Department of Homeland Security
DHS Directives System
Instruction Number: 262-19-001
Revision Number: 00
Issue Date: 7/28/2023

DHS USE OF SOCIAL MEDIA AND OTHER THIRD-PARTY DIGITAL SERVICES

I. Purpose

This Instruction implements the Department of Homeland Security (DHS) Directive 262-19, DHS Use of Social Media and Other Third-Party Digital Services.

II. Scope

A. This Instruction applies throughout DHS.

B. The scope of this Instruction is limited to the use and management of Social Media and Other Third-Party Digital Services, where the intent is to make DHS-related or other government information available to the public or to a general audience within DHS, or to monitor non-DHS accounts for non-operational situation awareness related to DHS missions and activities. The scope of this Instruction also provides guidance regarding online engagement using these services in a personal capacity, where such personal engagement relates to DHS activities or as otherwise outlined in this document.

C. This Instruction applies to DHS employees, contractors and non-DHS entities that are supporting DHS mission-related activities or accessing Social Media and other Third-Party Digital Services via DHS information systems technologies, including internet connections, computers, and mobile communication devices, or in support of DHS-related activities.

D. This Instruction does not apply to operational use of Social Media and other Third-Party Digital Services as a tool of screening, vetting, operational situational awareness, or other uses where Social Media and Other Third-Party Digital Services are not used to make information available to the public.

III. References

A. Title 5, United States Code (U.S.C.), Section 552a, “Records Maintained on Individuals” [The Privacy Act of 1974, as amended]

B. 5 C.F.R., Part 2635, "Standards of Ethical Conduct for Employees of the

Executive Branch", Part 4601, "Supplemental Standards of Ethical Conduct for Employees of the Department of Homeland Security"

C. Title 5, Sections 7321-7326, "Hatch Act;" 5 C.F.R. Part 734, "Political Activities of Federal Employees"

D. Title 6, U.S.C., Section 142, “Chief Privacy Officer”

E. Title 15, U.S.C., Sections 6501-6505, "Children's Online Privacy Protection Act"

F. Title 17, U.S.C., Chapters 1-13, "Copyright Law"

G. Title 18, U.S.C., Section 2071, "Concealment, Removal or Mutilation of Records"

H. Title 29, U.S.C., Section 794d, “Electronic and Information Technology” [Section 508 of the Rehabilitation Act of 1973]

I. Title 36, C.F.R., Chapter 12B, "Records Management"

J. Title 44, U.S.C., Chapter 21, “National Archives and Records Administration,” Chapter 29, “Records Management by the Archivist of the United States and by the Administrator of General Services,” Chapter 31, “Records Management by Federal Agencies,” Chapter 33, “Disposal of Records,” Chapter 35, “Coordination of Federal Information Policy,” Chapter 35, “Information Security (The Federal Information Security Management Act of 2002, as amended),” and Chapter 36, “Management and Promotion of Electronic Government Services”

K. OMB Circular A-130, Managing Information as a Strategic Resource (July 28, 2016)

L. OMB Memorandum M-10-06, Open Government Directive

M. OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies

N. OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications

O. OMB Memorandum M-13-10: Antideficiency Act Implications of Certain Online Terms of Service Agreements

P. OMB Guidance, Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act (April 7, 2010)

Q. DHS Delegation 2001, “Delegation to the Assistant Secretary for Public

Affairs”

R. Public Law 106-554, Section 515, "Information Quality Act"

S. Public Law 107-347, “E-Government Act of 2002,” as amended, Section 208

T. Public Law 113-187, "Presidential and Federal Records Act Amendments of 2014"

U. DHS Directive 047-01, Privacy Policy and Compliance

V. DHS Directive 110-01, Privacy Policy for Operational Use of Social Media

W. DHS Directive 140-01, Information Technology Security Program

X. DHS Directive 0480.1 Ethics/Standards of Conduct

Y. DHS/ALL/PIA-031 Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue

Z. White House Memorandum on Transparency and Open Government (Jan. 21, 2009)

AA. National Archives and Records Administration (NARA) Bulletin 2014-02, Guidance on Managing Social Media Records

IV. Definitions

For purposes of Directive 262-19 and this Instruction, the following definitions apply.

A. **Account.** Any and all profiles, pages, feeds, registrations, or other means of access that allow for the creation, posting, or monitoring content on a Social Media and other Third-Party Digital Service.

