

NAVY SOCIAL MEDIA HANDBOOK

***FOR SAILORS
& FAMILIES***

2022



For social media queries
please email:
NavySM@us.navy.mil

Page Intentionally Left Blank



ASSISTANT TO THE SECRETARY OF DEFENSE

1400 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-1400

DEC 20 2021

Public Affairs

MEMORANDUM FOR MILITARY SERVICE CHIEFS OF PUBLIC AFFAIRS NATIONAL GUARD CHIEF OF PUBLIC AFFAIRS

SUBJECT: Core Operational Principles on the Use of Official Social Media Accounts within the Department of Defense

While the information and technological environment continue to evolve, our professional and ethical conduct must remain steadfastly aligned to the highest core principles of our service to the Nation.


The Department of Defense's (DoD) reputation for transparency rests in large part on the foundation of the Department's Principles of Information contained in DoD Directive 5122.05, "Assistant to the Secretary of Defense for Public Affairs (ATSD(PA))," and the Department's adherence to these standards. DoD's use of official social media plays an important role in ensuring a free flow of information to the public consistent with these principles. In accordance with DoD Directive 5122.05 and DoD Instruction 8170.01, "Online Information Management and Electronic Messaging," I am sharing these core principles to guide departmental use of official social media accounts and to set expectations of proper conduct for all official account holders.

The core operational social media principles are described below.

1. **Governance.** Public Affairs oversees and manages official DoD social media accounts. This ensures proper alignment with communication and information plans across all media and social media platforms.
2. **Professionalism.** All official social media content reflects upon the Department. Public Affairs Officers and social media administrators must exercise the same high standard of professional and ethical behavior on these accounts as with any other communication function or capability. Official social media accounts must not be used to promote or endorse non-Federal entities or personal financial interests.
3. **Propriety.** Information authorized and publicly released by DoD constitutes official DoD information; therefore, accuracy, appropriateness, timeliness, and proper tone are imperative.
4. **Acumen.** Official social media account administrators should have current knowledge of social media tactics, best practices, and trends, coupled with an understanding of public affairs objectives (e.g., DoD Communication Playbook) to act quickly and remain effective by properly employing social media to meet Departmental objectives in an appropriate manner.

5. **Establishment Appetite.** Establishing new official social media accounts should be carefully considered against existing accounts and platforms. More for the sake of more is not necessarily better.
6. **Transparency.** Content, including replies, will not be deleted from official accounts unless there is a factual or typographical error; violation of a law, policy, term of service, or user agreement; or a security concern. Removal of content will be publicly acknowledged and communicated to audiences to provide context and clarity of the action.
7. **Retention of Content:** DoD social media posts are agency records pursuant to the Federal Records Act (44 U.S.C Chapters 31 and 33). Public Affairs Officers and social media administrators are responsible for retaining information posted to their respective social media sites in accordance with the guidance provided by their DoD component records managers.

As leaders, public affairs practitioners, professional communicators, and public servants, we will continue to advance and improve the quality of information that we share with all DoD audiences, the news media, and the American public. These principles, coupled with a pending DoD instruction on social media usage, are necessary to sustain the trust and credibility of our message on a global information stage.



John F. Kirby

Cc:

Secretaries of the Military Departments
Chairman of the Joint Chiefs of Staff
Under Secretaries of Defense
Chiefs of the Military Services
Chief of the National Guard Bureau
Commanders of the Combatant Commands
General Counsel of the Department of Defense
Chief Information Officer of the Department of Defense
Assistant Secretary of Defense for Special Operations and Low Intensity Conflict

TABLE OF CONTENTS

2	Social Media Do's
2	Online Behavior Considerations
3	The UCMJ & Navy Regulations
4	Reporting Incidents
6	(Social) Media Literacy
6	What Are Bots?!
7	DoD Personnel and Political Activity: The Hatch Act
9	Glossary
12	Appendix A: Controlled Unclassified Information Toolkit
13	Appendix B: Political Activity



SOCIAL MEDIA HANDBOOK FOR SAILORS AND FAMILIES

Individual responsibility online is a SHARED responsibility – Sailors, Navy Civilians and their families. We all play a part in putting our best foot forward in representing our Navy as well as securing its operations and most importantly the safety and well-being of all. This handbook is intended to help you and your families understand the left and right limits of sharing your story safely in the social media space.

SOCIAL MEDIA DO'S

- DO tell your Navy story – while respecting operational security and the responsibility of representing the Navy and your Shipmates – you should share Navy life and experiences that help connect Americans with their Navy; help our fellow citizens understand what we do and why the work you and your Shipmates do is important to national defense.
- DO use #ShareMyNavy on your posts if you would like big Navy pages to share them.
- DO be authentic. Your own original take on your service, your voice, is unique to you and yours alone.
- DO share your rate, and how that rate contributes to the larger mission.
- DO share your experience as a Navy spouse, parent or family member. We want you to show what life is like on your installation, what kind of resources and support are available for you and your children; as well as challenges and joys of being a part of the Navy family.

ONLINE BEHAVIOR CONSIDERATIONS

Rule of thumb: If you wouldn't tag your boss or Sailor's boss in a post due to its content, you probably shouldn't post it. Keep in mind – rightly or wrongly – any time you post a photo of yourself in uniform, you immediately become a spokesperson for the entire Navy in the eyes of the external audience. Anything you post, no matter how small your intended audience can become viral in a matter of seconds.

It is also important to note that just as with physical misconduct offline, misconduct ONLINE is also subject to UCMJ. This does not mean you should not engage. On the contrary, engaging on social media in a positive way; representing yourself and the Navy well, carries the Navy story to Americans and others and gives you an opportunity to tell your own story. Talk with your immediate supervisors when you have questions.

