NAVY COMMAND
SOCIAL MEDIA HANDBOOK

Fall 2010

Cover Photo
PACIFIC OCEAN (Nov. 10, 2007) – Cmdr. Daniel P. Dusek, commanding officer of Arleigh Burke-class guided-missile destroyer USS Fitzgerald (DDG 62), looks ahead as his ship maneuvers behind Military Sealift Command underway replenishment oiler USNS Rappahannock (T-AO 204) awaiting an underway replenishment. Fitzgerald, part of Destroyer Squadron 15 and permanently forward deployed to Yokosuka, Japan, is underway on a scheduled deployment. (U.S. Navy photo illustration)

Table of Contents

Open Letter from the Chief of Information

Navy Leaders,

This is an exciting, dynamic and challenging time to be a leader in the Navy. Among the myriad of challenges that you face, there has been a dramatic change in the communication landscape in just the past few years. The rapid growth of social media platforms and technologies have flattened and democratized the communication environment in ways we are just beginning to comprehend.

Effective communication has always contributed to unit and mission success. In today's more connected environment, talking to and engaging with your audiences is absolutely essential. During the recent flooding in Millington, the base commanding officer and his staff effectively used social media as part of their approach to understand and respond to questions and concerns, which significantly contributed to their successful response. During Operation Unified Response, commanders of participating units used social media to communicate their units' and their Sailors' contributions in responding to Haiti.

Social media is an effective channel to communicate relevant, aligned, and targeted information to the stakeholders that we want to reach, including some we have had a hard time reaching before. As with the advent of other communication technologies – phone, fax, email, websites – we must exercise caution to use these tools safely and effectively, and we must educate our Sailors and families to do the same.

This handbook was put together by the Emerging Media Integration Team at CHINFO and is intended to provide you with the information needed to more safely and effectively use social media. This handbook is not intended to be a comprehensive guide on command use of social media or take the place of official policy.

The information in this handbook is a useful guide for navigating a dynamic communication environment. I hope after reviewing this handbook you're better prepared to use social media as an effective channel to share your command's story.

DENNIS J. MOYNIHAN
RDML USN
CHIEF OF INFORMATION

Executive Summary

WHAT IS SOCIAL MEDIA?

Social media describes the different means by which people, enabled by digital communication technologies, connect with one another to share information and engage in conversations on topics of mutual interest. Social media is an umbrella term describing a variety of communication mediums and platforms, social networking being the most well known of them. While specific mediums, platforms, and technologies may change over time the overall trend of people connecting with other people using technology only increases. The way people get information has changed and their desire to have real conversations individuals, businesses, organizations, and government has increased. This presents a tremendous opportunity for all commands to more effectively communicate with Sailors, Navy families and the public.

WHY USE SOCIAL MEDIA?

Social media, as part of your overall command communications strategy, helps fulfill your obligation to communicate with all of your stakeholders. It also provides another, often richer, means of sharing information with internal and external audiences. Your stakeholders are increasingly using social media, and you're better off reaching them there than not at all.

Social media creates some considerations for the commander over traditional means of communicating:

- It is efficient: Anything you communicate in social media is sent in an instant and is then available anywhere in the world for your stakeholders to access. Additionally, social media may provide a means of communications reach that is available when other means are not (i.e. times when people cannot access NMCI, message traffic, etc. due to travel, base closures, disasters, etc).
- It is unmediated: There is no gatekeeper – that means that you when you say something it will appear to your audience just as you want it to appear (keep in mind that your message might be misinterpreted so try to minimize that before posting)
- Provides feedback: You can gauge – and act on – communication thanks to the open feedback that social media enables.
- Promotes trust: Responsively exchanging information builds a relationship and in return trust with your stakeholders. By listening, sharing and engaging with others in social media you have the unique opportunity to assume a leading role in what is said about your command and relevant issues regarding your command.

WHO USES SOCIAL MEDIA?