B. **Account Manager.** DHS employee who manages an official Social Media or other Third-Party Digital Service account. The account manager is a full-time, permanent federal employee. Exceptions to the full-time, permanent federal employee status can be granted on a case-by-case basis by the DHS Office of Public Affairs.

C. **Non-DHS Entity.** Individuals and/or organizations that are supporting DHS mission-related activities, are funded by DHS, or accessing Social Media and other Third-Party Digital Services via DHS information systems. Examples include Department of Defense personnel that are supporting FEMA activities, educational institutions that are part of the community of practice sponsored by DHS, non-DHS members of the Surge Capacity Force, etc.

D. **Official Account**. A Social Media or other Third-Party Digital Service account that has been approved for DHS public communication purposes by the Office of Public Affairs. A public communication purpose could include proactively providing information to the general public through an approved DHS official account or to be used for non-operational situational awareness.

E. **Operational Use of Social Media.** Authorized use of Social Media and other Third-Party Digital Services to collect information for the purpose of enhancing operational 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 and other Third-Party Digital Services for public affairs activities (including non-operational situational awareness) for individual professional development (such as training and continuing education), or for facilitating internal meetings.

F. **Personally Identifiable Information (PII).** Any information that permits the identity of an individual to be directly or indirectly inferred, including any other 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. For example, when linked or linkable to an individual, such information includes a name, social security number, date and place of birth, mother's maiden name, account number, license number, vehicle identifier number, license plate number, device identifier or serial number, internet protocol address, biometric identifier (e.g., photograph, fingerprint, iris scan, voice print), educational information, financial information, medical information, criminal or employment information, information created specifically to identify or authenticate an individual (e.g., a random generated number).

G. **Privacy Compliance Documentation.** Any document required by statute or by the Chief Privacy Officer that supports compliance with federal government requirements (e.g., Privacy Act of 1974, E-Government Act of 2002) and DHS privacy policy, procedures, or document requirements, including Privacy Threshold Analyses (PTA), Privacy Impact Assessments (PIA), System of Records Notices (SORN), Notices of Proposed Rulemaking for Exemption to Privacy Act System of Records (NPRM), Final Rules, and Privacy Act Statements/Privacy Notices.

H. **Privacy Notice.** A brief description of how the Department's Privacy Policy will apply in a specific situation or for a specific Social Media or other Third-Party Digital Service.

I. **Privacy Policy.** A consolidated explanation of the Department's general privacy-related practices that pertain to its official website and its other online

activities. It is a single, centrally located statement that is accessible from the Department's official homepage.

J. **Public Communication.** Proactively providing DHS-related or other government information to the general public.

K. **Published Content.** Any materials, documents, photographs, graphics, and other information that is created, posted, distributed, transmitted, or otherwise made available to the public using Social Media or other Third-Party Digital Service accounts.

L. **Non-operational Situational Awareness**. The process of identifying or assessing what is being said about a particular topic on the public internet and social media to gain insight on the public's perception of topics related to DHS missions and activities.

M. **Social Media.** The sphere of websites, applications, and web-based tools that connect users to engage in dialogue, share information and media, collaborate, and interact. Social media take many different forms, including web-based communities and hosted services, social networking sites, video and photo sharing sites, blogs, virtual worlds, social bookmarking, broadcast/push text messaging services, and other emerging technologies. Social media sites are a type of Third-Party Digital Service.

N. **Third-Party Digital Service (website, application, or platform).** Web-based technologies that are not exclusively operated or controlled by a government entity, or web-based technologies that involve significant participation of a nongovernment entity. Often these technologies are located on a ".com" website or other location that is not part of an official government domain. However, third-party applications can also be embedded or incorporated on a Department's official website.