Deputy Secretary of Defense Policy Memorandum, Hazing and Bullying Prevention and Response in the Armed Forces, Dec. 23, 2015:

Identifies **hazing** as so-called initiations or rites of passage in which individuals are subjected to physical or psychological harm. It identifies **bullying** as “acts of aggression intended to single out individuals from their teammates or coworkers, or to exclude them from a military



element, unit or Department of Defense organization.” Additionally, the memo states that hazing and bullying are *unacceptable and prohibited* in all circumstances and environments, including off-duty or unofficial unit functions and settings, as well as on social media and other digital environments.

Also, **intimate images taken without consent**, or posted online without consent constitute *violations of the UCMJ and Navy Regulations*. As outlined in the CNO’s Design for Maintaining Maritime Superiority core attributes, the Navy is a values-based organization where everyone is expected to conduct himself or herself in a manner that is **“always upright and honorable, both in public or when no one is looking.”**

THE UCMJ & NAVY REGULATIONS

When online, to include when using social media, Sailors are subject to the **UCMJ and Navy regulations**, *even when off duty*. Commenting, posting or linking to material that violates the UCMJ or Navy Regulations may result in administrative or disciplinary action, including administrative separation and may, subject civilians to appropriate disciplinary action. Punitive action may include Articles 88, 89, 91, 92, 120b, 120c, 133 or 134 (General Article provisions, Contempt, Disrespect, Insubordination, Indecent Language, Communicating a threat, Solicitation to commit another Offense, and Child Pornography offenses), as well as other articles, including Navy Regulations Article 1168, non-consensual distribution or broadcast of an image.

Behaviors with Legal Consequences

Electronic harassment

47 U.S.C. § 223 (a)(1)(C) makes it a crime to anonymously use a telecommunications device (i.e. telephone, computer, or other electronic devices used for communication) to harass a person; 47 U.S.C § 223 (a)(1)(E) prohibits initiating communication via a telecommunications device solely to harass the recipient.

Electronic threats

18 U.S.C § 875 prohibits transmitting communications containing threats to kidnap or physically injure someone. It also criminalizes the actions of someone who, with intent to export (receive anything of value), electronically threatens to injure the property or reputation of a person. Sextortion (being tricked into providing sexual images and then being asked for money to not have the images published online) may fall under provisions of this law.

Cyberstalking

18 U.S.C. § 2261A prohibits a person, with the intent to kill, injure, harass, or intimidate someone, from using a computer (or other digital communications system), to engage in actions (course of conduct) reasonably expected to cause a person (or immediate family member, spouse, or intimate partner) substantial emotional distress.

Obscenity

47 U.S.C. § 223(a)(1)(A) prohibits using a telecommunications device to make, create, or solicit and transmit any obscene comment, request, suggestion, proposal, image, or other communication.



Child exploitation / Child sexual exploitation

18 U.S.C. § 2251, 2252, and 2252A. Using a computer (a smartphone is a computer) to solicit, make, create, transmit, or receive child pornography is illegal. For these provisions, a child is anyone under the age of 18. 18 U.S.C. § 1462 makes it a crime to transmit obscene matters. 18 U.S.C. § 1470 criminalizes the transfer of obscene materials, including digital images, to persons under the age of 16. **Sending sexually explicit (graphic dirty talk) electronic messages to minors, or soliciting sexually explicit communications, also are criminal offenses.**

Computer misuse (hacking)

A person engaging in cyber misconduct may also commit violations of 18 U.S.C. § 1030, if, for example, he or she exceeds authorized access to the computer or accesses the computer without authorization (i.e. hacks into an account or network) to send harassing, intimidating, humiliating, or even threatening communication.

Extremism

NAVADMIN 044/21 covers the Navy's policy on Extremism in the ranks:

"Extremist behaviors and conduct, even if from only a small percentage of our force, violate our Core Values, are detrimental to good order and discipline, reduce warfighting readiness and degrade the toughness, trust and connectedness we are building in our Sailors and teams through our Culture of Excellence campaign.

Service members and civilian personnel must clearly understand the damaging effects of extremism and begin developing more effective, sustainable ways to eliminate the corrosive impacts extremist activity can have on our Force. As public servants, we took an oath to the Constitution and we will not tolerate those who participate in actions that go against the fundamental principles of the oath we share, particularly actions associated with extremist or dissident ideologies. Service members, Department of Defense civilians and all those who support our mission, are entitled to an environment free of discrimination, hate and harassment."

Speech in the workplace that interferes with the mission, espouses extremist or discriminatory doctrine, or is disrespectful and harmful to colleagues, will have consequences.

Extremism Training and resources: <https://go.usa.gov/xtsc8>

REPORTING INCIDENTS

Any member of the Navy community who experiences or witnesses incidents of improper online and/or extremist behavior should promptly report it to their chain of command via the Command Managed Equal Opportunity manager or Fleet and Family Support office.

Additional avenues for reporting include Equal Employment Opportunity offices, the Inspector General, Sexual Assault Prevention and Response offices, and Naval Criminal Investigative Service.

*** NCIS encourages anyone with knowledge of criminal activity to report it to their local NCIS field office directly or via a web or smartphone app. Specific instructions are available here: <https://www.ncis.navy.mil/Resources/NCIS-Tips>



Rules of the road for our Sailors, Families and Navy civilians online:

- When you are online, you are in public — so act like it.
- Do not do or say anything online you would not do or say in public.
- Keep relationships and personal life private; setting your page to private is a good practice.
- There is no such thing as complete anonymity online (even if your page is private).
- Before you post, STOP and THINK.
- Words matter and can be taken out of context.
- Images can be taken out of context.
- Cool off before responding to messages out of emotion.

Anyone anywhere can see what you post. The internet doesn't forget. All it takes is a screenshot or download of an image to make sure one moment online lasts an eternity. Anything shared online, although intended to be private and confidential, has the possibility to become public — if it is best left unsaid, do not say it. If you do not want it shared, do not post it.

