gov |

DHS-001-02632-00013305/02/2022

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



## SPECIFIC PTA QUESTIONS

**1. Reason for submitting the PTA: New PTA**

The HSI Cyber Crimes Center (C3) is submitting this PTA to document Clearview AI, a new facial recognition service C3 will use to identify perpetrators and victims pictured in child exploitation materials.

C3 delivers computer-based technical services to HSI components to support domestic and international investigations into cross-border crime. C3 is comprised of the Cyber Crimes Unit (CCU), the Child Exploitation Investigation Unit (CEIU), and the Computer Forensics Unit (CFU). Specifically, within CEIU, is the Victim Identification Lab (VIL). The VIL conducts examinations of newly-discovered images of child pornography, where the subject's and victim's identities are not known to law enforcement. (b) (7)(E)

(b) (7)(E)

Clearview is a web-based service that acts as a search engine of publicly available images. Clearview pulls and compiles publicly available images from across the internet into a proprietary image database to be used in combination with Clearview's facial recognition technology. Clearview boasts a 98.6% accuracy rate for its algorithm and an image gallery greater than 1 billion images. A system's accuracy rate measures the algorithm's ability to match an individual in two images successfully. The images are unconstrained and may have multiple individuals in the image. All images are collected via simple searches, and no social media terms of service or privacy settings are violated in the collection of images.

Clearview's stated accuracy is self-certified and has not yet been independently confirmed by the National Institute of Standards and Technology (NIST) Face Vendor Recognition Test[1]. The software allows HSI to input any facial image that appears in an investigation, regardless of quality or angle, into the program. Personnel at CEIU isolate facial images from exploitative material and manually upload them into the Clearview portal. CEIU may crop, rotate, or resize an image prior to being uploaded in Clearview to ensure the subject face is the focal point. ICE Privacy intends to work with HSI on developing Rules of Behavior (ROBs) and/or Standard Operating Procedures (SOPs) for the use of this tool to the extent that such use is permitted.

(b) (7)(E)

Clearview allows for customized user access restrictions, audit logs, and "splash screens" that can present rules of behavior for a user. The parameters of the restrictions and contents of the rules of behavior are being developed during the pilot. Clearview does not interact with any ICE systems at any

[1] *See* https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt.

Homeland Security

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



time.(b) (7)(E)
(b) (7)(E)

At the time of upload, CEIU is able to set the retention schedule for the image. CEIU sets the retention schedule to immediately delete the image in Clearview's database as soon as the facial recognition algorithm is complete. Clearview has the ability to store a HashID of the results of the algorithm that is run on an image. The HashID cannot be used to recreate a facial image, but rather informs the Clearview program what to look for in its gallery to find a match. CEIU can opt for the HashID to remain on Cleaview servers to run against new images incorporated into their database. If the HashID hits on a new image, CEIU is then alerted.

(b) (7)(E)

CEIU investigators will thoroughly check information derived from the open source site against government and public databases to either validate or eliminate candidates prior to generating leads to send to the field for additional investigation. Clearview returns will not be used as a positive identification nor will they be used for probable cause. They are merely a tool to provide possible suspects and will require additional investigative steps to verify identities.

Clearview searches are treated as equivalent to open web searches in that the entirety of returned search results are not saved in CEIU systems. CEIU will only collect and document salient results as they pertain to the investigation. If CEIU concludes that certain photographs returned from Clearview are not relevant to an ongoing investigation, then the photographs will not be maintained in any ICE repository.

CEIU uses Clearview to further existing investigative leads or ongoing investigations, and any pertinent information collected from a Clearview search is handled in the same manner as all other evidence obtained through open source research.(b) (7)(E)
(b) (7)(E)

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



# (b) (7)(E)

| | |
|---|---|
| **2. Does this system employ any of the following technologies:**<br>*If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.* | ☐ Closed Circuit Television (CCTV)<br>☒ Social Media<br>☐ Web portal[2] (e.g., SharePoint)<br>☐ Contact Lists<br>☐ None of these |

| | |
|---|---|
| **3. From whom does the Project or Program collect, maintain, use, or disseminate information?**<br>*Please check all that apply.* | ☐ This program does not collect any personally identifiable information[3]<br>☒ Members of the public<br>☒ DHS employees/contractors (list components):<br>ICE<br>☐ Contractors working on behalf of DHS<br>☐ Employees of other federal agencies |

**4. What specific information about individuals is collected, generated or retained?**

CEIU uploads unidentified images of perpetrators and victims from child exploitation material. Since these images are unidentified, these images are linked to case files (i.e. case file number) and not personal identifiers(b) (7)(E)

Clearview returns images from open sources on the internet that are determined by Clearview to be

[1] Informational and collaboration-based portals in operation at DHS and its components that collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are "members" of the portal or "potential members" who seek to gain access to the portal.