Social media is an important – and growing – means by which many people communicate. According to an annual Forrester Research survey in 2009, more than 4 in 5 online adults in the United States participate in social media. Similarly, a recent poll conducted by the Navy Personnel, Research, Studies & Technology (NPRST) office in November 2009 shows that an overwhelming majority of Navy personnel use Facebook and other forms of social media to communicate. So while all key stakeholders may not be on social media, the majority of them use some form of social media to get information and communicate. Reaching Navy stakeholders via social media is critical, as shown by Navy leadership's presence– the Secretary of the Navy, the Chief of Naval Operations and the Master Chief Petty Officer of the Navy all use social media to great effect.

WHAT DOES DOD AND THE NAVY SAY ABOUT SOCIAL MEDIA?

On February 25, 2010 the DoD issued a Directive-Type Memorandum (DTM) providing guidelines for military use of social media and acknowledged "that Internet-based capabilities are integral to operations across the Department of Defense." DTM 09-026 Responsible and Effective Use of Internet-based Capabilities established the requirement that "the NIPRNET shall be configured to provide access to Internet-based capabilities across all DoD Components." While implementation by the services is ongoing, the intent is clear – the use of social media in DoD is authorized and encouraged.

On August 19, the DON issued ALNAV 056/10 Internet-based Capabilities Guidance – Official Internet Posts and ALNAV 057/10 Internet-based Capabilities Guidance – Unofficial Internet Posts. These two ALNAVs provide policy guidance for the use of Social Media for both official use and for unofficial or personal use. A SECNAV instruction on Internet-based Capabilities, which is currently in staffing.

Guidelines for Sailors & Navy Personnel

The Navy encourages service members to tell their stories. With fewer Americans having served themselves in the military, it is important for our service members to share their stories of service with the American people. Not surprisingly, this makes every blogging, tweeting or Facebooking Sailor an ambassador for your command and the Navy. Educating our Sailors and personnel about how to maintain the integrity of this ambassadorship is important.

COMMUNICATE OPSEC measures to your Sailors and personnel so they can best navigate sharing information without hazarding the fleet or family. Although standard OPSEC measures apply to social media, there are several new considerations that should be communicated. These are touched on in the "Operations Security" section of this booklet.

MEMBERSHIP WITHIN SOCIAL GROUPS by Sailors and personnel is going to happen. Informal groups such as "The Facebook Group Against Another Uniform Change in the Navy," exist and may draw some of your Sailors and personnel into joining. As long as they do not undermine their chain of command, or otherwise conduct themselves in an unprofessional manner, there is nothing wrong with them connecting with other people on subjects of mutual interest and in fact their participation in groups such as this might provide you valuable information on their thoughts and concerns.

COMMUNICATE EXPECTATIONS ABOUT ONLINE INTERACTIONS with your Sailors and personnel. The Navy encourages Sailors to serve as ambassadors to online communities. The Navy asks Sailors to live their core values online, and understand that communication in social media is both public and international – even when they think they are just talking to family and friends. When commenting about Navy matters, Sailors and Navy personnel need to be transparent about who they are and should identify themselves and their rank and/or position. They should also be clear that their opinions are their own, and do not represent their command or the Navy when commenting publically on Navy topics.

AVOID VIOLATING COPYRIGHT AND TRADEMARK by not including any copyrighted or trademarked material in online posts without written permission from the copyright or trademark holder. This includes embedding a song in a video or using a picture in a blog post. This does not include the use of social media icons that are used to point to an official social media presence.

REPLACE ERROR WITH FACT, not argument, if you are engaging someone else online. If you see an error or misinformation, correct it courteously and factually but do not engage in a heated argument.

ADMIT MISTAKES. If you make a mistake then admit it and correct it immediately. If you do edit a posting online, make it clear that it has been updated or edited – don't just try to make a change and pretend you never made the error. If people can't trust you to own up to your own mistakes you will lose credibility.

Remember that everything posted on the Internet even for a second may live on forever.