Protect your privacy and your friends' privacy too by not sharing without their permission. ***And unless you are prepared to attach that post, text, or photo to your next security clearance package, or resume — again, do not post it.***

Anything posted on the internet is permanent. Through the use of publicly available online tools, data can be recovered and used against you.

OPSEC and Identity Management Concerns

We've all heard the phrase "practice good OPSEC" — but what does that mean in the social space? The same thing it has always meant. The same information that can be collected and pieced together by adversaries in person, can be done so more swiftly and easily via social media. Be careful not to post movements, deployment dates, ship dates (if you are a new recruit), when your spouse or parent is gone or coming home (if you are a Navy spouse or dependent). If you wouldn't share it with a complete stranger in person, do not disclose it to complete strangers online. Even if your page is "private" there are ways for bad actors to acquire information.

What is Identity Management?

Identity management (IdM), also known as identity and access management (IAM) aims to ensure that ONLY authorized people have access to the technology resources they need to perform their jobs. It includes policies and technologies that encompass an organization-wide process to properly identify, authenticate, and authorize employees based on their identities.

Identity management has gained importance over the past decade due to the growing number of global regulatory, compliance, and governance mandates that seek to protect sensitive data from exposure of any kind.

Take your identity and your personal brand seriously. Report fake profiles of yourself, leadership, or others you may know to the platforms themselves and flag them for CHINFO staff if the page(s) are not taken down or taken to resolution. In the same way you protect your



credit, CAC card, social security number and other personal information; be careful what you share about yourself online. Is your birthday, or other PII displayed on your profile? Make sure to check your page from another browser or account in order to see what your profile actually reveals to other and then fix your profile settings accordingly to ensure you are not revealing more about yourself than you'd want a stranger to know. A lot can often be gleaned from profiles even when they are set to "private".

(SOCIAL) MEDIA LITERACY

Media Literacy: the ability or skills to critically analyze for accuracy, credibility, or evidence of bias the content created and consumed in various media, including radio and television, the internet, and social media.

Social media literacy is the above applied to the social media space. What media do you consume? How are the messages conveyed on those platforms constructed? With what in mind? What is ground truth?

Let's start with a reason social media companies exist — to make money. Every platform wants you to spend as much time as possible on it with algorithms designed to populate your "feed" with content and information you will like and engage with most; and that will keep you on the platform the longest.

This is convenient, when it comes to innocuous content like entertaining videos or photos, but it becomes problematic where misinformation pops up in searches disguised as valid information.

So what do you do? Stop and THINK.

Look beyond initial searches with the understanding that the search terms you use may sway the information you receive. If you search a positive phrase for something and negative phrase for something, for example, you might return completely different results on the same topic; each supporting the narrative of the initial phrasing. The key is to search a few different ways with different keywords to get different perspectives. You should avoid limiting yourself to results that agree with your perspective.

Lastly, keep an open mind and do not believe — and certainly don't share — the first thing you read in a social media post at face value. Take the time to critically think about the information, consider its source, and any agenda of the source.

WHAT ARE BOTS ?!

Knowing whether an account is a bot or troll pretending to be an actual person is difficult. By some estimates, a quarter of all social media accounts may be bots and/or inauthentic accounts. Bots have been used by foreign governments, private companies, and terrorist organizations.

Some are controlled by an AI, others are controlled in what are often referred to as "troll farms", places where real people are paid to use hundreds of fake accounts online to pose as real accounts, usually using stolen identities. These types of accounts are often referred to as "sock puppets".

If you come across a tweet and are not sure if it is from a bot, here are the following steps you can take to assess whether it is a bot or a real person:

- Check for account verification. If there is a check mark next to the account name, then it has been verified to be a real person or organization by the site.

If there is no check mark:

- Check the handle of the account. Fake accounts often contain a lot of random numbers or letters in the handle (i.e., RealPatriot274hg6yt).
- Look at the age of the account. If an account is around or less than a year old, it could likely be a bot. If the account is years old, but only appears to have started tweeting, posting, sharing etc., within the past few months, it is also likely a bot. Many bad actors will create hundreds of accounts with the intent of keeping them quiet for a couple years to try and escape detection.

Some platforms have free, open-source tools to help identify inauthentic accounts. Bot Sentinel for example, analyzes Twitter accounts and grades them on the likelihood the account is a bot or troll.

DOD PERSONNEL AND POLITICAL ACTIVITY: THE HATCH ACT

DoD Personnel and Political Activity: The Hatch Act

The U.S. Office of Special Counsel (OSC) routinely receives questions from federal employees and others about when the use of social media could violate the Hatch Act. Social media platforms are easily accessible to most employees while at work — on computers, smartphones, or other devices. OSC has created this guidance to help federal employees understand what the Hatch Act does and does not.

In general, all federal employees may use social media and comply with the Hatch Act if they remember the following three prohibitions:

1. On Duty or in the Workplace Prohibition — Employees may not engage in political activity while on duty or in the federal workplace.
2. 24/7 Prohibition — Employees may not knowingly solicit, accept, or receive a political contribution for a political party, candidate in a partisan race, or partisan political group.
3. 24/7 Prohibition — Employees may not use their official authority or influence to affect the outcome of an election.

Military Personnel: DoD has a longstanding policy of encouraging military personnel to carry out the obligations of citizenship. However, AD members will not engage in partisan political activities and all military personnel will avoid the inference that their political activities imply or appear to imply DoD sponsorship, approval or endorsement of a political candidate, campaign or cause.

Civilian Personnel: For DoD civilians, participation in political activity is regulated by a number of sources: the Hatch Act (5 U.S.C. §§ 7321 - 7326), implementing regulations (5 C.F.R. § 733 and 5 C.F.R. § 734), as well as DoD policy. For purposes of the Hatch Act, 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". Because application of the rules may vary depending on an employee's position or office, it is extremely important that employees who are considering engaging in political activity know which rules apply.