[2] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

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



| | |
|---|---|
| similar to CEIU's uploaded images, as well as the URL of the website where the image was found. The image and the open source URL are the only information provided by Clearview AI. There is no individual PII associated with the image return. | |
| **4(a) Does the project, program, or system retrieve information by personal identifier?** | ☒ No.<br>☒ Yes. If yes, please list all personal identifiers used: photograph |
| **4(b) Does the project, program, or system use Social Security Numbers (SSN)?** | ☒ No.<br>☐ Yes. |
| **4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:** | N/A |
| **4(d) If yes, please describe the uses of the SSNs within the project, program, or system:** | N/A |
| **4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure?**<br><br>*For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?* | ☒ No. Please continue to next question.<br>☐ Yes. If a log kept of communication traffic, please answer the following question. |
| **4(f) If header or payload data[3] is stored in the communication traffic log, please detail the data elements stored.** | |
| N/A | |

| | |
|---|---|
| **5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems[4]?** | ☒ No.<br>☐ Yes. If yes, please list: |
| **6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?** | ☒ No.<br>☐ Yes. If yes, please list: |

[3] When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.

[4] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in Xacta.

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



| | |
|---|---|
| **6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?** | N/A |
| **7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?** | ☒ No.<br>☐ Yes. If yes, please list: |
| **8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals who have requested access to their PII?** | ☒ No. What steps will be taken to develop and maintain the accounting:<br>☐ Yes. In what format is the accounting maintained: |
| **9. Is there a FIPS 199 determination?[5]** | ☐ Unknown.<br>☒ No.<br>☐ Yes. Please indicate the determinations for each of the following:<br>Confidentiality:<br>☐ Low ☐ Moderate ☐ High ☐ Undefined<br>Integrity:<br>☐ Low ☐ Moderate ☐ High ☐ Undefined<br>Availability:<br>☐ Low ☐ Moderate ☐ High ☐ Undefined |

## PRIVACY THRESHOLD REVIEW

## (TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

| | |
|---|---|
| **Component Privacy Office Reviewer:** | (b6)(b7c) |

[5] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

DHS-001-02632-00013905/02/2022

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



| | |
|---|---|
| **Date submitted to Component Privacy Office:** | **June 27, 2019** |
| **Date submitted to DHS Privacy Office:** | **XXX** |

**Component Privacy Office Recommendation:**
*Please include recommendation below, including what new privacy compliance documentation is needed.*

The HSI Cyber Crimes Center (C3) is submitting this PTA to document Clearview AI, a new facial recognition service C3 will use to identify perpetrators and victims pictured in child exploitation materials. Clearview is a web-based service that acts as a search engine of publicly available images. Clearview pulls and compiles publicly available images from across the internet into a proprietary image database to be used in combination with Clearview's facial recognition technology. Clearview boasts a 98.6% accuracy rate and an image gallery greater than 1 billion images.

ICE's use of Clearview AI is privacy sensitive, requiring PIA coverage. DHS/ICE/PIA-045 Investigative Case Management System (ICM) PIA outlines the risk of utilizing intelligence products from public source databases in reports of investigation and should provide interim coverage for HSI's use of facial recognition technology. All candidate returns from Clearview's facial recognition service will be treated as investigative photographic data within ICM. All information derived from open source URL searches will be treated similarly to standard internet searches in ICM.

ICE Privacy will draft a PIA on its use of facial recognition services for transparency purposes.

Clearview AI requires SORN coverage because it retrieves information by a unique identifier. DHS/ICE-009 External Investigations SORN provides coverage for the use of PII, including photographs, to investigate violations of the law within ICE's jurisdiction. The forthcoming update to DHS/ICE-009 will provide further transparency on HSI's use of facial photographs for biometric purposes and collection of social media.

**(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)**

| | |
|---|---|
| **DHS Privacy Office Reviewer:** | Click here to enter text. |
| **PCTS Workflow Number:** | Click here to enter text. |
| **Date approved by DHS Privacy Office:** | Click here to enter a date. |
| **PTA Expiration Date** | Click here to enter a date. |

**DESIGNATION**

| | |
|---|---|
| **Privacy Sensitive System:** | Choose an item. If "no" PTA adjudication is complete. |
| **Category of System:** | Choose an item.<br>If "other" is selected, please describe: Click here to enter text. |
| **Determination:** | ☐ PTA sufficient at this time. |

DHS-001-02632-00013905/02/2022

DHS-001-02632-00014005/02/2022

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



| | |
|---|---|
| | ☐ Privacy compliance documentation determination in progress.<br>☐ New information sharing arrangement is required.<br>☐ DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies.<br>☐ Privacy Act Statement required.<br>☐ Privacy Impact Assessment (PIA) required.<br>☐ System of Records Notice (SORN) required.<br>☐ Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer.<br>☐ A Records Schedule may be required. Contact your component Records Officer. |
| **PIA:** | Choose an item.<br>If covered by existing PIA, please list: Click here to enter text. |
| **SORN:** | Choose an item.<br>If covered by existing SORN, please list: Click here to enter text. |
| **DHS Privacy Office Comments:**<br>*Please describe rationale for privacy compliance determination above.* | |
| Click here to enter text. | |

