DoD Instruction 5400.17

Official Use of Social Media for Public Affairs Purposes

Originating Component: Office of the Assistant to the Secretary of Defense for Public Affairs

Effective: August 12, 2022

Releasability: Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.

Approved by: Gordon Trowbridge, Acting Assistant to the Secretary of Defense for Public Affairs

---

Purpose: In accordance with the authority in DoD Directive (DoDD) 5122.05 and DoD Instruction (DoDI) 8170.01, this issuance:

- Establishes policies and provides procedures:
  - For initiating an external official presence (EOP) on social media platforms for public affairs (PA) purposes.
  - To maintain an EOP on social media platforms.
- Assigns responsibility to OSD and DoD Components for EOP on social media platforms.
- Provides:
  - Core principles regarding social media use within DoD.
  - Guidance regarding records management procedures for social media accounts.
  - Guidance on personal social media use by DoD personnel.

TABLE OF CONTENTS

FIGURES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

a. This issuance:

(1) Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").

(2) Does not apply to social media accounts established for marketing activities by Military Service recruiting commands, in accordance with DoDI 1304.35.

b. Nothing in this issuance should be construed as preventing the Inspector General of the Department of Defense from fulfilling their duties pursuant to Sections 7321-7326 of Title 5, United States Code (U.S.C.), Appendix, also known as the Inspector General Act of 1978, as amended.

1.2. POLICY.

a. It is DoD policy to use official DoD accounts on non-DoD controlled social media platforms to amplify timely and relevant information about the national security, defense strategy, and appropriate unclassified work of the Department.

b. It is DoD policy that:

(1) The ability to adapt to changing trends and technologies on dynamic social media platforms is needed to take full advantage of social media as a communication tool and in support of the National Defense Strategy in accordance with Section 113(g) of Title 10, U.S.C.

(2) The integration of social media is an integral element of DoD strategies to communicate official information publicly in accordance with DoDI 8170.01.

(3) Information communicated by OSD and DoD Components on official social media accounts constitutes a segment of PA activities, in accordance with DoDI 5400.13, DoDD 5122.05, and this issuance.

(4) Information disclosed will be in compliance with the DoD Principles of Information in accordance with DoDD 5122.05.

SECTION 2: RESPONSIBILITIES

2.1. ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS (ATSD(PA)).

The ATSD(PA):

a. Is the principal spokesperson for DoD and responsible for ensuring a free flow of information to the news media, general public, internal audiences of DoD, and other applicable forums through official DoD social media accounts managed by OSD and DoD Components, in accordance with DoDD 5122.05.

b. Provides the final approval for all EOPs established by OSD and DoD Component heads in accordance with DoDI 8170.01 concerning the use of social media.

c. May direct the removal of any official social media account that does not adhere to the policy, procedures, and instructions provided in this issuance.

d. Oversees the implementation of integrated communication strategies that incorporate digital media content on official DoD social media accounts.

e. Provides guidance and direction for OSD and DoD Components to use publicly available information (PAI) for PA activities through third-party social media management platforms, in accordance with DoDD 3115.18.

f. Ensures the conduct of appropriate pre-publication security and policy reviews in accordance with DoDIs 5230.09 and 5230.29, as applicable.

2.2. DOD CHIEF INFORMATION OFFICER.

The DoD Chief Information Officer:

a. In coordination with ATSD(PA), oversees implementation of policy and procedures for ensuring the quality of information the DoD disseminates to the public.

b. On a limited, case-by-case basis, reviews requests by OSD and DoD Component heads to negotiate terms of service with a non-DoD controlled electronic messaging service. In coordination with the ATSD(PA), Chief Digital and Artificial Intelligence Officer, and DoD Office of General Counsel, the DoD Chief Information Officer reviews the request in accordance with DoDI 8170.01.

2.3. OSD AND DOD COMPONENT HEADS.

The OSD and DoD Component heads:

a. May establish EOPs for their Components, in accordance with the provisions of Section 4.

b. May establish Component-specific social media regulations to manage social media managers, accounts, and activities.

c. For any EOP they establish, ensure proper management of records created or received through activity of the EOP throughout the lifecycle of the records in accordance with DoDI 5015.02.