With regard to civilian employees, there are two sets of restrictions for three groups of employees. The first and more restrictive set of restrictions applies to: (1) individuals appointed by the President and confirmed by the Senate and individuals serving in non-career SES positions; and (2) career members of the SES, contract appeals board members, and all employees of the National Security Agency (NSA), the Defense Intelligence Agency (DIA), and the National Geo-Spatial-Intelligence Agency (NGA). The second and more lenient set of restrictions applies to all other employees (including Schedule C political appointees).

Employees in Groups 1 and 2 are prohibited from taking an active part in partisan political management or political campaigns and are referred to as "further restricted" employees.

For further details on the above please see Appendix B.

CONCLUSION

Please continue to reference this handbook when you or your loved ones have questions. We encourage you to share your Navy story in a manner in keeping with your role as a Sailor or Navy family member.

The considerations above aren't meant to scare you; rather to make you aware of some of the pitfalls that exist and how best to avoid them.

If you have any questions, feel free to reach out to OI-2, CHINFO, at **NavySM@us.navy.mil**

GO NAVY!

GLOSSARY

Avatar: A static or moving image or other graphic representation that acts as a proxy for a person or is associated with a specific digital account or identity, as on the internet: Not the blue animated characters, an avatar is another word for profile picture or icon that visually represents and identifies your organization on the social media platform.

Bio: Biography, or short description in profile that easily describes who and what your organization is about. Recommend sharing website links, common hashtags, contact information, or disclaimers in this section.

Bots: A software program that can execute commands, reply to messages, or perform routine tasks, as online searches, either automatically or with minimal human intervention (often used in combination): *a social media bot retweeting certain posts; a customer service chatbot to answer product questions*. Especially prevalent on Twitter, a bot is an automated account run by software capable of posting content or interacting with other users. Some bots pretend to be humans.

Catfishing: When a person assumes a false identity or personality on the internet, especially on social media websites, as to deceive, manipulate, or swindle.

Command Presence: A profile on a social networking website which is considered distinct from an actual user personal or personal-professional profile in that it is created and managed by at least one other registered user, usually Public Affairs staff or Mass Communication Specialist as a representation of a non-personal online identity for that command. These pages are listed by command and/or ship name vice and individual and push out content to tell the story of that particular command/ship and its mission writ large.

Content: Something that is to be expressed through some medium, as speech, writing, or any of the various arts.

Cover Photo: A header image on Facebook, Twitter, and YouTube that tells people what your organization is about at first glance upon coming to your page.

DM: Direct message, or not publicly posted communication between two accounts. Keep in mind, however, that this correspondence is only private to the extent that one user can screenshot and publish the conversation.

Engagements: Social media engagement measures the public shares, likes and comments for an online business' social media efforts. Engagement has historically been a common metric for evaluating social media performance. How people react to the content, including likes, comments, retweets, shares, reactions, and more.

Ephemeral Content: Sometimes called "disappearing content," these social media posts delete automatically after a set amount of time has lapsed. Instagram and Snapchat stories disappear after 24 hours. However, content is also susceptible to screen recording or other methods of indefinitely capturing the content.



Feed: A social media feed is an updated list of all the new content posted by the user follows on social media platforms. This stream of content published by other users, most often the “homepage” and most common way to see and engage with posts. Rather than being purely chronological, most social media feeds are controlled by an algorithm.

Hashtag: A word or phrase preceded by a hash sign (#), used on social media websites and applications, especially Twitter, to identify digital content on a specific topic.

Header: Your header photo is the **image that spans the top of your Twitter, Facebook, or YouTube profile page**. It’s quite a bit larger than your profile photo so make sure to save it at the highest resolution possible. Because you have more room to be creative with this picture and it will likely be the first thing your visitors see, make it something captivating.

Identity Management: IdM and IAM are terms often used interchangeably, however identity management is more focused on a user identity (or username), and the roles, permissions, and groups that user belongs to. IdM also focuses on protecting identities through a variety of technologies such as passwords, biometrics, multi-factor authentication, and other digital identities.

Impressions: How many people potentially saw the post; how many times the post was shown in users’ feeds, can be duplicated, and different social media networks define (and therefore calculate) this metric a little differently.

Influencer: **One who exerts influence:** a person who inspires or guides the actions of others; often, specifically: a person who is able to generate interest in something (such as a consumer product) by posting about it on social media.

Internet Sites: Any website or web page.

Mentions: **Social mentions include any mention of your organization or personal brand** on social media. It’s important to remember this doesn’t only include the mentions that tag your page. There are tons of conversations about your organization on social media that you aren’t receiving notifications for. Keeping an eye on mentions, following what your audience is saying; more passive approach than social listening.

Microinfluencer: A micro-influencer is someone who has between **1,000 to 100,000 followers**. Micro-influencers focus on a specific niche or area and are generally regarded as an industry expert or topic specialist. “[Micro-influencers] have stronger relationships than a typical influencer.

Personal Page: Personal web pages are world wide web pages created by an individual to contain content of a personal nature rather than content pertaining to a company, organization or institution.

Personal-Professional Page: A page where you (or your team) represent(s) yourself as yourself; but in a professional capacity; tied to your official Navy title and in your official Navy capacity.

Platform: Also may be referred to as a social media “network” or social media “channel”.

Post: A post is a message, such as text or photos, published online by a user while referring to a message board, comment section, or social network.



Reach: **Post reach** is the number of people who saw a specific post in their news feed. **Page reach** is the number of people who saw any of your post content during a given period of time (daily, weekly or monthly).

Reels: **Reels** was created as a new way for users to create and discover short, entertaining videos on the platform. Unlike other short-form video platforms, **Reels** are 15 or 30-second multi-clip videos that you can record and edit them with audio, effects, and creative tools in a similar way to TikTok.

Social Listening: Tracking conversations around key topics and terms related to your brand, gathering mentions, comments, hashtags, and posts to provide insight on conversations surrounding your brand.