V. Responsibilities

A. The ***DHS Assistant Secretary for Public Affairs:***

1. Reviews and approves Social Media and other Third-Party Digital Services that are allowed for official public communication use by the Department;

2. Maintains a list of Social Media and other Third-Party Digital Services that have been approved for DHS public communication purposes in a location accessible to DHS employees/contractors on the DHS intranet (DHS Connect);

3. Approves official Social Media and other Third-Party Digital Service accounts for public communication use by the Department;

4. Maintains a list of official DHS Social Media and other Third-Party Digital Service Accounts used for public communication by the Department on DHS.gov;

5. Ensures that official Social Media and other Third-Party Digital Service Accounts used for public communication are accurately reported on the U.S. Digital Registry;

6. Provides procedural guidance and training for establishing, maintaining, and publishing content to official accounts on approved Third-Party Digital Services; and

7. Approves (or delegates the approval of) all content published to official Social Media and other Third-Party Digital Service accounts, consulting with relevant internal organizations (including the Officer for Civil Rights and Civil Liberties, Chief Freedom of Information Act Officer, Chief Information Officer, Chief Privacy Officer and General Counsel) to ensure compliance with applicable laws, policies, and procedures.

B. The ***DHS Chief Information Officer (CIO):***

1. Ensures adherence to information system policies, laws, regulations, and guidance including those regarding accessibility and security;

2. Determines the security posture of any new proposed Social Media or Third-Party Digital Service to ensure adequate information technology security and ensures Social Media and other Third-Party Digital Service platforms will not pose a security risk to the DHS enterprise network;

3. Approves and provides access to Social Media and other Third-Party Digital Service platforms that are approved for public communications purposes on the unclassified DHS network for DHS Headquarters employees and contractors with an approved mission requirement/business need;

4. Establishes and enforces account security/password policy requirements for official Social Media and other Third-Party Digital Service accounts that are approved for public communications use; and

5. In coordination with the National Archives and Records Administration (NARA), defines records management disposition for content posted to official Social Media and other Third-Party Digital Service accounts and ensures the execution of the quadrennial archival of all DHS Social Media and other Third-Party Digital Service accounts (to coincide with the Presidential Inauguration) as administered by the DHS Chief Records Officer.

C. The ***DHS Chief Privacy Officer and Chief Freedom of Information Act Officer:***

1. Serves as the authority on privacy matters relating to the DHS use of Social Media and other Third-Party Digital Services;

2. Approves any use, release, or disclosure of personally identifiable information (PII) through official Social Media and other Third-Party Digital Service accounts;

3. Assesses and mitigates privacy risks associated with the Department's use of Social Media and other Third-Party Digital Services;

4. Oversees the processing of Freedom of Information Act requests for records related to official DHS use of Social Media and other Third-Party Digital Services;

5. Ensures the Department's use of Social Media and other Third-Party Digital Services follows all applicable federal laws and DHS privacy policies, including compliance with applicable DHS privacy impact assessments.

D. The ***DHS Officer for Civil Rights and Civil Liberties:***

1. Serves as the authority on civil rights and civil liberty matters related to the Department's use of Social Media and other Third-Party Digital Services;

2. Assesses and mitigates risks to civil rights and civil liberties associated with the Department's use of Social Media and other Third-Party Digital Services; and

3. Ensures the Department's use of Social Media and other Third-Party Digital Services for public communication purposes follows all constitutional, statutory, regulatory, policy, and other requirements relating to the civil rights and civil liberties of all affected individuals.

E. The ***DHS General Counsel:***

1. Reviews, and provides legal guidance or advice, on agreements and terms of service with Social Media and other Third-Party Digital Service providers prior to the public communications use of any service and provides legal advice and guidance on issues that arise with respect to the Department's official use of Social Media and Third-Party Digital Services for public communication purposes; and

2. Reviews and provides legal guidance or advice on proposed public communication uses of Third-Party Digital Services consistent with

applicable statutes, standards of conduct for federal employees, and the Department's standards and requirements for the ethical conduct of Departmental business.

F. ***Component Public (External) Affairs Directors:***

1. Ensures that components only use Social Media and Third-Party Digital services that have been approved by the DHS Assistant Secretary for Public Affairs for public communications use.

2. Submit requests for all official Social Media and Third-Party Digital Service accounts to the DHS Office of Public Affairs for approval;

3. Maintain a list of official component Social Media and other Third-Party Digital Service accounts used for public communication purposes on the respective primary component website and reports any addition or deletion of official accounts to the DHS Office of Public Affairs immediately;

4. Maintains a current and accurate list of all account managers for official component Social Media and other Third-Party Digital Service accounts use for public communication purposes;

5. Ensure that official component Social Media and other Third-Party Digital Service accounts used for public communications purposes are appropriately reported on the U.S. Digital Registry and to the DHS Office of Public Affairs;

6. Establish a formal process for approving and publishing public communications information to Social Media and other Third-Party Digital Services that aligns with procedural guidance provided by the Assistant Secretary for Public Affairs and is approved by the DHS Office of Public Affairs; and

7. Respond to certification and reporting requirements for component Social Media and other Third-Party Digital Services.