SECTION 3: CORE PRINCIPLES OF SOCIAL MEDIA USE WITHIN DOD

3.1. OFFICIAL USE OF SOCIAL MEDIA.

a. Social media communication provides the opportunity and responsibility to communicate directly to the public. DoD uses official social media accounts for the sake of transparency and to disseminate information.

b. If social media is mismanaged or mishandled, the U.S. Government's reputation with the American public; relationships with interagency, international, State, local, and tribal entities; military operations; and reputation for a high ethical and professional standard may be compromised. DoD social media content can be consumed by any audience, intended or unintended, foreign or domestic. All DoD PA and social media managers should understand that even the smallest or newest official account will be interpreted as a representative of the whole of DoD.

c. DoD personnel may establish accounts for personal, non-official use in accordance with DoDI 8170.01. Personal accounts may not be used to conduct official DoD communications, unless by exception identified in Paragraph 3.26.a of DoDI 8170.01. DoD personnel must ensure that their personal social media accounts avoid use of DoD titles, insignia, uniforms, or symbols in a way that could imply DoD sanction or endorsement of the content. Where confusion or doubt is likely to arise regarding the personal nature of social media activities, personnel are encouraged to include a disclaimer clarifying that their social media communications reflect only their personal views and do not necessarily represent the views of their agency or the United States. See Section 8 of this instruction for additional guidance on the personal use of social media by DoD personnel.

3.2. DOD SOCIAL MEDIA PRINCIPLES.

The following principles will apply to official use of social media for PA purposes:

a. Governance.

OSD and DoD Component PA teams oversee and provide guidance on the use and management of official DoD social media accounts. Communications will align with and support PA objectives and efforts across all platforms.

b. Professionalism.

All official social media content is a reflection of the Department. When posting to official social media accounts, content should meet well-defined, appropriate objectives. Public Affairs Officers will remain respectful, responsive, and genuine, and exercise the same high standard of professional and ethical behavior on social media accounts as they do during any other function or on any other platform. Content should inspire and engage with audiences. At no time, however, should such content undermine the Department's efforts to remain a good steward of the public trust. No content will be released that could be reasonably construed as offensive, inappropriate, or unbecoming. Official social media accounts must not be used to promote or endorse non-Federal entities or personal financial interests. Only designated DoD personnel may authorize release of information on social media accounts; contractor personnel may support EOP maintenance but cannot authorize the release of public information.

c. Propriety.

Posts released from official DoD social media accounts must be:

(1) Accurate. The content is accurate.

(2) Appropriate. The account is the proper vehicle for the message.

(3) Timely. The message can be delivered at the proper time.

(4) In the Appropriate Tone. The message is being delivered in the proper tone.

(5) Approved for public release. The message has been reviewed for operations security and information security concerns and approved for public release, in accordance with DoDIs 5230.09 and 5230.29, as applicable.

d. Acumen.

PA officers and social media account managers should proactively maintain currency in the latest social media tactics, best practices, and trends, coupled with an understanding of and ability to apply PA objectives (e.g., as articulated in the DoD Communications Playbook). Social media account managers must complete operations security training Level 2 and be prepared to act quickly and implement evolving capabilities intelligently to remain effective in the use of the platform.

e. Establishment Need.

New official accounts should only be established if a specific communications outcome cannot be fulfilled by an existing account(s) or other means of communication. More for the sake of more is not necessarily better.

f. Transparency.

Social media account managers will not remove social media content from official DoD accounts unless there is a factual or typographical error; violation of a law, policy, term of service, or user agreement; or an operations or information security concern. Removal of content will be publicly acknowledged and communicated to audiences to provide context and appropriate clarification for the action; managers must persistently monitor, communicate, and, where appropriate, responsively engage with users regarding such removal. Removal of content can unintentionally discredit DoD information if the action appears to be taken to:

(1) Avoid embarrassment;

(2) Stifle or silence discussion about a controversial topic; or

(3) Mislead users to believe an issue is inconsequential or of minor significance.

SECTION 4: DOD EOP

4.1. ESTABLISHING AN OFFICIAL PRESENCE.

a. Considerations Concerning Official Accounts.

(1) OSD and DoD Components must assess the communication value of establishing an official presence on approved social media platforms to provide timely and accurate information to the public and the news media in accordance with DoDD 5122.05 and Paragraph 3.24 of DoDI 8170.01.

(2) The creation of EOPs on social media platforms should be carefully considered and avoided, unless the proposed EOP meets a specific communications objective that is not being fulfilled by any existing EOP or other PA activities. Commands at all levels will consolidate and deactivate EOPs that detract or disrupt users searching for official DoD information. Content on any deactivated official accounts must be archived in accordance with DoDI 5015.02.

(3) Organizations that identify a communication need that can be satisfied through social media should evaluate available resources to establish and manage an account with the intent to build and engage audiences, and use analytics to elevate their digital impact.

(4) PA offices should be resourced with the industry standard equipment, training, and personnel to manage social media accounts, especially over multiple social media platforms, including public web activities pursuant to DoDD 5122.05.

(5) Pursuant to Paragraph 3.24.k. of DoDI 8170.01, mission-related contact information must be used to establish an EOP.

(6) DoD personnel managing or having access to an official social media account will coordinate with their local information technology offices and sign an acceptable use policy agreement for tracking purposes in accordance with Component cybersecurity regulations.

(7) Acceptable use policy agreements must include the statements in Figure 1. If the existing acceptable use policy agreement does not contain the language in Figure 1, it should be amended accordingly or a standalone acknowledgement containing the language in Figure 1 should be signed.