DHS-001-02632-00014005/02/2022

**From:** (b6)(b7c)
**Sent:** 28 Feb 2020 14:46:40 +0000
**To:** Holz, Jordan
**Subject:** FW: Clearview PTA
**Attachments:** PTA, ICE- ClearView, 20200228, toDHS .docx, Clearveiw Ai - Accuracy Test - Oct 2019.pdf, Code of Conduct.pdf, Clearview AI Marketing Materials.with Tax ID and pricing.pdf, Clearview Legal Memo.pdf, Clearview example search return.png

Find enclosed with supporting materials

Best,
(b6)(b7c)
Mobile: 202-870(b6)(b7c)

**From:** (b6)(b7c)
**Sent:** Friday, February 28, 2020 8:30 AM
**To:** (b) (6)
**Cc:** PIA <PIA@HQ.DHS.GOV>
**Subject:** Clearview PTA

Good Morning Hannah,
Please find enclosed the Clearview PTA. (b) (5)
(b) (5)
(b) (5) If you have any questions or if you'd like more information please let us know.

Best,
(b6)(b7c)
Privacy Analyst, J.D., CIPP/US/G
Office of Information Governance and Privacy
U.S. Immigration and Customs Enforcement
Desk: 202-732-(b6)(b7c)
Mobile: 202-87
Main: 202-732

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

Thanks!

(b6)(b7c)

(b)(7)(E)

**From:** DHS ESOC <DHSESOC@hq.dhs.gov>
**Sent:** Thursday, February 27, 2020 3:19 PM
**To:** ICE SOC (b) (7)(E) ice.dhs.gov>; (b6)(b7c) @associates.ice.dhs.gov>
**Subject:** Investigation Notification: Publish SEN - (Unconfirmed) (b) (7)(E)
(b) (7)(E)
**Importance:** High

(UNCLASSIFIED//FOUO)
**Department of Homeland Security (DHS)**
**Enterprise Security Operations Center (ESOC)**

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO).
It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid need-to-know without prior approval of an authorized DHS official.

**Investigation Number:** INV-2020-02-6274307 - Potential Privacy Spill

**Category**: Privacy Spill

**Criticality**: Unconfirmed

**PII Suspected:** Yes

**Classified Spill:** Yes

**Component Reporting**: DHS ESOC

**Components Requiring Remediation**: CBP; DC1; DC2; DHS ESOC; DHS HQ; FEMA; FLETC; ICE; CISA; OIG; S&T; TSA; USCG; USCIS; USSS

**Executive Summary**:

DHS ESOC is investigating the possible exposure of DHS data in the wake of the Clearview AI data breach, which was made public on February 26, 2020. OSI reports that a malicious actor "gained unauthorized access" to its list of customers, which may include DHS Components. No timeframe for the unauthorized access has been made public. ICE, CBP, and USSS are all known to have obtained the "free trials" that the company markets directly to law enforcement personnel, instead of via traditional procurement channels. ESOC is requesting that components provide information as to any use of

Clearview AI and/or possible exposure due to the breach.

https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

https://www.fox61.com/article/news/clearview-ai-has-billions-of-our-photos-its-entire-client-list-was-just-stolen/520-7eda551a-77e0-494a-a51f-1ca6d9d742cb

https://www.pymnts.com/news/security-and-risk/2020/facial-recognition-firm-clearview-ais-client-list-hacked/

Please visit the link below for more details:
https://ecop.dhs.gov/default.aspx?requestUrl=..%2fGenericContent%2fRecord.aspx%3fid%3d6274307%26moduleId%3d433

**Contact Information:**
**DHS Enterprise Security Operations Center (ESOC)**
**Phone: 1-877-347-1638 Option 2**
**Email: DHSESOC@hq.dhs.gov**
(UNCLASSIFIED//FOUO)

**From:** Holz, Jordan
**Sent:** 24 Jan 2020 19:21:43 +0000
**To:** (b6)(b7c)
**Cc:** (b6)(b7c)
**Subject:** FW: Privacy in the News: January 24, 2020

Forwarding this to all of you for awareness. This is a tool currently in use by HSI NSID for which there's considerable litigation.

I'm heading to a meeting until 3:15 but can discuss later this afternoon (or next week).

**Jordan Holz**
Privacy Officer
Office of Information Governance and Privacy
U.S. Immigration and Customs Enforcement
Desk: 202-732(b6)(b7c)
Mobile: 202-7
Main: 202-732

**From:** Lindner, David (b) (6)
**Sent:** Friday, January 24, 2020 2:20 PM
**To:** DANISEK, DEBRA Cantor, Jonathan Holz, Jordan (b) (6) RUCKER EDNA G (b) (6)
**Cc:** Vogel, Lindsay <Lindsay.Vogel@hq.dhs.gov>; Mathews, Scott <Scott.Mathews@HQ.DHS.GOV>; Holzer, James <James.Holzer@hq.dhs.gov>; CAPPARRA, MICHAEL V. <michael.v.capparra@cbp.dhs.gov>; ISRAEL, JASON A <jason.a.israel@cbp.dhs.gov>
**Subject:** RE: Privacy in the News: January 24, 2020

As we've discussed previously, I'd really like to talk to OGC about these free licenses that everyone is using these days. That used to be a huge no-no from a procurement law standpoint, but now they seem to utilize free trials Dept-wide.