More detailed information regarding the responsible use of social media by Navy personnel is included in Enclosure (1), Department of the Navy Guidance on Unofficial Posts

OPERATIONS SECURITY (OPSEC)

"Loose tweets sink fleets" is a modern-day take on a classic saying that loose communication can affect OPSEC, but there is more to OPSEC in social media than just ships' movements. When posting information online, everyone should be cognizant that their audience is likely larger than just those to whom you think you're talking. Keep family safety top-of-mind when talking about service members and their loved ones, as enemies have noted publically that they monitor social media sites for information on families as well as troops and equipment.

PROTECT YOUR FAMILIES by limiting the amount and kind of information that you post about them (their names, their addresses, even their towns or schools) online. How hard would it be for someone to figure out who your loved ones are based on your personal profile? You never know who is watching and collecting information on you.

UNDERSTAND PROFILE SECURITY SETTINGS so you can make informed choices about who sees what in your profile. Just because someone isn't your "friend" doesn't mean that all of your information or even photos are blocked from that person. If you are not managing your personal security settings, it is quite possible that when you leave a comment on a public forum (like the Navy Facebook page) anyone who sees it there (including people you don't know) could see your entire profile. Be mindful that social media sites can change their privacy or security settings with little or no notice. Pay attention to changes, and if in doubt ask the CHINFO for recommended settings.

> *"Establish expectations for your Sailors' behavior online, set the example for them to follow and hold them accountable for their actions online just as you would do elsewhere."*

KEEP CLASSIFIED AND SENSITIVE INFORMATION SAFE by educating your personnel not to discuss critical information such as ship's movements, deployments, personnel rosters, weapons information, etc. If you see what you think is a potential OPSEC breech, document it and remove it as soon as possible. More than likely, the OPSEC violation was done in error or out of ignorance. Have your public affairs officer or command OPSEC officer engage the person to explain to them why his or her post violated OPSEC so that he or she don't repeat the same mistake. If OPSEC violations from this person persist or if there is a spillage or other COMSEC violation (e.g. leak of classified information) notify the command Special Security Officer (SSO) or Security Manager in accordance with Department of the Navy (DON) Information Security Program (ISP) Instruction (SECNAVINST 5510.36A), contact NCIS and send an appropriate OPREP in accordance with the OPNAV Special Incident Reporting Procedures Instruction (OPNAVINST F3100.6).

Professional Standards/ Conduct for Command Leadership

As social media brings the world closer together it also raises some new ethical issues for command leadership. In most cases, ethical issues online can be dealt with using the same ethical guidance that has traditionally guided commanders and Navy leadership. To help guide your use of social media, we have addressed a few of the ethical considerations you might find yourself dealing with online.

ONLINE RELATIONSHIPS WITH SUBORDINATES:

With the ability to connect with everyone in our lives online, it only makes sense that Sailors and personnel might be interested in connecting with you through social media and you with them.

SO SHOULD YOU FRIEND OR FOLLOW THOSE IN YOUR COMMAND? A lot depends how you are using social media. If your social media presence exists simply to engage with people on a professional basis then becoming a friend of one of your Sailors or following them is less of an issue. However, if you use social media actively to communicate with your close friends and family then including Sailors who work for you is a more difficult decision. However you approach your connecting with subordinates from your command, it is up to you to lead by example and ensure that the relationship remains on a professional level and that deference to your rank and position is respected online and in the real world.

MILITARY CONDUCT ONLINE:

When it comes to your position as command leadership, your conduct online should be no different than your conduct in the rest of your life and you should hold that same standard to your Sailors and personnel. If evidence of a violation of command policy, UCMJ, or civil law by one of your Sailors comes to your attention from social media then you can act on it just as if it was witnessed in any other public location. This adds an ethical wrinkle to friending or following your subordinates, but the key is for you to maintain the same relationship with them at work as you do online and to be clear about that.