Figure 1. Mandatory Acceptable Use Policy Agreement Statements

I will use official DoD social media accounts on non-DoD-controlled social media platforms (e.g., Facebook, YouTube, Twitter, Instagram) only as authorized by my job or duty description and to conduct official business, including to release official agency information or other official communication. I will not use personal social media accounts to conduct official business except as authorized in accordance with DoDI 8170.01.

b. Registering an Account.

(1) All DoD owned and/or operated social media accounts must be registered at https://www.defense.gov/Resources/Register-a-Site/ and must register with the U.S. Digital Registry at https://www.digitalgov.gov/services/u-s-digital-registry/ in accordance with DoDI 8170.01.

(2) Registering accounts constitutes the official status for DoD social media accounts on authorized platforms.

c. Establishing EOPs for OSD and DoD Component Heads.

(1) In coordination with the ATSD(PA), OSD and DoD Component heads approve the creation of individual social media accounts for their positions. OSD and DoD Component heads will submit an action memo to the ATSD(PA) requesting the establishment of a new individual or institutional social media account.

(2) DoD personnel, including OSD and DoD Component heads and other military and civilian leaders, are prohibited from converting personal accounts to official DoD accounts associated with their DoD position, title, duty, component, or any other DoD organizational entity.

(3) OSD and DoD Component heads are authorized to close or archive any social media accounts deemed unnecessary and of no informational value to the public, media, or mission of the Component. The process to archive and close a social media account is provided in Paragraph 7.1.e.

d. EOPs Below the Component Level.

(1) OSD and DoD Component heads, in consultation with PA, will review and determine the criteria for establishing an EOP for elements within their responsibility to operate and execute their PA activities. PA representatives should assess establishing an EOP based on mission or operational needs and support of approved communication plans and campaigns.

(2) EOPs at all levels must follow the procedures, policies, and guidelines outlined in this issuance. Organizations that establish an EOP will provide guidance to social media managers to effectively direct activities and properly maintain the organization's public presence.

4.2. NEW AND EMERGING PLATFORMS.

a. PA and social media managers must consider the communication value of expanding their digital presence and conduct researched analysis of new platforms. Some of the elements that PA and social media managers should consider include, but are not limited to, audience analysis, content strategy for the platform, and available resources. Approving officials should obtain data-driven decisions from PA and social media managers and ensure compliance with Paragraph 3.24 of DoDI 8170.01 before accepting recommendations to expand their digital footprint.

b. The process to review platforms for official presence requires an application to be vetted through the Defense Information Systems Agency's DoD Application Vetting Environment. The application must be submitted after coordination with the Component Chief Information Officer to ensure all information provided s complete.

c. Once the DoD Application Vetting Environment review process is completed, the Defense Information Systems Agency will issue a decision. This decision is applicable for all OSD and DoD Components and is considered final.

d. PA and social media managers should **not** test, use, or otherwise engage on new platforms for official use (including on personal devices) prior to undertaking the steps in Paragraphs 4.2.a- c.

SECTION 5: BRANDING GUIDELINES

5.1. CLEAR IDENTIFICATION.

To maintain an EOP, all DoD Components will adhere to branding guidelines in accordance with DoDD 5535.09 and:

a. Provide clear identification that they are supplying the content for the EOP.

b. State their mission and provide the purpose of the EOP, as workable.

c. Will not mislead users of the site as to the originator of the EOP.

5.2. OFFICIAL DOD AND MILITARY DEPARTMENT AND SERVICE SEALS VS. EMBLEMS AND LOGOS.

a. The use of the official DoD seal, official Military Department seals, and official Military Service seals on EOP accounts is reserved for official communication only, such as letterheads, and briefing documents. The use of DoD and Military Service emblems, logos, or coats of arms may be more appropriate for general use on EOPs to affiliate the account with DoD. Social media managers should reference Component guidance for the appropriate uses of Component marks for official social media use.

b. DoD and OSD Components should develop Component-specific guidance for the use of their emblems or logos on EOPs and social media content.

SECTION 6: AUTHORIZED ACCOUNTS

6.1. OFFICIAL SOCIAL MEDIA CONDUCT.

a. All EOPs and their content represent DoD, reflect the values of the Department, and serve as official communication platforms to the general public, the news media, and internal audiences of DoD. Content posted on official accounts is subject to the same guidance, policy, regulations, and oversight for the release of official DoD information.

b. PA chiefs and social media managers must establish communication planning techniques to ensure the information published on a social media account is synchronized and approved for release. Social media content management software and tools may be used for PA activities.

c. PA chiefs, social media managers, and other DoD personnel operating official individual accounts must ensure all content is reviewed and approved for public release in accordance with DoDIs 5230.09 and 5230.29, as applicable.

d. While not exhaustive, the following restrictions apply to the official use of social media by DoD personnel. Restrictions pertaining to the personal use of social media by DoD personnel are addressed in Section 8 of this instruction and in the standards of conduct that apply to DoD personnel through DoD 5500.07-R and applicable Office of Government Ethics regulations.