David

**David Lindner, CIPP/G**
Senior Director, Privacy Policy and Oversight | U.S. Department of Homeland Security
(b) (6) DHS Privacy Website

**From:** DANISEK, DEBRA (b) (6)
**Sent:** Friday, January 24, 2020 2:18 PM
**To:** Cantor, Jonathan (b) (6) Holz, Jordan (b) (6) RUCKER EDNA G (b) (6)
**Cc:** Vogel, Lindsay (b) (6) Lindner, David (b) (6) Mathews, Scott (b) (6) Holzer, James (b) (6) (b) (6) (b) (6)
**Subject:** RE: Privacy in the News: January 24, 2020

CBP has terminated any relationship with Clearview. Per the NTC, they gave us a handful of free licenses that we have ceased using.

DD

**From:** Cantor, Jonathan (b) (6)
**Sent:** Friday, January 24, 2020 2:04 PM
**To:** DANISEK, DEBRA (b) (6) Holz, Jordan (b) (6) RUCKER EDNA G (b) (6)
**Cc:** Vogel, Lindsay (b) (6) Lindner, David (b) (6) Mathews, Scott (b) (6) Holzer, James (b) (6)
**Subject:** Fwd: Privacy in the News: January 24, 2020

And the legal circus begins against Clearview. The Illinois based lawsuit is likely a big deal. Facebook has been unable to get its BIPA lawsuit dismissed (the first item in Privacy in the courts).

Jonathan R. Cantor
Chief Privacy Officer (A)
Department of Homeland Security
(b) (6)

---

**From:** Cutshall, Charles (b) (6)
**Sent:** Friday, January 24, 2020 1:29:29 PM
**Subject:** Privacy in the News: January 24, 2020

# PRIVACY IN THE NEWS

## The One Privacy Article You Must Read This Week.

- **The Secretive Company That Might End Privacy as We Know It**
  https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

  *"Searching someone by face could become as easy as Googling a name. Strangers would be able to listen in on sensitive conversations, take photos of the participants and know personal secrets. Someone walking down the street would be immediately identifiable — and his or her home address would be only a few clicks away. It would herald the end of public anonymity."*

## Privacy in the Legislature.

- **Democratic senator presses facial recognition company after reports of law enforcement collaboration**
  https://thehill.com/policy/technology/479564-democratic-senator-presses-facial-recognition-company-after-reports-of-law

- **Like CCPA, But Make it Virginia: States Scramble to Introduce Data Privacy Legislation of Their Own**
  https://www.adamsandreese.com/news-knowledge/like-ccpa-but-make-it-virginia-states-scramble-to-introduce-data-privacy-legislation-of-their-own

  *"Virginia added itself to the ever-growing list of states considering such bills when the Virginia Privacy Act (VPA) was introduced to the General Assembly for consideration January 8."*

## Privacy in the Courts.

- **Supreme Court declines to hear Facebook facial recognition case**
  https://thehill.com/policy/technology/479126-supreme-court-declines-to-hear-facebook-facial-recognition-case

  *"The Supreme Court on Tuesday declined to take up a high-profile court battle over whether users can sue Facebook for using facial recognition technology on their photos without proper consent."*

- **Clearview AI Hit With Biometric Privacy Lawsuit**
  https://www.mediapost.com/publications/article/346121/clearview-ai-hit-with-biometric-privacy-lawsuit.html

- **IBM Hit With Lawsuit Claiming Image Use for Facial Recognition**
  https://news.bloomberglaw.com/privacy-and-data-security/ibm-hit-with-lawsuit-claiming-image-use-for-facial-recognition

  *"IBM Corp. allegedly used people's images without permission to develop facial recognition technology in violation of Illinois' biometric privacy law, according to class claims filed in an Illinois state court."*

- **Immigrants Win Access To USCIS Data In Vetting Program Suit**

https://www.law360.com/articles/1235131/immigrants-win-access-to-uscis-data-in-vetting-program-suit

*"More than two dozen documents detailing how the U.S. Citizenship and Immigration Services evaluates immigration applications — including the agency's scoring methodologies, risk factors and indicators of national security concerns — must be handed over to class counsel within three weeks, U.S. District Judge Richard A. Jones ruled Thursday."*

## Privacy in the Executive Branch

- **DNA Collection at the Border Threatens the Privacy of All Americans**
  https://www.nytimes.com/2020/01/23/opinion/dna-collection-border-privacy.html