G. ***Component Chief Information Officers:***

1. Approve and provide access to Social Media and other Third-Party Digital Service platforms that are approved by the DHS Assistant Secretary for Public Affairs for public communications purposes on the unclassified DHS component networks for DHS component employees and contractors with an approved mission requirement/business need;

2. Ensure the component's execution of the quadrennial archival of all component Social Media and other Third-Party Digital Service accounts (to coincide with the Presidential Inauguration); and

3. Promptly report security, connectivity, latency, and other information technology-related issues related to Social Media and other Third-Party Digital Services that have a potential for Department-wide impact to the DHS CIO Council and/or the DHS CIO.

H. ***Account Managers:***

1. Are a full-time, permanent federal employee. Exceptions to the full-time, permanent federal employee status can be granted on a case-by-case basis by the DHS Office of Public Affairs.

2. Submit requests for all new official Social Media and other Third-Party Digital Service accounts used for public communication purposes to the DHS Office of Public Affairs for approval. Component account managers submit requests for Component Public/External Affairs, which will then coordinate and present to the DHS Office of Public Affairs for approval;

3. Prior to the creation of the account, provide a copy of their DHS Cybersecurity Awareness Training certificate to the DHS Office of Public Affairs (for headquarters accounts) or Component Public/External Affairs (for component accounts). The Cybersecurity Awareness Training must be for the same fiscal year they are requesting an account and must be submitted yearly thereafter while the account is active.

4. Prior to the creation of the account, complete all required DHS or component trainings related to the use of Social Media and other Third-Party Digital Services used for public communication purposes.

5. Serve as the point of contact for the account;

6. Ensure that all content posted is approved through appropriate and existing communication channels, following procedural guidance established by the Assistant Secretary for Public Affairs and Component Public (External) Affairs (if applicable), before publication and distribution;

7. Ensure that all content posted meets the requirements of Section 508 of the Rehabilitation Act, including those requirements related to accessibility;

8. Ensure that public communication efforts using Social Media and other Third-Party Digital Services that constitute research involving human subjects are reviewed and approved by the Compliance Assurance Programs Office (CAPO) for Human Subjects Research (HSR) per Directive 026-04;

9. Provide all relevant and current account access credentials

(username, password, two-factor authentication, etc.) to the DHS Office of Public Affairs upon creation of account and immediately upon request;

10. Coordinate with the appropriate headquarters or component privacy office to ensure that DHS engages on the account in a manner that respects freedom of speech and expression, protects privacy, respects the intent of users, and does not solicit or collect PII;

11. Coordinate with the appropriate headquarters or component records management office to affect the quadrennial archival of Social Media and other Third-Party Digital Service accounts as required by NARA; and

12. If the account is no longer needed for official business, notify the appropriate headquarters or component Office of Public/External Affairs and records liaison/manager and complete the archival of the account per DHS Chief Records Officer and NARA requirements.

VI. Content and Procedures

A. ***General:***

1. The Department of Homeland Security uses Social Media and other Third-Party Digital Services to communicate the Department's mission and activities to the public. Their use is intended to be part of a larger, integrated communications apparatus coordinated by the Department's Office of Public Affairs and/or delegated to components/offices.

2. It is the policy of the Department of Homeland Security that Social Media and other Third-Party Digital Services be accessed and used in a responsible manner that enables and furthers the mission of the Department. Official use of Social Media and other Third-Party Digital Services to communicate and engage with the public must be in accordance with all applicable Federal laws, regulations, and policies including those regarding accessibility, freedom of speech, information quality, intellectual property, privacy, civil rights and civil liberties, records management, and security.

B. ***Use of Approved Social Media and other Third-Party Digital Services:***

1. DHS components and offices may only use approved Social Media Third-Party Digital Services for public communications purposes. Social Media and other Third-Party Digital Services are approved for public communications use following an official review process coordinated by the DHS Office of Public Affairs, with consultation from the DHS Headquarters Privacy Office, Office for Civil Rights and Civil Liberties, Office of the Chief Information Officer (Chief Information Security Officer

and Records Management) and Office of General Counsel.