(1) Misuse of Position.

DoD personnel will not:

(a) Use their official position or public office for private gain, for the endorsement of any product, service, or enterprise, or for the private gain of friends, relatives, or other acquaintances.

(b) Use or permit the use of their government position or title or any authority associated with their public office in a manner that is intended to coerce or induce another person to provide any benefit, financial or otherwise, to themselves or to friends, relatives, or persons with whom the employees are affiliated in a nongovernmental capacity.

(c) Use their government position or title in a manner that could reasonably be construed to imply that the government endorses or sanctions their personal activities or those of another. The use of one’s official position or public office may include the use of any reference to one’s status, name, image, or likeness as a DoD employee or member of the uniformed services.

(2) Use of Government Time and Property.

Section 2635 of Title 5, Code of Federal Regulations and DoD 5500.07-R require that DoD personnel use official time in an honest effort to perform official duties. These regulations and standards also require employees and Service members to protect and conserve government property and to use government property only to perform official duties, unless they are authorized to use government property for other purposes.

(3) Use of Non-Public Information.

(a) DoD personnel may not disclose non-public information on official or personal social media accounts. They will not allow the improper use of non-public information to further their own private interest or that of another.

(b) PA offices, social media managers, and other DoD personnel operating EOP accounts will report known or suspected occurrences of information on the accounts that is not authorized for release to their Component's security office and insider threat hub, and respond based on applicable DoD policy.

(4) Misuse of Personal Accounts.

DoD personnel must only use official DoD social media accounts to disseminate official information. DoD personnel are prohibited from using personal social media accounts for official purposes, including for conveying DoD information or official DoD positions. This does not prohibit using personal social media accounts to forward, like, or link to official information, provided it is done in a manner that does not express or imply DoD sanction or endorsement of any personal content.

(5) Political Activity.

(a) Engaging in political activity on official DoD social media and EOP platforms is prohibited. Additionally, DoD personnel may not engage in political activity, on their personal social media, while in the Federal workplace or while on-duty including while teleworking. Political activity is defined as an activity directed toward the success or failure of a political party, candidate for partisan political office or partisan political group.

(b) Certain DoD personnel have additional restrictions. Guidance on political activity restrictions is available from the DoD Standards of Conduct Office, https://dodsoco.ogc.osd.mil/.

(6) Discrimination, Harassment, and Extremism.

In accordance with DoDI 1020.03 and DoDI 1020.04, all DoD personnel must maintain an appropriate level of professional conduct and treat others in the workplace with dignity and respect. Military personnel are prohibited from actively participating in extremist activities in accordance with DoDI 1325.06, which can include activity on social media. At all times, DoD personnel must adhere to the terms of service and community guidelines dictated by the social media platform and to applicable DoD discrimination, harassment, and extremism policies. On official DoD social media and EOP platforms, engaging in activities that are illegal, inappropriate, or offensive to fellow users or to the public is prohibited. Such activities include, but are not limited to:

(a) Hate speech or material that ridicules others on the basis of race, religion, color, sex, disability, national origin, gender-identity, or sexual orientation.

(b) Speech or material promoting violent extremist or terrorist activities.

(c) Speech or materials advocating the overthrow of the government.

(7) Children.

Agency social media accounts may not collect any personal information from children (i.e., individuals under the age of 13), consistent with the standards of the Children's Online Privacy Protection Act (Section 6501-6506 of Title 15, U.S.C.) as applied to Federal agencies by Office of Management and Budget Memorandum M-03-22.

(8) Professionalism.

DoD personnel will at all times adhere to applicable standards of professionalism, including as provided in this issuance.

(9) Possible Collection of Personally Identifiable Information (PII).

All DoD personnel must limit the collection, use, maintenance, and dissemination of PII in accordance with DoDI 5400.11.

6.2. PA OFFICIAL USE OF SOCIAL MEDIA.

There are three types of official social media accounts for official use within DoD: organizational, institutional, and individual. These account types are used to release official DoD information and visual information materials. Any public disclosures must comply with DoDI 5230.09 and DoDI 5230.29, as applicable.

a. Official Organizational Accounts.

Official organizational accounts communicate on behalf of the DoD or OSD Component or program, and are representative of the DoD and Federal Government digital presence for public information (e.g., @USArmy or @DeptofDefense). Organizational accounts are communication platforms of an agency's digital brand strategy and managed by a team that has access to the account to publish content that supports a communication plan.

b. Official Institutional Accounts.

(1) Official institutional accounts are denominated only with an official position title (e.g., @SecDef, @DepSecDef) and are not associated with a personal name. These accounts are managed by the individual in the position in coordination with a PA office.