ENDORSEMENT OF NON-GOVERNMENT CONTENT:

The same guidelines regarding endorsement of non-government organizations and charities applies online, but it can be a challenge knowing when they apply. For example, liking a page on Facebook and following an account on Twitter does not constitute endorsement, just as having a subscription to a newspaper is not endorsing the paper. However, posting content about a business, organization, media or charity (other than CFC or NMCRS) or repurposing existing content about such groups (such as a retweet on Twitter) from an official command presence could be seen as endorsement if there is not a clear tie to the command. For example, linking to or reposting a link to a story about the command on a local television station is okay, but linking to or promoting that station or stories from that station that are not about the command can be considered endorsement and should be avoided.

SELF PROMOTION: Using your rank, job, and/or responsibilities as a means of promoting yourself for personal benefit is not appropriate and can ultimately tarnish the image of you, your command and/or the service.

PAID SUBMISSIONS: Treat requests from non-government blogs for a blog post as a media request and coordinate with your PAO or the next PAO in you chain of command for relevant talking points and assistance in drafting your response. Just like public speaking, it is against Navy Ethics regulations to accept compensation for such posts.

POLITICAL DISCOURSE: As command leadership what you say and do is more visible and taken more seriously than that of your personnel. You have a greater responsibility to speak responsibly, even about issues that you don't intend to reflect on your command or the Navy.

DOD and Navy policy as well as ethical requirements state that Navy personnel acting in their official capacity may not "associate DOD with any partisan political campaign or election, candidate, cause or issue" (SECNAVINST 5720.44B). As a service member you are permitted to express your political views within certain guidelines. The following list is provided to guide your decision in speaking on political topics:

Before engaging in political speech you need to fully consider the following:

- You can express your political views on public issues or political candidates online, but not as part of an organized communication campaign*
- If you are intent on voicing your opinion on a political issue you need to consider where you are going to comment (is it your personal Facebook account, or are you going to write it on a blog) and who the audience is (is it a professional forum or somewhere you use to communicate with your Sailors). In general, you should avoid political comments where they are likely to be viewed by your personnel.
- Don't attempt to hide or obscure your affiliation with the Navy – this just makes what you say more suspect.
- If your communication identifies you as a member of DoD/DON, fully disclose who you are by rank and/or title and disclaim that your opinions are not necessarily those of the Navy*, for example: "…in the interest of full disclosure I am a Captain in the U.S. Navy and Commanding Officer of USS Neversail and the opinions expressed here are my own and not necessarily those of the U.S. Navy."
- Avoid discussing political issues, local or national, that are affiliated with the Navy and Department of Defense as there is a high potential for saying something inappropriate.
- You cannot solicit votes for or against a party, candidate, cause*
- You cannot participate in any interview or discussion as an advocate for or against a party, candidate, cause*
- Avoid ad hominem attacks and keep your political discourse substantive.
- Commissioned officers must avoid contemptuous words against the President, Vice President, SECDEF, Dept. Secretary (i.e. SECNAV), Governor and Legislature of any state he or she is on duty in or present**

For specific, timely guidance please consult the most recent election year public affairs guidance.

* DoD Directive 1344.10 - Political Activities by Members of the Armed Forces
** Title 10 of U.S. Code, Sec. 888. Art. 88. Contempt toward officials

Guidelines and Requirements for Command Social Media

HAVE A SINGLE COMMAND PRESENCE

In larger commands, there is a tendency for offices/units within a command to want to have their own presences. For example, the chapel may want to have its own presence, the Navy Counselor or DAPA for your command may want their own presence. While this is up to the discretion of the command, it is recommended that you maintain a single command presence within each social media platform and allow those different offices/units feed content to the command presence. That means one command Facebook page, Twitter account, and so on. The reason for this is that each subset of the command that has its own social media presence splinters the audience for the command and can increases the time spent managing multiple presences. Unless there is a compelling reason for a social media presence as a subset of the command presence, such as reaching a unique audience; it is strongly recommended that there be only one command social media presence per application.