2. The application for requesting the approval of a new Social Media or other Third-Party Digital Service for DHS public communications purposes can be found on DHS Connect.

3. A list of Social Media and other Third-Party Digital Services approved for public communication purposes is available on DHS Connect.

C. ***Access to Social Media and other Third-Party Digital Services:***

1. Due to the high threat of malware infiltration and the sensitive nature of the information maintained at DHS, Social Media and other Third-Party Digital Service hosts sites are blocked at the Department's Trusted Internet Connection (TIC).

2. Network connectivity to approved Social Media and other Third-Party Digital Service websites or applications is approved by the DHS Chief Information Officer (for headquarters employees and contractors) or Component Chief Information Officers (for component employees and contractors) based on legitimate business need of the requesting office, unit, or individual supervisor. A legitimate business need includes the management of an official Social Media or other Third-Party Digital Service Account for public communications purposes or monitoring a Social Media or other Third-Party Digital Service for non-operational situational awareness.

D. ***Account Application and Approval:***

1. The public communications use of an approved Social Media or other Third-Party Digital Service in an official capacity must be approved and is granted by the DHS Office of Public Affairs. This includes receiving approval to create Social Media and other Third-Party Digital Service accounts for locations, programs, offices, and employees that are to be used in an official capacity.

2. Official Social Media and other Third-Party Digital Service accounts that are created for employees serving in an official capacity (individual accounts) and used for public communication purposes are considered federal records, are retained by the Department, and are subject to any and all applicable laws and regulations related to records management.

3. Content created and posted in an official capacity to a Social Media or other Third-Party Digital Service may constitute a federal record and is subject to relevant laws and regulations, including the Freedom of Information Act, Information Quality Act, and the Hatch Act.

4. DHS components and offices must follow the account approval process outlined by the DHS Office of Public Affairs when creating Social Media and other Third-Party Digital Service accounts for public communication purposes.

5. Any official Social Media or other Third-Party Digital Service account used for public communication purposes that has not been appropriately approved is subject to immediate termination.

6. Any official Social Media or other Third-Party Digital Service account used for public communication purposes can be terminated at the discretion of the Assistant Secretary for Public Affairs.

7. The Application for an official DHS Social Media or other Third-Party Digital Service account to be used for public communication purposes can be found on DHS Connect.

8. The list of official DHS Social Media or other Third-Party Digital Service accounts used for public communication purposes can be found on DHS.gov.

E. ***Accountability:***

1. Official Social Media or other Third-Party Digital Service accounts must have a current and active primary point of contact (Account Manager) who is responsible for managing account security and overseeing activity on the account. The Account Manager must be a full-time, permanent federal employee. Exceptions to the full-time, permanent federal employee status can be granted on a case-by-case basis by the DHS Office of Public Affairs. A current roster of Account Managers and their assigned accounts is kept by DHS OPA (for headquarters accounts) and component public affairs (for component accounts).

2. The Account Manager is responsible for the content published to an official Social Media or other Third-Party Digital Service account.

3. Any content posted by DHS to an official Social Media or other Third-Party Digital Service account is considered public, regardless of any privacy controls inherent to the platform that are meant to restrict access to that content.

4. It is assumed that any content posted by DHS to an official Social Media or other Third-Party Digital Service account will be available to a large audience (public), may be published or discussed in the media, and is subject to FOIA, discovery, and other laws and policies requiring public disclosure.

5. DHS employees posting content to an official Social Media or other Third-Party Digital Service are expected to adhere to DHS Directive 0480.1, “Ethics/Standards of Conduct” and 5 C.F.R. 735.203 which states ”An employee shall not engage in criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, or other conduct prejudicial to the Government." DHS employees are also required to adhere to any component-specific standards of conduct as well.

6. Account Managers must ensure compliance with all laws, rules, and regulations regarding official communications and activity on Social Media and other Third-Party Digital Services, including those relating to the protection of privacy, civil rights and civil liberties. Restrictions include:

a. The use of vulgar or abusive language, personal attacks of any kind, language that expresses discriminatory animus towards an individual or group based on a protected characteristic (e.g., race, gender, or sexual orientation), or offensive terms targeting individuals or groups;

b. Endorsement or advertising of products, services, or any non-federal entity;

c. Solicitation of donations of any kind;

d. Inclusion of PII unless authorized by the Chief Privacy Officer;

e. Engaging in activity directed toward the success or failure of partisan political parties, candidates, or groups (including the use of campaign slogans); and

f. Advocating for a policy or piece of legislation.