(2) When the official vacates the position, social media managers will archive the content of their account. PA representatives will assess the communication value to transition the account to the incoming official or archive the account. The out-going official is prohibited from maintaining the account. If the account is archived, PA and social media managers will

inform audiences that the account is no longer maintained and redirect users to platforms or accounts that will provide information of similar interest.

c. Official Individual Accounts.

(1) Official individual accounts include a personal name or identifier (e.g., @DASDSmith). Individual accounts are the least preferred account type due to the custom name associated with a position title.

(2) Individuals may not merge, rename, or convert a personal account or prior non-DoD account into a DoD EOP.

(3) Individuals serving in DoD who assume a new position and title within DoD may not merge, rename, or convert a prior official individual account to a personal account. The prior individual account expires once the individual is no longer associated with the position or title.

(4) Individuals with an official DoD individual account who depart DoD may not merge, rename, or convert the official DoD individual account into another account, personal or otherwise. The prior DoD individual account expires once the individual is no longer associated with the DoD position or title.

(5) Individuals from one OSD or DoD Component who are assigned to another joint, interagency, intergovernmental, or multinational entity may establish an EOP for their position in this new entity in accordance with Paragraph 4.1. The social media account is non-transferrable and expires once the individual is no longer associated with that entity.

6.3. MILITARY MARKETING AND RECRUITMENT ACCOUNTS.

Although this issuance does not apply to military recruitment/marketing accounts, social media accounts for PA activities may support local or national recruitment efforts by amplifying appropriate content on their account. In accordance with DoDI 1304.35, recruiting personnel will coordinate with local PA chiefs when conducting marketing engagement or other community events, in accordance with Paragraph 3.3 of DoDI 1304.35.

SECTION 7: MAINTAINING AN EOP

7.1. RECORDS MANAGEMENT.

a. DoD Information Security

DoD personnel must ensure that only information authorized for release is released to the public via social media, in accordance with DoDIs 5230.09 and 5230.29, as applicable.

b. Managing Social Media Records.

(1) Any content posted by DoD to an EOP is an official communication, regardless of the format.

(2) The records associated with the EOP will be managed in accordance with the appropriate OSD or DoD Component records schedule pursuant to Part 1226 of Title 36, Code of Federal Regulations.

(3) A complete social media Federal record must have content, context, and structure, along with associated metadata. The complete record must be maintained pursuant to OSD or DoD Component records management policies and procedures to ensure reliability and authenticity.

(4) Derogatory, inappropriate, and offensive content posted on an EOP by a user on the platform must be addressed in accordance with the terms of service and acceptable online conduct guidelines. Social media and records managers should evaluate the content in context, including whether a DoD response was provided, to determine if the post is a Federal record.

c. Capturing Social Media.

(1) Social media managers and other DoD personnel responsible for retaining social media content on behalf of their component can use the following non-exhaustive list of questions to help determine the appropriate disposition authorities applicable to a social media post:

(a) Does it contain evidence of the department or agency's policies, business, or mission?

(b) Is the information only available on the social media site?

(c) Does the agency use the social media platform to convey official agency information?

(d) Is there a business need for the information?

(2) Methods to capture social media records include:

(a) Using web crawling or other software to create local versions of sites.

(b) Using web capture tools to capture social media.

(c) Using platform-specific application programming interfaces to pull content.

(d) Using Really Simple Syndication feeds, aggregators, or manual methods to capture content.

(e) Using tools built into some social media platforms to export content.

(3) The options for successful social media capture will depend on the technical configuration of a social media platform. Component needs may also affect which social media capture method is used. Once the Component determines the capture method, they must provide training to applicable staff on how and when to use capture tools for social media. Components may need to work with third-party providers to implement social media capture.

d. Private or Direct Messages from DoD Social Media Accounts.

(1) Engaging in private or direct messaging to communicate official DoD information from DoD social media accounts should be conducted with care.

(2) Private or direct messaging is allowed if PA and social media managers identify a specific need to remain responsive to authentic public interest or questions.

(3) Due to potential preservation issues, DoD social media accounts may not send direct or private electronic messages that automatically expire.

(4) If public comments on or to a DoD social media account warrant a non-public response, the DoD social media account manager(s) should publicly comment on the post(s) and suggest the individual(s) email the specific question(s) to the official DoD email account displayed in the profile.

e. Account Transition and Archiving of Official Social Media Accounts.

Consistent with Paragraph 6.2 of this instruction, DoD personnel operating an EOP may not retain official accounts or access to any official accounts in a personal capacity after departing the government or the government position associated with the account, as applicable.

(1) Official Organizational and Institutional Accounts.

(a) Within 30 days after the departure of the official associated with the institutional account, content posted to the account during the departing official's tenure must be managed and preserved in accordance with the proper records schedule.