MANAGING YOU SOCIAL MEDIA PRESENCE

Management of command presences does take time, depending on the popularity of your content and the community size. Although some commands find it useful to have just one main point of contact to manage social media sites, it's strongly recommended that any social media presence be run by a small team to ensure that there is no potential single point of failure for being able to manage information in a timely manner. A commander should choose a team of people that he or she trusts to monitor the command social media presences, develop and post content when needed, remove public posts when required, interact with those who engage the command within that social tool and respond to public inquiry when necessary. Since this will more than likely be a collateral duty for the members of this team, it is recommended that the people you select be motivated out of personal interest to communicate with the command's audiences. Your public affairs officer is a logical choice to head up this team. To ensure consistent management, commands should establish standard operating procedures to monitor, post content, and engage with people. You should not expect to be able to monitor social media for your command around the clock, that's a full time job for anyone! Instead you should aim for your team to be able to check on your command's social media presences periodically throughout the day. By having this work distributed throughout a team of people you will ensure better monitoring and management of social media. Once your team is established you can keep them on task by requiring periodic (weekly, monthly) reports that include basic analytics provided by the social media platforms, popular content, relevant public posts and planned content. Don't remove content or take a page offline unless there is a specific violation of OPSEC or your published business rules warranting removal. Organizations who remove content simply because that content is unflattering lose the trust of their audience and risk very public backlash. The commander has the responsibility to ensure enforcement of the posting policy, but taking something down just because it is unflattering is not recommended and ultimately counterproductive. While the fear of someone posting negative content about your command on your social site is an often cited argument against social media, research finds that about 65% of organization/brand mentions on the Web are positive and only 8% of brand mentions are negative. If an unfairly negative comment is posted by your user on your social site chances others will be addressed by the community you've developed within that social tool.

COMMUNICATING WITH FAMILIES

Many Navy ombudsman and family readiness groups are also using social media to more effectively communicate with families. As a leader it is crucial that you actively participate in your commands' social media presences. Your participation will demonstrate a willingness to listen to your families. Not everything you hear may be positive, but you'll be better positioned to make informed decisions and understand sentiment.

RECORDS KEEPING

Records keeping policy guidance for social media is being developed by USG/DoD. In the interim, it is up to COs and their PAOs to make a determination on when and what kind of information to archive. For example, if a unit is involved in an operation of historical significance then it would be prudent for the command to archive as much of the content of their social media presences as possible for the historical record. Some effective means of archiving information include ensuring the content posted on social presences is also available via a command website, archiving e-mail related to command social presences, taking screen captures of social presences and copying and pasting posted content into a text file or word document.

REGISTRATION

According to the DTM, official use of social media is a public affairs function. This means that any official command use of social media must remain in compliance with Navy public affairs policy. Any content posted to an official social media presence must be either already in the public domain or must be approved for release by the Commanding Officer, Public Affairs Officer or anyone else designated with release authority on behalf of the command. Commands are ultimately responsible for official content posted on their social media presences as well as any presences run by other parts of their command. Contractors may help manage a social media presence but they cannot serve as a spokesperson for the Navy. Also, to the maximum extent possible, any content released by the command must also be present, in some form, on the command website for compliance issues.

The DTM also requires that all official uses of social media be registered with DoD. This is because on many social media platforms anyone can create an account to discuss issues related to any subject, including your command. Therefore, it is necessary to clearly delineate which social media presences are official. This can be done by registering a command presence with the Navy Social Media Directory at www.navy.mil/socialmedia.

Besides being a requirement, registration benefits your command. First, it puts your command social media presences on the social media directory at Navy.mil. It also adds your command point of contact to the distribution list for the weekly social media update e-mail. This e-mail includes news, information and best practices on social media. Finally, registration ensures that your command's presences are included in any USG/DoD Terms of Service (ToS) Agreement(s). For example, official sites on Facebook have targeted advertising removed.

Checklist for Establishing a Command Social Media Presence

CONSIDERATIONS FOR AN OFFICIAL COMMAND SOCIAL MEDIA PRESENCE

□ AUDIENCE

- Identify who you are interested in communicating to and on what social media site(s) you can use to best reach them.

□ BRANDING

- The name of your social media presence is critical; this is how people will find you. Follow the guidelines contained in the Social Media Snapshot on brand management to select the most appropriate name.