  *"On January 6, the federal government began collecting DNA from any person in immigration custody — previously, it had required only fingerprints. With this move, the federal government took a decisive step toward collecting and tracking large numbers of its citizens' genetic information too."*

- **WeLeakInfo, a search engine for breached personal data, shut down**
  https://www.cyberscoop.com/weleakinfo-shutdown-personal-information-for-sale/

  *"The U.S. Department of Justice on Thursday announced its seized weleakinfo.com, which has existed since 2017. The site sold different subscription levels, making it possible for scammers to access and search through the database."*

## Privacy in the Private Sector.

- **The US needs a national privacy law for personal data, Salesforce co-CEO says**
  https://www.cnbc.com/2020/01/21/the-us-needs-a-national-privacy-law-for-personal-data-salesforce-co-ceo-says.html

- **So far, under California's new privacy law, firms are disclosing too little data — or far too much**
  https://www.washingtonpost.com/technology/2020/01/21/ccpa-transparency/

- **Apple vs FBI: Pensacola Isn't San Bernardino**
  https://www.lawfareblog.com/apple-vs-fbi-pensacola-isnt-san-bernardino

- **250 million Microsoft customer service records briefly exposed online: report**
  https://thehill.com/policy/cybersecurity/479426-250-million-microsoft-customer-service-records-briefly-exposed-online

## Privacy in the Public Sector.

- **Privacy International Report on "Cloud Extraction" Programs Sheds Light on Far-Reaching Government Surveillance Technology**
  https://www.cpomagazine.com/data-privacy/privacy-international-report-on-cloud-extraction-programs-sheds-light-on-far-reaching-government-surveillance-technology/

  *"Authentication tokens for various cloud services can remain active for weeks at a time, and in some cases are permanent. If the investigating agency can extract these tokens, they do not need to coerce the subject into giving up login information; if they already have login information, they can maintain ongoing access even if the subject later changes their password. This also allows them to circumvent most two-factor authentication (2FA) measures."*

- **Hospitals Give Tech Giants Access to Detailed Medical Records**
  https://www.wsj.com/articles/hospitals-give-tech-giants-access-to-detailed-medical-records-11579516200?mg=prod/com-wsj

  *"Hospitals have granted Microsoft Corp., International Business Machines Corp. and Amazon.com Inc. the ability to access identifiable patient information under deals to crunch millions of health records, the latest examples of hospitals' growing influence in the data economy."*

## Privacy around the World.

- **Britain Plans Vast Privacy Protections for Children**
  https://www.nytimes.com/2020/01/21/business/britain-children-privacy-protection-kids-online.html

  *"The rules will require social networks, gaming apps, connected toys and other online services that are likely to be used by people under 18 to overhaul how they handle those users' personal information. In particular, they will require platforms like YouTube and Instagram to turn on the highest possible privacy settings by default for minors, and turn off by default data-mining practices like targeted advertising and location tracking for children in the country."*

- **EU considers temporary ban on facial recognition in public spaces**
  https://www.politico.eu/pro/eu-considers-temporary-ban-on-facial-recognition-in-public-spaces/

- **London Police Amp Up Surveillance With Real-Time Facial Recognition**
  https://www.nytimes.com/2020/01/24/business/london-police-facial-recognition.html

- **Amazon Alexa Eavesdropping Spurs EU-Wide Privacy Safeguards**
  https://www.bloomberg.com/news/articles/2020-01-17/amazon-s-snooping-on-alexa-chats-spurs-eu-wide-privacy-response

- **Thousands of Chinese Students' Data Exposed on Internet**
  https://www.wsj.com/articles/thousands-of-chinese-students-data-exposed-on-internet-11579283410

## Your Devices, Your Privacy.

- **The Apps on My Phone Are Stalking Me**
  https://www.nytimes.com/2020/01/22/opinion/phone-data-privacy.html

  *"Your location, your purchases, video and audio from within your home and office, your online searches and every digital wandering, biometric tracking of your face and other body parts, your heart rate and other vital signs, your every communication, recording, and perhaps your deepest thoughts or idlest dreams — in the future, if not already, much of this data and more will be collected and analyzed by some combination of governments and corporations, among them a handful of megacompanies whose powers nearly match those of governments."*

- **People Are Calling SWAT Teams to Tech Executives' Homes**
  https://www.nytimes.com/2020/01/23/technology/fake-swat-calls-swatting.html

  *"Swatting is online lingo used to describe when people call the police with false reports of a violent crime of some sort inside a home, hoping to persuade them to send a well-armed SWAT team. [...]*

  *The attacks have been aided by forums that have sprung up both on the public internet and on the camouflaged sites of the so-called dark web. These forums name thousands of people, from high-ranking executives to their extended families, who could be targets, providing cellphone numbers, home addresses and other information."*

- **Google and Apple Clash Over Web Browser Privacy**
  https://www.bloomberg.com/news/articles/2020-01-22/google-and-apple-clash-over-web-browser-privacy