(b) OSD and DoD Components should follow the most pertinent records schedule, in consultation with their records manager, because not every Component has a records schedule specific to social media records. This is to ensure the records are preserved appropriately if the new official chooses not to use the previously established official presence.

(c) On the final day of activity for the account, PA and social media managers will post a final message, and provide the password and login information to the designated point of contact for use by the next official.

(d) If the new official indicates he or she does not want to use the official institutional account before the account holder's final day of service, the account should be closed, and the associated records managed in accordance with the proper records schedule.

(2) Official Individual Account.

Within 30 business days after the departure of the official associated with the official individual account, all content posted to the account during the departing official's tenure must be managed and preserved in accordance with the proper records schedule. On the final day of activity for the account, the account will issue its final content and the account will be closed.

7.2. USE OF PAI FOR PA.

a. Public engagement on social media platforms requires situational awareness of the information environment. PAI enables PA to generate audience insights, provides social media trend analysis, and inform leaders of emerging communication crises. In accordance with DoDD 3115.18, and Appendix 3A of DoDI 8170.01, PA offices may access and use PAI for PA activities.

b. PA offices may use third-party social media management platforms or services to manage official social media accounts. OSD and DoD Component PA offices must follow acquisition processes and procedures to obtain authorization for software or services. PA offices may need to coordinate with relevant Component offices, including their Chief Information Officer, for additional instructions, guidance, and policy to access third-party or commercial off-the-shelf services to access PAI.

c. PA offices with authorization and authority to use third-party social media management platforms must maintain records management procedures in accordance with Paragraph 7.1.

d. PA offices will coordinate with their local records manager for specific guidance and recommendations to capture and schedule records through third-party content scheduling platforms, if the platform or service has the capability or function to capture social media records. PA offices default to capturing and scheduling records directly from the social media platform if the content scheduling platform is inadequate or incapable of providing content, context, and structure along with associated metadata for records management.

7.3. RISKS ASSOCIATED WITH OPERATING EOP.

a. Social Media Cyber-Vandalism.

(1) Responding to cyber-vandalism events involving official social media accounts is the responsibility of multiple officials including, but not limited to, PA officials, social media account manager(s), legal advisors, and information technology security personnel. These key personnel form the response team that must establish incident response procedures, consistent with DoDIs 8500.01 and 8170.01. The response team must exercise and rehearse various scenarios to quickly assess, recover, and respond to an incident. The response team manages the process to ensure all elements of the incident are reported and addressed. The response team will determine when the incident is closed.

(2) The response team should conduct an incident after-action report and assessment to review, update, or draft procedural tasks, regulations, or policy.

(3) A template response to cyber-vandalism is provided through the General Services Administration's Technology Transformation Services at https://digital.gov/resources/readiness-recovery-response-social-media-cyber-vandalism-toolkit/. The response team should amend and adapt the template as necessary to conform to its Component's guidance, regulations, and policies.

b. Fake or Imposter Social Media Accounts of DoD Employees and Service Members.

Users, malign actors, and adversaries on social media platforms may attempt to impersonate DoD employees and Service members to disrupt online activity, distract audiences from official accounts, discredit DoD information, or manipulate audiences through disinformation campaigns. PA offices managing an EOP must address fake or imposter accounts.

(1) Reporting Fake or Imposter Social Media Accounts.

(a) PA chiefs and social media managers must report fake or imposter accounts through the social media platform's reporting system. Social media platforms and applications establish the information requirements to report such accounts. PA offices must establish local procedures to identify, review, and report fake or imposter accounts. PA and social media managers must notify operations security officials of fake or imposter accounts, as well as cyber operations, counterintelligence elements, and Military Department Counterintelligence Organization in accordance with DoDD 5240.06

(b) PA chiefs and social media managers must record the reporting of fake or imposter accounts.

(c) PA chiefs or social media managers may need to provide additional information as evidence that the identified account is fake or impersonating a DoD official.

(2) Indications or Common Identifiers Associated with Imposter Accounts.

Indications or common identifiers associated with imposter accounts include, but are not limited to the following:

(a) The account is not registered as an official DoD account.

(b) The account has very few photos that were recently uploaded and reflect the same date range.

(c) The account has very few followers and comments.

(d) The account sends friend requests to individual users on the platform.

(e) The account name and photos do not match.

(f) There are obvious grammatical or spelling errors.

(g) Key information is missing.