□ CONTENT

- Think about the kind of content you intend to post and how frequently you intend to post – including responses to those expressing themselves on your site.

□ MANAGEMENT

- Identify a team of people to manage the social media presence(s). Your trust in them and their good judgment are paramount.
- A diverse team managing the page will be more effective than a single person. A single manager is a single point of failure.

□ POLICY & TRAINING

- Establish a policy to include business rules on how your team will manage the social media presence(s). Hold them to it.
- Train your personnel and their families on the safe and responsible use of social media and what they can expect from your social media presences.
- A good resource for policy and training can be found at www.slideshare.net/USNavySocialMedia

REQUIREMENTS FOR AN OFFICIAL COMMAND SOCIAL MEDIA PRESENCE

□ **COMMANDING OFFICER OR PUBLIC AFFAIRS OFFICER APPROVAL**

- Someone with release authority for the command must approve

□ **THE POC MUST INCLUDE A VALID .MIL ADDRESS WHEN SUBMITTING**

- Only exception is if submission is from a command authorized to use .edu or .com

□ **THE PRESENCE MUST HAVE A URL TO AN OFFICIAL DON WEBSITE**

- Your command's or in the absence of a command site www.navy.mil

□ **THE PRESENCE MUST POST DISCLAIMER TEXT (REQUIRED)**

- The disclaimer identifies the page as an official DON social media presence and disclaims any endorsement
- An approved disclaimer is available at http://www.chinfo.navy.mil/socialmedia/user_agreement.doc

□ **THE PRESENCE MUST HAVE A USER AGREEMENT (AS APPROPRIATE)**

- The user agreement establishes what is acceptable criteria for posts
- This is required for any site where public comment is possible
- An approved user agreement is available at http://www.chinfo.navy.mil/socialmedia/user_agreement.doc

□ **THE PRESENCE MUST BE CLEARLY IDENTIFIED AS "OFFICIAL"**

- Site needs to clearly be identified as an "official" presence
- However, this does not need to appear in the site name

□ **THE PRESENCE MUST BE UNLOCKED AND OPEN TO THE PUBLIC**

- This primarily applies to Twitter

□ **ONLY 'OFFICIAL PAGES' ON FACEBOOK CAN BE REGISTERED AND SHOULD BE LABELED AS "ORGANIZATION-GOVERNMENT"**

- The use of Facebook Profile, Community and Group pages for official purposes is not with the government's terms of service agreement with Facebook

□ **SOCIAL MEDIA PRESENCES IDENTIFYING THE INDIVIDUAL VICE THE COMMAND OR BILLET ARE NOT ACCEPTABLE AS AN "OFFICIAL" PRESENCE WITH THE EXCEPTION OF A NOTABLE FEW (SECNAV, CNO, MCPON).**

- This does not prohibit the use of named accounts by any commander or senior leadership, only the requirement to register the site as "official."

□ **SUBMIT THE SOCIAL MEDIA PRESENCE FOR APPROVAL AND REGISTRATION TO WWW.NAVY.MIL/SOCIALMEDIA.**

Checklist for Operations Security

□ **IDENTIFY** those personnel that you authorize to post content to your social media presences.

□ **ESTABLISH** local procedures to ensure that all information posted on social media is released by you or someone at your command with release authority.