Social Monitoring: In basic terms, social media monitoring is the act of using a tool to listen to what is being said across the internet; monitoring media not just from traditional publishers, but on millions of social sites too.

Stories: See *Ephemeral Content*.

Target Audience: A particular group at which a film, book, advertising campaign, etc., is aimed.



APPENDIX A: CONTROLLED UNCLASSIFIED INFORMATION TOOLKIT

What is CUI?

- Government created or owned UNCLASSIFIED information that must be safeguarded from unauthorized disclosure.
- An overarching term representing many difference categories, each authorized by one or more law, regulation, or Government-wide policy.
- Information requiring specific security measures indexed under one system across the Federal Government.

Why is CUI important?

- The establishment of CUI was a watershed moment in the Department's information security program, formally acknowledging that certain types of UNCLASSIFIED information are extremely sensitive, valuable to the United States, sought after by strategic competitors and adversaries, and often have legal safeguarding requirements.
- Unlike with classified national security information, DoD personnel at all levels of responsibility and across all mission areas receive, handle, create, and disseminate CUI.
- CUI policy provides a uniform marking system across the Federal Government that replaces a variety of agency-specific markings, such as FOUO, LES, SBU, etc.

Where did CUI come from?

- Executive Order 13556 established CUI on November 4, 2010.
<https://www.gpo.gov/fdsys/pkg/FR-2010-11-09/pdf/2010-28360.pdf>
- Part 2002 of 32 Code of Federal Regulations prescribed Government-wide implementation standards on September 14, 2016.
<https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf>
- DoD Instruction 5200.48, "Controlled Unclassified Information," established DoD CUI policy on March 6, 2020.
<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.pdf>

With the issuance of DoD Instruction 5200.48, the Department is proud to be an early adopter of CUI Program requirements.



APPENDIX B: POLITICAL ACTIVITY

Overarching Guidance

The U.S. Office of Special Counsel (OSC) routinely receives questions from federal employees and others about when the use of social media could violate the Hatch Act. Social media platforms are easily accessible to most employees while at work — on computers, smartphones, or other devices. OSC has created this guidance to help federal employees understand what the Hatch Act does and does not allow when using social media.¹

In general, all federal employees may use social media and comply with the Hatch Act if they remember the following three prohibitions:

- (1) On Duty or in the Workplace Prohibition — Employees may not engage in political activity while on duty or in the federal workplace.
- (2) 24/7 Prohibition — Employees may not knowingly solicit, accept, or receive a political contribution for a political party, candidate in a partisan race, or partisan political group.
- (3) 24/7 Prohibition — Employees may not use their official authority or influence to affect the outcome of an election.

Some employees are considered “further restricted” under the Hatch Act.² In addition to the three prohibitions above, further restricted employees are subject to a fourth prohibition:

- (4) 24/7 Prohibition — Further restricted employees may not take an active part in partisan political management or campaigning.

As such, further restricted employees may not engage in political activity on behalf of or in concert with a political party, candidate in a partisan race, or partisan political group. For instance, taking an “active part” would include: distributing material created by a political party, candidate in a partisan race, or partisan political group; speaking at a political rally organized or sponsored by such entities; or serving as a campaign volunteer.

This guidance will discuss each of the above prohibitions in turn. The last prohibition discussed is applicable only to further restricted employees. There are some very limited exceptions to these prohibitions for certain employees in specific positions and, when in doubt, employees are encouraged to contact OSC at hatchact@osc.gov or (202) 804-7002 with any additional questions.

1 This Hatch Act Guidance supersedes OSC’s prior guidance on social media in 2012 and 2015.

2 You are a further restricted employee under the Hatch Act if you are a career member of the Senior Executive Service, an administrative law judge, a contract appeals board member, an administrative appeals judge, or if you work in one of the following agencies, or agency components: (1) Central Intelligence Agency; (2) Criminal Division of the Department of Justice; (3) Defense Intelligence Agency; (4) Election Assistance Commission; (5) Federal Bureau of Investigation; (6) Federal Election Commission; (7) Merit Systems Protection Board; (8) National Geospatial- Intelligence Agency; (9) National Security Agency; (10) National Security Council; (11) National Security Division of the Department of Justice; (12) Office of Criminal Investigation of the Internal Revenue Service; (13) Office of the Director of National Intelligence; (14) Office of Investigative Programs of the United States Customs Service; (15) Office of Law Enforcement of the Bureau of Alcohol, Tobacco, and Firearms; (16) Office of Special Counsel; or (17) Secret Service. See 5 U.S.C. § 7323(b)(2)-(3).



(1) ON DUTY OR IN THE WORKPLACE PROHIBITION – Employees may not engage in political activity while on duty or in the workplace.³ Political activity is an activity directed at the success or failure of a political party, candidate in a partisan race, or partisan political group.

(A) Posting, Liking,⁴ Sharing, or Retweeting Partisan Messages

Rule: Employees may not post, like, share, or retweet a message or comment in support of or opposition to a political party, candidate in a partisan race, or partisan political group while on duty or in the workplace, even if their social media account is private.

Example 1: You are at home after work. You may like or tweet a message encouraging others to vote for your favored candidate in a partisan race.

Example 2: You are on duty and looking at Facebook on your personal cell phone. You see that a friend posted a message encouraging others to vote for members of a certain political party. You may not like or share that message while you are on duty.

Example 3: You stay at work during your lunch break and check Facebook on your personal cell phone. A Facebook friend posted a message about an upcoming event supporting a candidate in a partisan race. Even if you are not in a pay status during your lunch break, you may not like or share that post while you are in the workplace.

Example 4: You are teleworking from home and on your lunch break in which you are not in a pay status. You are looking at Facebook on your personal iPad and see that a friend posted a message about an upcoming event supporting a political party. Because you are on your lunch break and not in a federal building, you may like or share that post.