*"Instead of making a big list of cookies to block, Apple's ITP continuously learns what websites users visit and which kinds of cookies try to hitch a ride. Over time, this creates unique cookie-blocking algorithms for each web surfer that can be used to identify and track them, according to the paper."*

- **Equifax Breach Affected 147 Million, but Most Sit Out Settlement**
  https://www.nytimes.com/2020/01/22/business/equifax-breach-settlement.html

***Have a wonderful weekend and an even better National Data Privacy Day (if it's not already blocked off on your calendar, it's next Tuesday)!***

Kind regards,
Charlie

Chief Privacy Officer
Office of the Executive Director | U.S. Commodity Futures Trading Commission
1155 21st Street, NW | Washington DC 20581 | Tel: (b) (6)

(b) (5)

DHS-001-02632-00015105/02/2022

DHS-001-02632-00015105/02/2022

(b) (5)

DHS-001-02632-00015205/02/2022

DHS-001-02632-00015205/02/2022

(b) (5)

DHS-001-02632-00015305/02/2022

DHS-001-02632-00015305/02/2022

(b) (5)

DHS-001-02632-00015405/02/2022

DHS-001-02632-00015405/02/2022

(b) (5)

DHS-001-02632-00015505/02/2022

DHS-001-02632-00015505/02/2022

(b) (5)

DHS-001-02632-00015605/02/2022

DHS-001-02632-00015605/02/2022

(b) (5)

DHS-001-02632-00015705/02/2022

DHS-001-02632-00015705/02/2022

(b) (5)

DHS-001-02632-00015805/02/2022

DHS-001-02632-00015805/02/2022

(b) (5)

DHS-001-02632-00015905/02/2022

DHS-001-02632-00015905/02/2022

(b) (5)

DHS-001-02632-00016005/02/2022

DHS-001-02632-00016005/02/2022

(b) (5)

DHS-001-02632-00016105/02/2022

DHS-001-02632-00016105/02/2022

DHS-001-02632-00016205/02/2022

# DHS Biometric Capabilities Executive Steering Committee

## *Briefing on Requirements Coordination with DHS Joint Requirements Council*

Office of Biometric Identity Management
Management Directorate
U.S. Department of Homeland Security
September 18, 2020



DHS-001-02632-00016205/02/2022

DHS-001-02632-00016305/02/2022

# Briefing Purpose & Agenda

**Purpose:** Provide the Department of Homeland Security (DHS) Biometric Capabilities Executive Steering Committee (BC-ESC) with an overview of the proposal to establish a coordinating relationship with the DHS Joint Requirements Council (JRC) on biometric gaps and requirements identification for JRC Portfolio Team (PT) studies, analysis, and development.

## Agenda:

- Bottom Line Up Front
- Background (BC-ESC, JRC PT)
- Concept for BC-ESC/JRC Coordination
- DHS BC-ESC/JRC Memorandum of Understanding
- Way Ahead
- Questions
- Back-up Slides

DHS-001-02632-00016405/02/2022

# Bottom Line Up Front & Background

- The JRC, Counter Terrorism & Homeland Security Threats (CTHST) PT recommended that the JRC leverage the BC-ESC as a coordinating body for biometric requirements before they are sent to PTs for studies and development actions.

- On July 15, 2020, Mr. Chris Moman, ICE CAE, alerted the Office of Biometric Identity Management (OBIM) to the new JRC approach to how its PTs operate, and intention to use existing governance bodies as sources for identifying capability gaps, issues, and/or ideas.
  - OBIM believes it is consistent with the BC-ESC Charter.

- OBIM staff collaborated with JRC and PT staff representatives from August 14 through September 15, 2020.
  - All agreed in concept but need to seek approvals from respective leadership chains and consensus from BC-ESC and JRC Principals.
  - OBIM and JRC staff are currently collaborating on a draft Memorandum of Understanding (MOU) between the BC-ESC and the JRC.

DHS-001-02632-00016505/02/2022

# Background – DHS BC-ESC

## DHS BC-ESC

- Chartered/established in 2019 Pursuant to an Acquisition Decision Memorandum issued by the Under Secretary for Management (USM), dated June 12, 2018.

- The mission of the BC-ESC is to provide effective governance, oversight, coordination, and guidance to all DHS and Component-level programs that are developing and/or providing biometric capabilities in support of DHS mission objectives. The Committee serves as a forum for cross-Component collaboration and the sharing of biometric challenges, needs, concepts, best practices, plans and efforts.

DHS-001-02632-00016605/02/2022

# Background – DHS BC-ESC

**DHS BC-ESC objectives (excerpts):**

- Serving as a forum to discuss DHS's approach to biometrics.
- **Supporting identification of biometric operational gaps and the needs of the DHS Components, and ensuring OBIM has the necessary guidance and support to help bring capabilities to fruition to address those needs.**
- **Eliminating duplication of biometric efforts across the Department.**
- **Ensuring complementary biometric efforts across the Department.**
- **Analyzing opportunities to integrate biometric efforts, systems, or activities across the Department.**
- Serving as an executive-level venue to present status on biometric capability pilots, demonstrations, and delivery by DHS and its Components.
- Reviewing and deliberating on issues elevated by ESC members.