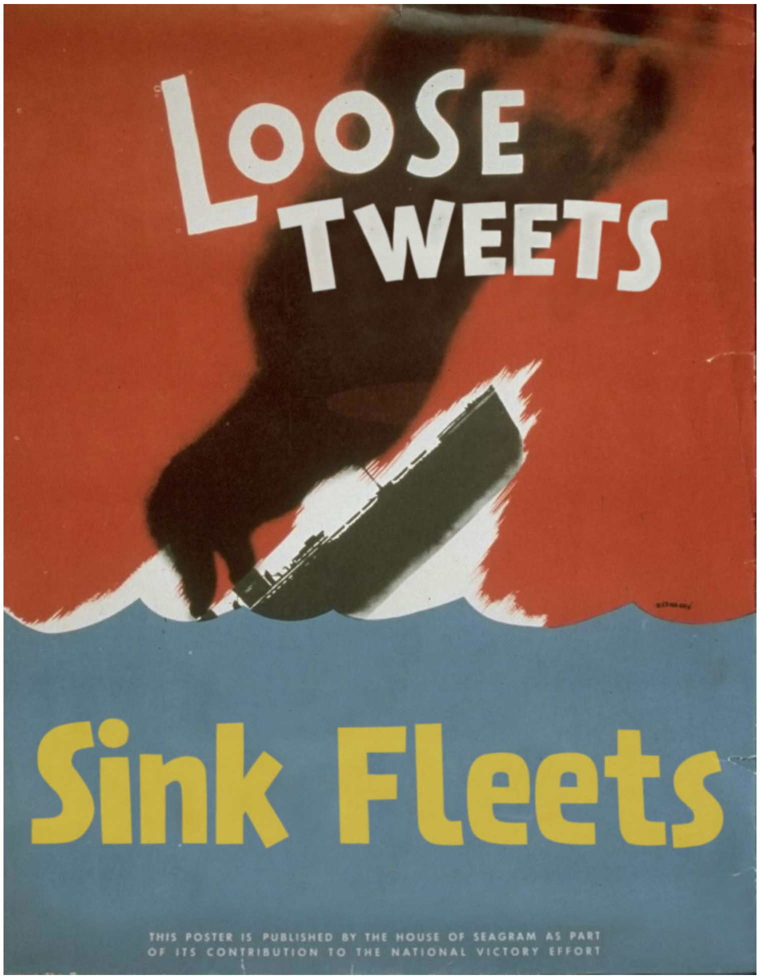
□ **ENSURE** all information posted is done so in accordance with local (ISIC, Numbered Fleet, etc.) Public Affairs Guidance and Navy Public Affairs Regulations.

□ **MONITOR** your social media presences for posts that violate OPSEC and remove as necessary.

□ **CONDUCT** periodic training with your Sailors and families on what kind of content is not appropriate for posting online – and not just to your command's social media presences (i.e. ship's movements, inspection results, personnel issues, etc.)

□ **INFORM** your Sailors and their families about maintaining security settings on their personal social media sites. Otherwise, their information is available to the world

□ Periodically **REMIND** your Sailors and families via your social media presences on maintaining OPSEC.


LOOSE TWEETS
Sink Fleets
THIS POSTER IS PUBLISHED BY THE HOUSE OF SEAGRAM AS PART OF ITS CONTRIBUTION TO THE NATIONAL VICTORY EFFORT

Poster design by Brian Moore Media, Flickr

Crisis Communication

Using social media to communicate with stakeholders during a crisis has already proven to be an especially effective use of the medium due to its speed, reach, and direct access. In recent crisis, social media has facilitated the distribution of command information to key audiences and media while providing a means for dialogue among the affected and interested publics.

YOU CAN'T SURGE TRUST, so your best course of action is to leverage already existing social presences. It is important to have a regularly updated channel of communication open between you and your key audiences before the crisis hits so they not only know where to find you online, but know that they can trust the information they get.

CREATE A CENTRALIZED LOCATION to funnel information. Don't fragment your command into "Command Emergency Services" and "Command Logistics" – make the official command page, or a higher echelon page if appropriate, the nexus for information. If you don't have a command presence then the people most interested in the crisis will more than likely decide as a group where they want to find information and start their own group. Whatever the case, you need to communicate where the people most affected are communicating.

MONITOR INCOMING CONTENT POSTED BY YOUR USERS on your social sites so you can understand what information they need and what is happening to them. Staff appropriately to answer questions as best as possible and ensure that your audience knows you are listening to them and actively engaged in the crisis. Experience shows this will be your single greatest source of RFIs in a crisis.

POST CLEARED INFORMATION AS YOU HAVE IT, and there's no need to wait for a formal press release. When you have solid information that your audiences want to know, post it. If you need to put out updated information later than do so but don't let perfect be the enemy of good enough.