Example 5: You are teleworking from home and looking at Twitter on your personal computer. You see that the President tweeted an endorsement of a congressional candidate. You may not like or retweet that message while on duty.⁵

Example 6: You are teleworking and looking at Facebook on your personal cell phone. You see that a Senate candidate posted a message asking for votes on Election Day. You may not post a comment in support of that message while on duty.

(B) Liking, Following, or Friending Candidates or Partisan Groups

Rule: Employees may not like, follow, or friend the social media account of a political party, candidate in a partisan race, or partisan political group while on duty or in the workplace.

Example 1: You are at home after work and find the Instagram account of a partisan political group. You may follow them on Instagram and like their posts.

Example 2: You are at work and looking at your private Facebook account on your personal iPad. A Facebook friend shared the post of a candidate in a partisan race announcing that he or she received an endorsement. You may not like, follow, or friend the candidate's Facebook page while on duty or in the workplace.

(C) Liking, Following, or Friending the Official Social Media Accounts of Government Officials

³ Employees also may not engage in political activity while wearing a uniform or official insignia identifying the office or employee's position, or while using a government owned or leased vehicle.

⁴ Liking includes the use of other emojis or reactions, such as those in the "like" function of Facebook.

⁵ The President and Vice President are not covered under the Hatch Act and, as a result, are not subject to its social media restrictions.



Rule: Employees may continue to follow, be friends with, or like the official social media accounts of government officials after those officials become candidates for reelection.

Example 1: You follow the official government Twitter account of the President or a Member of Congress, who has just announced their candidacy for reelection. You may continue to follow these official accounts.

(D) Using an Alias on Social Media

Rule: Employees may not use an alias on social media to engage in any activity that is directed at the success or failure of a political party, candidate in a partisan race, or partisan political group while on duty or in the workplace.

Example 1: Your name is John Smith, but you create a Facebook profile as John Jones. You are at home after work and see that a Facebook friend posted a negative message about a candidate in a partisan race. You may share or like that post.

Example 2: Your name is Jane Smith, but you create a Twitter account as Jane Jones. You are at work, on duty, and looking at your alias Twitter account on your personal cell phone. An actor you follow on Twitter posted a negative message about a political party. You may not like or retweet that message either as Jane Smith or Jane Jones while on duty or in the workplace.

(E) Profile Pictures on Social Media Accounts

Rule: Employees may display a political party or current campaign logo or the photograph of a candidate in a partisan race as a profile picture on personal Facebook or Twitter accounts; however, they may not post, share, tweet, or retweet on those accounts while on duty or in the workplace.⁶

Example 1: You decide to use a current campaign logo as your profile picture on your personal Twitter account. Although you may use the logo as your profile picture, you may not tweet or retweet any messages on that account while on duty or in the workplace.

(F) Cover and Header Photographs on Social Media Accounts

Rule: Employees may display a political party or campaign logo or photograph of a candidate in a partisan race as a cover or header photograph on their personal Twitter or Facebook accounts.⁷

Example 1: You recently took a photograph with a candidate in a local partisan race. You may use the photograph as the header on your personal Facebook account.

(2) 24/7 PROHIBITION – Employees may not knowingly solicit, accept, or receive a political contribution for a political party, candidate in a partisan race, or partisan political group.

(A) Posting or Tweeting Solicitations

⁶ Because a profile picture accompanies most actions on social media, employees would not be permitted, while on duty or in the workplace, to post, share, tweet, or retweet any items on Facebook or Twitter, because each such action would show their support for a political party, candidate in a partisan race, or partisan political group, even if the content of the post, share, tweet, or retweet is not about those entities.

⁷ Unlike profile pictures, cover and header photographs do not accompany most actions on social media. Therefore, the Hatch Act generally does not prohibit employees from using their social media accounts at work, even if they display a political party or campaign logo or photograph of a candidate in a partisan race as their cover or header photograph. But employees should always consult their agency's computer-use policies before using any social media at work.



Rule: Employees, even when not on duty or in the workplace, may not post or tweet a message that solicits political contributions or invites people to a fundraising event.

Example 1: You may not tweet a message asking your Twitter followers to contribute five dollars to help a candidate in a local partisan race.

Example 2: You are attending a political party's annual fundraising event. You may not post a message on Facebook inviting friends to join you at the event.

(B) Liking, Sharing, or Retweeting Solicitations

Rule: Employees, even when not on duty or in the workplace, may not like, share, or retweet a post that solicits political contributions, including invitations to fundraising events.

Example 1: Someone tweets a message offering to match the donation of the first five friends that donate to a certain candidate in a local partisan race. Although the Hatch Act does not prohibit you from donating to the campaign, you may not like, share, or retweet that post.

Example 2: A friend shares a post on Facebook that includes an invitation to a local fundraising event for a political party. You may not like or share that post.

Example 3: Someone tags you in a post, or posts a message to your Facebook page, that asks for donations for a partisan political group. You do not have an affirmative duty to remove that post from your Facebook page or un-tag your name from the post; however, you may not like or share the post.

(C) Accepting Invitations to Fundraising Events on Social Media

Rule: If not on duty or in the workplace, employees may accept invitations to, or mark themselves as "attending," a fundraising event on social media.

Example 1: A friend sends you an invitation on Facebook to a fundraising event for a candidate in a partisan race. You may accept the invitation or mark yourself as "attending" the fundraising event, provided you are not on duty or in the workplace.

(D) Using an Alias on Social Media

Rule: Employees, even when not on duty or in the workplace, may not use an alias on social media to solicit a political contribution for a political party, candidate in a partisan race, or a partisan political group.

Example 1: Your name is John Smith, but you create a Facebook profile as John Jones. You are at home after work and see that a Facebook friend posted a message that solicits campaign contributions for a candidate in a partisan race. You may not share that message either as John Smith or John Jones.