# Background – JRC PT

DHS-001-02632-00016705/02/2022

**Updated PT Concept**

- JRC will charter portfolio teams to address DHS priorities for capabilities and requirements.
- PTs will be focused on specific tasks/purposes and limited duration:
  - Receive JRC executive sponsorship/support for integrated, cross-Component studies for requirements development.
  - Align under one or more of the capabilities and requirements mission leads
  - Include cross-Component representation and the analytic and project management support necessary to generate appropriate recommendations to the JRC.
  - Push and pull cross-Component requirements issues for JRC consideration.
  - Generate mission area capabilities and requirements priorities and consolidated capabilities and requirements priorities across missions to inform JRC recommendations.

**Requirement and Gap Sources**

- JRC intends to leverage existing chartered bodies (DHS committees, working groups, etc.) to help identify mission/operational capability gaps for potential PT assignments.
- The DHS BC-ESC would be the first opportunity to execute this concept.

DHS-001-02632-00016805/02/2022

# DHS BC-ESC Coordination with JRC

## Concept

**Task:** The **DHS BC-ESC acts as a biometric requirements coordination body** consistent with its charter to generate ideas for biometric studies and to identify capability gaps **in a two-way information flow with the DHS JRC.**

- **Identifies gaps/needs and requirements** for greater integration of DHS biometric capabilities.
- **Partners with JRC** in order to identify areas of study that will require further analysis to be completed by a PT.

**Purpose: Create a common operating picture** regarding potential emerging requirements/gaps/operations to inform JRC PT assignments.

- **JRC initiates focused PTs** to develop studies that will provide both the BC-ESC and JRC Principals with the information needed to make determinations regarding identified capability gaps.
- **PTs generate cross-Component coordination**/DHS programmatic requirements.
- **BC-ESC supports Biometric PTs** with SMEs, Leads, sub-working groups.
- **BC-ESC contributes to biometric economies/effectiveness of building capabilities towards a "One-DHS" concept;** ensures complementary biometric efforts across the Department consistent with the BC-ESC Charter.

# Background – JRC PT Concept

DHS-001-02632-00016905/02/2022

(b) (5)

DHS-001-02632-00017005/02/2022

# DHS BC-ESC Coordination with JRC

(b) (5)

# BC-ESC/JRC MOU

DHS-001-02632-00017105/02/2022

- **BC-ESC and JRC PT leads are collaborating on a Memorandum of Understanding (MOU)**
  - DHS MGMT/OBIM: Eric Barr, Nefertari Farrell, Mike Klesius
  - JRC PT: Alex Moscoso, Portfolio Team Coordinator; Craig Mastapeter I&A, PT lead

- **MOU PURPOSE**: This MOU establishes a coordinating partnership between the DHS BC-ESC and the DHS JRC to identify biometric requirements that need further study and analysis by a JRC-appointed PT with the primary focus on horizontal alignment across DHS.

- **MOU Signatures** from JRC and OBIM Leadership
  - Mr. Shonnie Lyon as DHS/MGMT CXO for BC-ESC
  - Mr. Joseph Wawro as Executive Director, JRC

# BC-ESC/JRC MOU

**RESPONSIBILITIES:** The duties and responsibilities of the parties will include the following.

- **The BC-ESC and the JRC will establish coordination** and a two-way information flow to identify gaps and potential biometric requirements for greater integration of DHS biometric capabilities.
- **The DHS BC-ESC will act as a biometric requirements coordination body,** consistent with its charter, to identify capability gaps and to generate ideas for biometric studies and analyses by JRC-appointed PT.
- **The JRC PTs will inform the BC-ESC of its biometrics studies** and validation to ensure BC-ESC visibility. The JRC PTs will also share any deliverables from these studies with the BC-ESC.
- **The JRC will inform the BC-ESC of biometric requirements** submitted to the Capabilities Gap Register on a quarterly basis.

DHS-001-02632-00017305/02/2022

# BC-ESC/JRC MOU

## REQUIRED DOCUMENTATION:

- **Record of BC-ESC and JRC Principals' approvals** of this relationship will be provided to JRC and BC-ESC Principals once this MOU is signed.
- **BC-ESC meeting minutes** will be provided to the JRC to include amendments identifying those activities (action items) that will be handed off to a PT to work to serve as a log and a running status report.
- **JRC meeting minutes** will be provided to the BC-ESC identifying biometric gap and requirement topics for studies and affirming receipt of BC-ESC generated topics.
- **JRC Biometric PT assignments and requirements documentation** as appropriate will be provided to the BC-ESC for situational awareness and related coordination.