7.4. LINKING AND SHARING FROM OFFICIAL SOCIAL MEDIA ACCOUNTS.

a. In accordance with DoDI 8170.01, OSD and DoD Components may establish hyperlinks only to information or services related to the performance of the DoD Component's function or mission and the purpose of the electronic messaging service. Any links from an official social media account must comply with DoDI 8170.01, section 3.20.

b. DoD cannot endorse, sponsor or advertise on behalf of another non-government service, facility, event, or product. The use of external links on official accounts may convey a misrepresentation of government endorsement or provide an incorrect interpretation of DoD policy, position, or message. DoD officials, PA chiefs, and social media managers of EOP must assess the information value of the source before sharing an external link by considering factors including, but not limited to, the author and publisher's credibility, the validity of the information at the source, the references or subject matter experts cited within the source, and whether the information is true and factual. When external links to non-U.S. Government websites are posted on official social media accounts, content managers will include the following disclaimer: "The appearance of external hyperlinks does not constitute endorsement by the United States Department of Defense of the linked websites, or the information, products or services contained therein. Other than for authorized activities, such as military exchanges and Morale, Welfare and Recreation sites, the United States Department of Defense does not exercise any editorial control over the information you may find at these locations." Content managers will not direct users to paid sites or subscription services.

c. OSD and DoD Component EOPs may link and share content found on DoD-registered, public-facing websites, and social media platforms without formal coordination.

d. PA and social media managers will establish local guidelines to share external links from non-DoD sources that support PA activities, including a specific, mission-essential reason or a Commander's information objective(s) in accordance with DoDI 8170.01.

7.5. SOCIAL MEDIA PLATFORM VERIFIED ACCOUNTS.

a. EOPs registered with DoD do not need to display a "verified" status with the social media platform to be recognized by DoD as an official account. While PA chiefs and social media managers should attempt to have an EOP recognized as a verified account by the social media platform for all account types, they are not required to do so. All registered EOPs in the DoD registry or the U.S. Digital Registry are official accounts, in accordance with Paragraph 4.1.b.

b. A "verified" personal account on a social media platform does not constitute an official DoD account. Personal accounts that are "verified" as a government account by a social media platform may be misconstrued as an official DoD account.

SECTION 8: PERSONAL SOCIAL MEDIA USE BY DOD PERSONNEL

DoD personnel may use unofficial personal social media. In doing so, DoD personnel must adhere to the rules discussed in this instruction, including preventing the unauthorized disclosure of non-public information (or unclassified information that aggregates to reveal classified information) and refraining from any appearance of DoD endorsement or sanction. The following guidance applies to DoD personnel who maintain a personal social media presence.

a. Maintain a Clear Distinction Between Personal and Official Accounts.

(1) DoD personnel must ensure that all personal social media accounts are clearly identifiable as personal accounts. DoD personnel must ensure that their personal social media accounts avoid use of DoD titles, insignia, uniforms, or symbols in a way that could imply DoD sanction or endorsement of the content. DoD personnel should use personal, non-official contact information, such as personal telephone numbers or postal and e-mail addresses, to establish personal, nonofficial accounts.

(2) Where confusion or doubt is likely to arise regarding the personal nature of social media activities, personnel are encouraged to include a disclaimer clarifying that their social media communications reflect only their personal views and do not necessarily represent the views of their agency or the United States. (See sample disclaimer Figure 2.) The use of a disclaimer does not otherwise allow DoD personnel to accept compensation that is prohibited by this instruction or other applicable regulations.

Figure 2 Sample Disclaimer for Personal Social Media Accounts

The views and opinions presented herein are those of the author and do not necessarily represent the views of DoD or its Components. Appearance of, or reference to, any commercial products or services does not constitute DoD endorsement of those products or services. The appearance of external hyperlinks does not constitute DoD endorsement of the linked websites, or the information, products or services therein.

(3) DoD personnel are not prohibited from using personal social media accounts to forward, like, or link to official information, provided it is done in a manner that does not express or imply DoD sanction or endorsement of any personal content.

b. Do Not Disclose Non-Public Information.

DoD personnel are prohibited from disclosing non-public information to further their private interests or the private interests of others. Additionally, DoD personnel must adhere to operations security and unit-level directives, including while in forward-operating environments. Release of unauthorized content through any means, including social media, may unnecessarily hazard individuals, units, and the mission.

c. Do Not Conduct Official Business on Personal Social Media Accounts.

(1) Personal accounts may not be used to conduct official DoD communications, in accordance with Paragraph 3.26.a of DoDI 8170.01 and Section 2911 of Title 44, U.S.C.

(2) A personal social media account must not be an avenue for friends, followers, or private contacts to gain access to DoD programs or seek action from DoD officials in a manner not available to the general public.

d. Do Not Accept Compensation for any Activity Relating to One's Status as a DoD Civilian Employee or Military Service Member.

DoD personnel are prohibited from using their official position or public office for personal financial gain, for the endorsement of any product, service, or enterprise, or for the private gain of friends, relatives, or persons with whom the employee is affiliated in a nongovernmental capacity. (Section 2635.702 of Title 5, CFR). DoD personnel are also prohibited from using government resources for non-official, personal activities.

(1) Use of Official Position or Public Office.