(3) 24/7 PROHIBITION – Employees may not use their official authority or influence to affect the outcome of an election.

(A) Using Official Title or Position in Social Media Profile

Rule: Employees may include their official titles or positions and where they work in their social media profiles, even if they also include their political affiliation or otherwise use their account to engage in political activity.

Example 1: Your Twitter profile includes your official title or position and where you work. You



may also list your political affiliation.

Example 2: Your Facebook profile includes your official title or position, where you work, and your political affiliation. You may post a message supporting a candidate in a partisan race, provided you are not on duty or in the workplace.

(B) Using Official Title or Position in Social Media Communications

Rule: Employees may not use their official titles or positions when posting messages directed at the success or failure of a political party, candidate in a partisan race, or partisan political group.

Example 1: While at home after work, you decide to post a positive comment on the Twitter account of a candidate in a local partisan race. You may not mention your official title or position in that comment, even if your Twitter account is private.

Example 2: Your LinkedIn profile headline includes your official title or position. You may not use that LinkedIn account to post or share messages directed at the success or failure of a political party, candidate in a partisan race, or partisan political group.⁸

(C) Using Official Social Media Accounts

Rule: Employees may not use a social media account designated for official purposes to post or share messages directed at the success or failure of a political party, candidate in a partisan race, or partisan political group. All such official social media accounts should remain politically neutral.

Example 1: While accessing the Twitter account you use for official purposes, you see that a political party tweeted its support for a candidate in a partisan race. You may not retweet or like that post from the account used for official purposes (or from your personal social media account if you are on duty or in the workplace).

(D) Misusing Personal Social Media Accounts

Rule: Employees may not engage in political activity on a personal social media account if they are using such accounts for official purposes or posting in their official capacities. Factors indicating that a personal social media account is being used in ways that suggest it is an official social media account include, for example: (1) the account contains little to no personal content; (2) the account identifies the individual as a federal employee; (3) the account extensively uses photographs of the employee's official activities; (4) the account often references, retweets, likes, comments, or otherwise shares material related to official activities; or (5) the account is linked to an agency website or other official page. No one factor is dispositive.

Example 1: You are a federal employee and maintain only a personal Twitter account. While you have some personal posts about family vacations and events with friends, most of your posts are retweets of your agency's initiatives and photographs of you at official events. You may not use this account to make posts directed at the success or failure of a political party, candidate in a partisan race, or partisan political group.

⁸ A LinkedIn profile headline accompanies most actions on LinkedIn. Therefore, employees who include an official title or position in their LinkedIn profile headline would not be permitted to post or share any messages on LinkedIn that are directed at the success or failure of a political party, candidate in a partisan race, or partisan political group.



(E) Targeting Subordinates and Certain Groups⁹ in Social Media Communications

Rule: Supervisors and subordinates may be friends or follow one another on social media platforms. However, supervisors may not send to subordinates, or to a subset of friends that includes subordinates, any message that is directed at the success or failure of a political party, candidate in a partisan race, or partisan political group.

Example 1: You are a supervisor. You may tweet generally about your support of a candidate in a local partisan race even if one of your subordinates follows you on Twitter, provided you are not on duty or in the workplace.

Example 2: You are a supervisor. You may not mention, or use the Twitter handle of, a subordinate who follows you on Twitter when tweeting your support of a candidate in a partisan race.

Example 3: You are a supervisor. You want to send via Facebook Messenger your opinion about which candidate to support in an upcoming partisan election. You may not include a subordinate employee in the recipient group of that message.

(4) 24/7 PROHIBITION – *Further restricted employees* may not take an active part in partisan political management or campaigning.

(A) Sharing or Retweeting Partisan Messages

Rule: Further restricted employees may not share or retweet posts from, or the page of, a political party, candidate in a partisan race, or partisan political group, even if they are not on duty or in the workplace.

Example 1: You are at home using your personal cell phone to look at Facebook. You see that a political party has posted a message about voting on Election Day. You may not share that post.

Example 2: You may like the campaign Facebook page of a candidate in a partisan race, but you may not share that page.

Example 3: A friend has shared a Facebook post from the campaign of a Presidential candidate. You may not share that post.

(B) Linking to Partisan Material or Websites

Rule: Further restricted employees may not link to campaign or other partisan material of a political party, candidate in a partisan race, or partisan political group, even if they are not on duty or in the workplace.

Example 1: You may not include in your Facebook profile the link to the website of a candidate in a partisan race.

Example 2: You may not tweet a message in support of a candidate in a partisan race that includes a link to that candidate's Twitter account.

(C) Posting to or Liking Partisan Social Media Accounts or Messages

Rule: Further restricted employees may post to or like the social media accounts or messages

⁹ The Hatch Act prohibits an employee from knowingly soliciting or discouraging the political activity of any person who, for example, has a grant application pending before, or is the subject of an investigation by, the employee's employing office.



of a political party, candidate in a partisan race, or partisan political group, provided they are not on duty or in the workplace.

Example 1: Your friend is running for Congress. You may like her campaign Facebook page or post a message of support on her page, provided you are not on duty or in the workplace.

(D) Posting Personal Political Opinions

Rule: While not on duty or in the workplace, further restricted employees may engage in political activity on social media, provided it is not done in concert with or on behalf of a political party, candidate in a partisan race, or partisan political group.

Example 1: You may tweet your own message advocating the defeat of a Presidential candidate, provided you are not on duty or in the workplace.

Guidance For Armed Forces

Q1. What is the DoD policy regarding political activities by members of the Armed Forces?

A1. DoD has a longstanding policy of encourage military personnel to carry out the obligations of citizenship. However, AD members will not engage in partisan political activities and all military personnel will avoid the inference that their political activities imply or appear to imply DoD sponsorship, approval or endorsement of a political candidate, campaign or cause.

Q2. Can political candidates visit a DoD installation or facility?