DHS-001-02632-00017405/02/2022

# Way Ahead

- ✓ 8/18 – 9/18 Develop draft MOU w/ JRC
- ✓ Draft MOU NLT 9/14
- Briefings –
  - ✓ OBIM Director and DUSM MGMT
  - ✓ 9/15 JRC Leadership/staff
  - ✓ 9/17 JRC Principals
  - ○ 9/18 BC-ESC
- 9/22-30 (or until complete) Finalize MOU and gain BC-ESC/DUSM MGMT and JRC approvals (final would include detailed process flow and responsibilities)
- 9/30 – BC-ESC & JRC begin coordination on biometric gaps/requirements
- 12/19 – Include in BC-ESC agenda

# DHS BC-ESC Coordination with JRC

DHS-001-02632-00017505/02/2022

Questions

# DHS BC-ESC Coordination with JRC

DHS-001-02632-00017605/02/2022

# DHS BC-ESC Coordination with JRC

DHS-001-02632-00017705/02/2022

## Back-up Slides

DHS-001-02632-00017805/02/2022

# Authorities

- The Joint Requirements Council (JRC), Directive Number: 071-02. Revision Number: 00. Issue Date: 02/1/2016
- Delegation to the Chair of the Joint Requirements Council, DHS Delegation Number: 00008, Revision Number: 00, Issue Date: 8/22/2016
- U.S. Department of Homeland Security Executive Steering Committee Charter for Biometric Capabilities, Version: 1.0, Date: March 2019
  - Pursuant to an Acquisition Decision Memorandum issued by the Under Secretary for Management (USM), dated June 12, 2018, and in accordance with authorities identified in Directive 102-01, Acquisition Management.

DHS-001-02632-00017905/02/2022

# BC-ESC/JRC MOU

**RESPONSIBILITIES:** The duties and responsibilities of the parties will include the following.

- **The BC-ESC and the JRC will establish coordination** and a two-way information flow to identify gaps and potential biometric requirements for greater integration of DHS biometric capabilities.
- **The DHS BC-ESC will act as a biometric requirements coordination body,** consistent with its charter, to identify capability gaps and to generate ideas for biometric studies and analyses by JRC-appointed PT.
- **The JRC PTs will inform the BC-ESC of its biometrics studies** and validation to ensure BC-ESC visibility. The JRC PTs will also share any deliverables from these studies with the BC-ESC.
- **The JRC will inform the BC-ESC of biometric requirements** submitted to the Capabilities Gap Register on a quarterly basis.

# BC-ESC/JRC MOU

## RESPONSIBILITIES (Cont).

- **The BC-ESC and the JRC will maintain regular communications on biometric capabilities issues to create a DHS common operating picture regarding potential gaps/requirements,** enabling the JRC to initiate focused PTs to develop studies of topics of interest or identify areas for potential horizontal alignment of biometric requirements.
  - This arrangement will allow for the effective generation of cross-Component coordination and the Department's understanding of programmatic biometric requirements in order to yield biometric resource economies and effective capability development, ensuring complementary biometric efforts across DHS consistent with the BC-ESC charter.

- **The JRC will coordinate with the BC-ESC as a resource to help identify biometric capability gaps associated with operational requirements and will propose solutions to mitigate those gaps through PT studies and validation in the Joint Requirements Integration and Management System (JRIMS).**
  - This will leverage opportunities for common solutions that enhance operational effectiveness, and better inform the Department's main investment pillars. The JRC will form PTs with defined scopes and timelines to conduct studies and projects related to developing biometric capabilities solutions in the JRIMS.

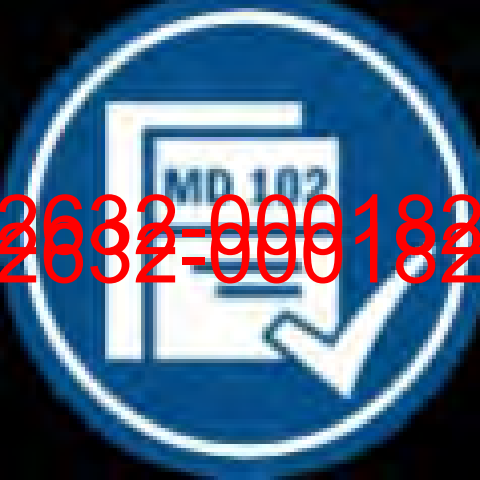
# BC-ESC/JRC MOU

## RESPONSIBILITIES (Cont).

- **The BC-ESC, as a Department-chartered forum for cross-Component discussion of DHS biometrics that supports identification of operational gaps and Component needs, will identify and analyze opportunities to integrate biometric efforts, systems, or activities across the Department.**

- **The JRC will provide the BC-ESC with insights on gaps for further assessment, such as identifying:**
  - R&D initiatives
  - Areas of consideration not yet entered into the Capabilities Gap Register and JRIMS
  - Component-vetted biometric needs

- **The BC-ESC will collaborate with the JRC to provide advisory support to serve in SME or leadership roles.**
  - BC-ESC Component representatives should have requisite biometric subject matter expertise and operational perspectives to coordinate and provide guidance to the PTs.



2632-000182