The use of one's official position or public office includes the use of any reference to one's status, name, image, or likeness as a DoD civilian employee or Service member. This includes the use of official titles, photographs that display a connection to one's status as a DoD civilian employee or Service member (e.g., a photograph while in uniform or while wearing an identifying device such as a lanyard or lapel pin); and the personal use of DoD protected symbols or other imagery.

(2) Endorsement.

DoD personnel are prohibited from using their official positon to either affirmatively endorse a non-federal entity, product, service, or enterprise, or by taking action that implies DoD endorsement through the unauthorized use of one's official position or public office.

(3) Private Gain.

Private gain includes the receipt of compensation from a third party, to include revenue from advertising, sponsorships or sponsorship agreements, affiliate marketing agreements, or promotion of commercial ventures on personal social media accounts. This does not preclude DoD personnel from engaging in compensated outside employment when permitted by applicable ethics and other regulations.

e. Do Not Engage in Prohibited Political Activity, as Defined in Applicable Law and Regulation.

See Paragraph 6.1.d.(5) of this instruction.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
ATSD(PA)	Assistant to the Secretary of Defense for Public Affairs
DoDD	DoD directive
DoDI	DoD instruction
EOP	external official presence
PA	public affairs
PAI	publicly available information
U.S.C.	United States Code

G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
counterintelligence	Defined in DoDD 5240.02.
DoD personnel	DoD civilian employees and military service members. For purposes of this issuance, "DoD personnel" does not include employees of DoD contractors.
electronic messaging services	Defined in DoDI 8170.01.
EOP	Defined in DoDI 8170.01.
Federal record	A "record" as defined in Section 3301 of Title 44, U.S.C.
manager	DoD employee or Service member responsible for managing DoD social media EOPs.
marketing	Defined in DoDI 1304.35.
Military Department Counterintelligence Organization	Defined in DoDD 5240.02.

TERM	DEFINITION
non-public information	Defined in DoD 5500.07-R.
PAI	Defined in DoDD 3115.18.
personal account	Non-DoD-controlled electronic messaging services account intended for personal use and not associated with official DoD functions.
social media platform	Non-DoD-controlled electronic messaging service with publicly accessible information capabilities and applications available across the internet that facilitates the sharing of user-generated content through virtual connections, networks, and communities through a computer or mobile device.
social media cyber-vandalism	An intrusion of social media accounts when an outside party takes control of an agency communication channel, establishes an impostor DoD social media account, or impersonates a DoD official using a social media account in an attempt to mislead the public or threaten the agency or the individual account.
terms of service	Defined in DoDI 8170.01.
third-party social media management platforms	Free or paid social media management tools that can schedule content and generate social media reports to improve audience engagement and manage social media platform capabilities.
verified account	A moniker or symbol which notifies users on the social media platform that the account of public interest is authentic and helps reassure users to trust the information on the account.

REFERENCES

Code of Federal Regulations, Title 5, Section 2635

Code of Federal Regulations, Title 36, Part 1226

DoD 5500.07-R, "Joint Ethics Regulation (JER)," August 30 1993, as amended

DoD Directive 3115.18, "DoD Access to and Use of Publicly Available Information (PAI)," June 11, 2019, as amended

DoD Directive 5122.05, "Assistant to The Secretary of Defense for Public Affairs (ATSD(PA))," August 7, 2017

DoD Directive 5240.02, "Counterintelligence (CI)," March 17, 2015, as amended

DoD Directive 5240.06, "Counterintelligence Awareness and Reporting (CIAR)," May 17, 2011, as amended

DoD Directive 5535.09, "DoD Branding and Trademark Licensing Program," December 19, 2007

DoD Instruction 1020.03, "Harassment Prevention and Response in the Armed Forces," February 8, 2018, as amended

DoD Instruction 1020.04, "Harassment Prevention and Responses for DoD Civilian Employees," June 30, 2020

DoD Instruction 1304.35, "Military Marketing," November 1, 2017, as amended

DoD Instruction 1325.06, "Handling Protest, Extremist, and Criminal Gang Activities Among Members of the Armed Forces," November 27, 2009, as amended

DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015, as amended

DoD Instruction 5230.09, "Clearance of DoD Information for Public Release," January 25, 2019, as amended

DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," August 13, 2014, as amended

DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019, as amended

DoD Instruction 5400.13, "Public Affairs (PA) Operations," October 15, 2008

DoD Instruction 8170.01, "Online Information Management and Electronic Messaging," January 2, 2019, as amended

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended

Office of Government Ethics' (OGE) Legal Advisory, LA-14-08, "Reference to Official Title and Position by Employees Affiliated with Outside Organizations in Their Personal Capacity," November 19, 2014

Office of Government Ethics' (OGE) Legal Advisory, LA-15-03, "The Standards of Conduct as Applied to Personal Social Media Use," April 9, 2015

Office of Management and Budget Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," September 26, 2003

United States Code, Title 5

United States Code, Title 15

United States Code, Title 44