A2. A candidate for civil office may not be permitted to engage in campaign or election related activities (e.g., public assemblies, town hall meetings, speeches, fund-raisers, press conferences, post-election celebrations, and concession addresses) while on a DoD installation, which includes overseas installations and areas under the control of combat or peacekeeping forces of the United States military.

Q3. Can a seated politician visit a DoD installation or facility if they are campaigning for office?

A3. A candidate who holds a civil office may visit a DoD installation or facility for the purpose of conducting official business or to access entitlements or benefits the candidate is authorized to use; however, no candidate running for office is permitted access for campaign or election purposes.

Q4. How does DoD define when a political campaign begins and ends?

A4. According to DoD policy, a political campaign or election begins when a candidate, including an incumbent officeholder, makes a formal announcement to seek political office or when an individual files for candidacy with the Federal Election Commission or equivalent regulatory office. Once initiated, a political campaign or election does not end until one week after the conclusion of the relevant election.

Q5. What political activities can a service member participate in and which ones are prohibited?

A5. DoD has a longstanding policy of encouraging military personnel to carry out the obligations of citizenship, and certain political activities are permitted, such as voting and making a personal monetary donation. However, active duty members will not engage in partisan political activities, and all military personnel will avoid the inference that their political activities imply or appear to imply DoD sponsorship, approval or endorsement of a political



candidate, campaign or cause.

Examples of political activities that are prohibited include campaigning for a candidate, soliciting contributions, marching in a partisan parade and wearing the uniform to a partisan event. For a complete list of permissible and prohibited activities, please consult

DoD Directive 1344.10, Political Activities by Members of the Armed Forces Guidance for Military Personnel.

Q6. Does that mean a service member can vote, but not actively support a particular candidate or cause?

A6. Unquestionably, service members can exercise their right to vote. However, AD members will not engage in partisan political activities and will avoid the inference that their political activities imply or appear to imply DoD sponsorship, approval, or endorsement. For a list of permissible and prohibited activities, please consult DoD Directive 1344.10, Political Activities by Members of the Armed Forces (reference (c)).

Q7. Does DoD support and encourage its personnel to vote?

A7. DoD encourages all members of the Armed Forces and federal civilian employees to register and vote. The department actively supports the Federal Voting Assistance Program to ensure its personnel have the resources, time and ability to participate in their civic duty. Additionally, department leaders and military commanders appoint voting assistance officers at every level of command and ensure they are trained and equipped to provide voting assistance.

Q8. Can a DoD installation be used as a polling place in an election?

A8. As of December 31, 2000, if an installation facility is designated as an official polling place by an election official or has been used as a polling place since January 1, 1996, installation commanders will not deny the use of that facility as a polling place for any election. The Secretary of Defense or the secretary of the military department concerned may grant a waiver of the requirement to allow use of the facility if it is determined that security is a concern. All members of the Armed Forces on AD are instructed to remain clear of all polling places except when voting.

Q9. Does DoD provide any voting assistance?

A9. Yes, DoD provides voting assistance via the Federal Voting Assistance Program. FVAP works to ensure service members, their eligible family members and overseas citizens are aware of their right to vote and have the tools and resources to successfully do so – from anywhere in the world – via FVAP.gov. The services also provide voting assistance officers at the unit level to facilitate in-person assistance when required.

Guidance For Civilians

Before posting about politics on social media, Department of the Navy civilians need to consider the Hatch Act and DoD policy.

In general, as a federal employee, you may use social media and comply with the Hatch Act if you:

- Don't engage in political activity while on duty or in the workplace, even if you're using your



personal smartphone, tablet, or laptop to do so. Federal employees are “on duty” when they’re in a pay status (including during telework hours, but not including paid leave) or are representing the government in an official capacity.

- Don’t post political opinions, likes, shares, etc. while on government property, even if inside your vehicle on a lunch break, using your own device to post to your personal account.
- Don’t engage in political activity in an official capacity at any time. Political activity refers to any activity directed at the success or failure of a political party or partisan political group or candidate in a partisan race.
- Don’t solicit or receive political contributions at any time.

As a civilian, you may express your opinions about a partisan group or candidate in a partisan race by posting, liking, sharing, tweeting or retweeting, but there are a few limitations. The Hatch Act prohibits federal employees from:

- Referring to your official titles or positions while engaged in political activity at any time; it’s important to note that including your official title or position in your social media profile is not an improper use of official authority.
- Suggesting or asking anyone to make political contributions at any time, including providing links to the political contribution page of any partisan group or candidate in a partisan race or liking, sharing or retweeting a solicitation from one of those entities.
- Liking, sharing or retweeting an invitation to a political fundraising event; however, you may accept an invitation to a political fundraising event from such entities via social media.
- Posting political opinions/likes/shares while on government property, even if inside your vehicle on a lunch break, using your own device to post to your personal account.

Civilians who fall in the “further restricted employees” category may express opinions about a partisan group or candidate in a partisan race by posting or sharing content, but there are a few limitations. In addition to the limitations above, the Hatch Act prohibits further restricted employees from:

- Posting or linking to campaign or other partisan material of a partisan group or candidate in a partisan race. Sharing those entities’ social media sites or their content, including retweeting.

Civilians are allowed to identify their political party affiliation in their social media profiles, even if the profile also contains their official title or position, without more. As a civilian, you may display a political party or campaign logo or a candidate photograph in your profile picture, but it’s subject to the following limitations: Because a profile picture accompanies most actions on social media, while in the workplace you would not be permitted to post, share, tweet, or retweet any partisan social media content because each such action would show your support for a partisan group or candidate in a partisan race, even if the content of the action is not about those entities.

For the full policy and more details, see the U.S. Office of Special Counsel website at:
<http://www.osc.gov>



Page Intentionally Left Blank

Page Intentionally Left Blank

For social media queries
please email:
NavySM@us.navy.mil