F. ***Official Accounts vs. Personal Accounts for Official Business***

1. Social Media and other Third-Party Digital Service accounts created or used to communicate official Department business to the public (official account) must stay under the control of the Department.

2. A unique Department-administered account (official account) must be created when an employee uses a Social Media or other Third-Party Digital Service to communicate official Department business to the public.

3. Personal accounts that are only used to access an official DHS account (if required by the platform) are not considered Federal records and will not be retained by the Department.

G. ***Personal Use of Social Media and other Third-Party Digital Services:***

1. Official DHS Social Media and other Official Third-Party Digital Service accounts used for public communication must remain distinctly separate from employees' personal accounts unless the platform in question requires a personal account to access an official DHS account.

2. Employees must avoid creating the appearance that DHS or the Federal Government endorses or supports their personal activities or the activities of another, or that they are using their official title, position, or any authority associated with their public office for private gain. Use of photos in uniform or use of official insignia (e.g., the DHS seal or component logos) are likely to be construed as use of official position and authority associated with official position for private gain depending on the context the photos in uniform or official insignia are used. An employee does not create the appearance of government endorsement merely by identifying his or her official title or position in an area of the personal social media account designed for biographical information. However, employees should either refrain from including a reference to their official title or position in a specific post that expresses the employee's own personal views or recommendations, or include a conspicuous disclaimer that makes it clear that the communications reflect only the employee's personal views and do not represent the views of DHS or the Federal Government. An example of an appropriate disclaimer is below:

"The views expressed are my own opinion, and do not represent the positions, or opinions of the U.S. Department of Homeland Security or the Federal Government."

3. If an employee identifies themselves as a DHS employee in a social media or other third-party digital service profile/post/message/etc., or otherwise indicates that they work for DHS, they should include an appropriate disclaimer when referring to or discussing DHS's operations, programs, and policies on social media.

4. Employees should be mindful of the possibility that anything they post online will be attributed to them personally, even if they post anonymously. Employees should also be aware that the public may recognize them as employees of DHS, particularly if they include career information on their social media profiles. DHS respects employees' decision to use social media and post online while off duty. However, employees are prohibited from engaging in online activities that would reasonably be expected to cause an unwarranted disruption to DHS's operations, such as activities that violate the law (e.g., stalking) or express discriminatory animus towards an individual or group based on a protected characteristic (e.g., race, gender, or sexual orientation). The effectiveness of DHS's operations depends on public trust and confidence, and employees should use common sense and good judgment to recognize

situations where a reasonable person would find that their online activities could so seriously undermine that public trust and confidence as to harm DHS's ability to achieve its mission. Note that this policy should not be construed as barring employees from engaging in legally-protected speech activities, such as whistleblowing or expressing opposition to discrimination or harassment pursuant to applicable law.

5. Employees are allowed to share or 'retweet' posts from official DHS Social Media or other Third-Party Digital Service accounts used for public communication purposes on their personal accounts. To the extent that they convey any other messages when sharing or retweeting those posts, they should include an appropriate disclaimer stating that these personal messages reflect only the employee's personal views and do not represent the views of the Department of Homeland Security.

6. In the event an image, video, or other posting by a DHS employee regarding DHS-related topics gains public attention or popularity on an employee's personal account (e.g. "goes viral"), there is a heightened risk that any comments or statements that affected employees make will be misconstrued or misreported as reflecting the position of the Department. Employees should contact the DHS Office of Public Affairs or the appropriate component Public/External Affairs Office for guidance and coordination.

7. DHS has authorized specific employees to speak on its behalf. Employees who are not authorized to speak on behalf of the Department must not use Social Media or other Third-Party Digital Services to speak, respond, or post on behalf of DHS without explicit written authorization from either the Office of Public Affairs or their component Office of External/Public Affairs.

8. Employees must not disclose nonpublic information when using Social Media or other Third-Party Digital Services, in accordance with DHS MD No. 11042.1, "Safeguarding Sensitive But Unclassified (For Official Use Only Information)."

9. Employees may not accept compensation for statements or communications made over social media that relate to their official duties.

10. Employees must follow the guidance and restrictions found in the Hatch Act, which govern prohibited partisan political activity by federal employees regardless of whether or not they are posting to an official DHS account or to a personal account.

11. Employees may use personal social media accounts to fundraise for nonprofit charitable organizations in a personal capacity, however, they must avoid personally soliciting funds from a subordinate or a known

prohibited source by directly naming or linking to these individuals in a solicitation request, pursuant to 5 C.F.R. § 2635.808(c). Employees also may not use their official titles, positions, or authority associated with their official positions to further the fundraising efforts.

12. Although DHS employees are authorized to conduct 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 and other Third-Party Digital Services. This restriction also applies to contractors and other individuals using DHS equipment.

13. The use of Social Media and other Third-Party Digital Services is an attack vector routinely exploited by cybercriminals, whose activities may expose the Department to unacceptable risk. DHS prohibits personal use of, and access to, Social Media and other Third-Party Digital Services from government equipment unless an exception to policy has been granted.

H. ***Postings to Official Accounts:***

1. DHS uses Social Media and other Third-Party Digital Service accounts to communicate and represent the Department's mission and activities to the public.

2. Content published to official Social Media and other Third-Party Digital Service accounts must be approved prior to publication, following procedural guidance issued by the Assistant Secretary for Public Affairs, to ensure maximization of quality, utility, objectivity, and integrity of information. The Assistant Secretary for Public Affairs, DHS Privacy Office, or General Counsel may direct and require additional scrutiny and/or levels of approval for some content, posts, and/or accounts at their discretion.

3. Communication of information that is considered non-public and has not been approved for release through official processes is prohibited.

4. The posting of internal (e.g. For Official Use Only), sensitive (e.g. Law Enforcement Sensitive), proprietary, or classified information to Social Media or other Third-Party Digital Services is strictly prohibited. Failure to comply may result in disciplinary action or criminal penalties.

5. Do not post anything to an official Social Media or other Third-Party Digital Service account that should not be shared publicly. Whatever is posted may be public for an indefinite time, even if attempts are made to modify or delete it.

6. Do not use Social Media and other Third-Party Digital Service Accounts as the sole venue for conducting official government business or the sole outlet for disseminating information related to official DHS functions and activities. Any information that could constitute a federal record (e.g., press releases, policy statements, and other official announcements) should also be provided on another publicly available platform hosted on a DHS system (such as official DHS websites).

I. ***Comments:***

1. The Department of Homeland Security respects different opinions and the freedom of speech of those engaging with official Social Media and other Third-Party Digital Service accounts.

2. The DHS Moderation/Comment policy can be found on DHS.gov. DHS does not pre-moderate users' comments on third-party digital accounts, meaning any users' comments are immediately published, but they can be removed if they contain:

   a. Vulgar or abusive language;

   b. Personal or obscene attacks of any kind;

   c. Discriminatory language or offensive terms (hate speech) targeting individuals or groups;

   d. Threats or defamatory statements;

   e. Links to external sites unrelated to the discussion;

   f. Suggestions or encouragement of illegal activity;

   g. Multiple successive off-topic posts by a single user or repetitive posts copied and pasted by multiple users, or spam;

   h. Unsolicited proposals or other business ideas or inquiries; or

   i. Promotion or endorsement of commercial services, products, or entities. (Note that non-commercial links that are relevant to the topic or another comment are acceptable.)

3. Questions regarding the removal of comments should be directed to the Office of General Counsel and the DHS Office of Public Affairs.

4. Comments containing an imminent threat or a threat against a person or place will be immediately reported through appropriate law enforcement channels.

5. Aside from the specific guidelines outlined in the DHS Moderation/Comment policy, the Department does not control, moderate, or endorse the comments or opinions provided by general public users on official DHS accounts.

6. If available on the service, DHS Social Media and other Third-Party Digital Service accounts are approved to use profanity filters, such that it meets the comment policy outlined above, but does not limit free and open expression of speech.

J. ***Liking/Following/Blocking:***

1. Anyone in the general public can like/follow a DHS Social Media or other Third-Party Digital Service account.

2. Members of the general public who consistently and repeatedly violate the comment or privacy policy set forth by DHS for a DHS official account can be blocked from interacting with that account using the tools provided by the Social Media or other Third-Party Digital Service. Great care should be exercised when deciding whether to block a member of the public and detailed reasons for blocking should be documented and retained. It is recommended that account managers consult with the Office of General Counsel before blocking a member of the public's account.

3. Official DHS accounts will only like and/or follow verified/official accounts that are related to the mission or activities of the Department.

4. Care should be taken when liking and following content created by non-governmental entities to avoid the appearance of US government or Department endorsement of non-governmental statements, activities, or positions.

5. Official account activity, including liking, following, and blocking, should not reflect or promote personal interests or values.

K. ***Privacy:***

1. While DHS may use a Social Media or other Third-Party Digital Services, these platforms, by definition, are controlled and operated by third parties that maintain and provide their own privacy and use policies.

2. As part of the approval process for the service, the DHS Office of Public Affairs coordinates with the DHS Privacy Office to complete a Privacy Threshold Analysis and, if necessary, a Privacy Impact Assessment (PIA) for the individual service.

3. The privacy policy/notice for each Social Media or other Third-Party Digital Service approved for public communications use is available on

DHS.gov.

4. Account Managers are responsible for ensuring that DHS engages on these platforms in a manner that protects privacy, including the blurring or obfuscating the identity of those with a reasonable expectation of privacy, and does not solicit or collect PII.

5. Collection, maintenance, and retention of PII is prohibited unless authorized by DHS privacy policies and in accordance with federal law. This prohibition includes the collection, maintenance and retention of federal records related to non-operational situational awareness.

L. ***Records Management:***

1. All original content generated by DHS is subject to the National Archives and Records Administration (NARA) records retention schedules for retention, storage and publication. The NARA-approved DHS Enterprise-wide records retention schedule requires social media records be retained for at least five (5) years.

2. Social Media and other Third-Party Digital Service accounts created or used for official Department business must stay under the control of the Department, including accounts created for (or by) employees and used in an official capacity. These accounts are retained by the Department after that employee has left.

3. DHS requires the creation of unique Department-administered accounts when an employee uses a Social Media or other Third-Party Digital Service platform on behalf of the Department. This allows for a clear delineation of when an employee is acting in an official or personal capacity. The only exception is if a personal account is required by a platform to log in to/access an official DHS account.

4. Departing employees will remove two-factor authentication (if applicable) and provide the login credentials (username and password) for any official Social Media or other Third-Party Digital Service accounts (or personal accounts used for Department business) to the office administering the account (or DHS Office of Public Affairs upon request) prior to their departure.

5. Account Managers must copy and forward Federal records created or received by official Department accounts to the appropriate headquarters or component records management office within 20 days of closing an account.

6. Account Managers are responsible for coordinating with the appropriate headquarters or component records management office to

affect the quadrennial archival of the Social Media or other Third-Party Digital Service account as required by NARA.

M. ***Security/Multi-Factor Authentication/Password Protection:***

1. Unless otherwise specified, the following guidelines must be followed with regards to account/password security for Social Media and other Official Third-Party Digital Service accounts:

a. Use Multi-factor Authentication (MFA) when available from the Social Media or other Third-Party Digital Service;

b. Password must be at least 8 characters in length; however a 12 character minimum is highly recommended for strong security;

c. Password must contain a random mixture of keyboard characters such as lowercase, uppercase, digit (number), punctuation, or special characters;

d. Password must be changed if the password is compromised or suspected compromise and previously used passwords should not be reused;

e. Password must not contain your system username, a dictionary word, or common patterns known to malicious actors such as the first character being capitalized and the last characters being the only digit, punctuation, or system; and

f. If a password requires a change, the same previous password reuse with just an increase in a digit (number) shall not be used.

2. Creating a stronger password with an increased length, eliminates the need to periodically change the password on a set change period; however, a strong password meeting the above must be used.

3. Prior to the creation of the account, account managers must provide a copy of their DHS Cybersecurity Awareness Training certificate to the DHS Office of Public Affairs (for headquarters accounts) or Component Public/External Affairs (for component accounts). The Cybersecurity Awareness Training must be for the same fiscal year they are requesting an account and must be submitted yearly thereafter while the account is active.

VII. Questions

Address any questions or concerns regarding this Instruction to the DHS Office of Public Affairs.

DANIEL M WATSON Digitally signed by DANIEL M WATSON
Date: 2023.07.28 21:06:27 -04'00'

Daniel Watson
Assistant Secretary for Public Affairs

Date