USE MOBILE DEVICES to keep your social presences up to date. The myriad of mobile devices available today – even Navy-issued mobile phones – allow you to update social sites without being tied to your computer at a desk. Whether the base is on lock-down, you're weathering out a storm at home or you're at a remote site at the scene, mobile devices allow you to share quick updates immediately. To that end, ensure your mobile devices are continuously charged. During Hurricane Katrina, bloggers would charge their mobile devices in their car because their power was out indoors. Be creative in finding power solutions that work for your situation.

ANSWER QUESTIONS as often as practicable. Avoid just posting information on a social media presence – that is what command websites are for. Be prepared to have people ask questions. Respond back as quickly as possible through the most appropriate means of communication.

MONITOR EXTERNAL CONVERSATIONS regularly and correct inaccuracies. This is the best way to stop rumors before they run rampant. Use search engines and other monitoring tools to track discussion on the topic.

SHARE AND CROSS-PROMOTE critical information with your network of trusted social media sites, such as other Navy command sites, government and official NGO sites like the American Red Cross. You never know who may be reached through the extended network of the social Web.

ENCOURAGE ON-SCENE AND FIRST-RESPONDER PERSONNEL TO ENGAGE via social media. You can do this by having them either use their personal accounts or feeding you information to post on the official command social sites. Regardless, the command site should promote this content when appropriate.

PROMOTE THE SOCIAL MEDIA PRESENCE on outgoing materials like press releases, e-mail signatures, links on the home page and even in conversations with reporters. The social media presence isn't helpful if it isn't discoverable or people don't know about it.

ANALYZE SUCCESS of crisis communication via social media by looking at click-throughs, conversation, replies and reactions to postings, etc.

Crisis Communication

In crisis situations, information is at a premium. Depending on the event, you may be dealing with a distributed population, interrupted communication ability and a rumor mill running rampant. Your audience will quickly grow from those impacted first-hand by the crisis to family members and the general public who are keeping their eyes on the crisis to see how it unfolds.

In recent years, organizations like the American Red Cross and the Navy, among others, have found social media an effective channel of communication during crisis events. A recent survey conducted by the American Red Cross found that almost half of respondents said they would use social media to tell loved ones they are safe during a crisis, this number up from 16% in a previous poll. Of them, 86% would use Facebook, with a smaller portion turning to Twitter and other tools. If someone else needed help, 44% would try to get help by asking others in a social network to get in touch with authorities. These statistics mixed with the real world case studies of social media being used by commands during the Millington floods in 2010 and the Navy's humanitarian assistance in Haiti show the value of social media in a crisis.

BEFORE

- □ Receive buy in from the command to ensure that the command supports this communication
- □ Establish a command presence on relevant social media platforms. At a minimum we suggest Facebook and Twitter.
- □ Plan and train multiple people at the command to communicate on your social media platforms during a crisis.
- □ Identify keywords that might be used when communicating about your command and any potential crisis you might face. (i.e. crash, collision, evacuation, humanitarian assistance).
- □ Identify your key audiences in a crisis (e.g. families, Sailors, employees, community) and how you will communicate with them in a crisis
- □ Ensure your key audiences in a crisis situation know how you will put out information (e.g., family care line, website, Facebook, local radio, television).
- □ Understand that communication service (such as the telephone or NMCI access) may be interrupted during a crisis. Often times when telephone and cellular phone access is limited, text message and data transmission from mobile devices are the only way to get information out. Devise creative contingency plans for disseminating information, and keep in mind the public affairs officer may be charging his Blackberry in his car in order to manage Facebook because power may be out in the community.

DURING

- □ Communicate as you planned, use all of your communication channels to get information out to relevant audiences.
- □ If you hadn't previously started a social media presence get one off the ground ASAP! If you don't, someone else will communicate in this space for you and it may not be accurate information.
- □ Actively use your social media presences to communicate relevant and timely information. Accuracy is important but don't delay putting out useful information that can effect the safety and security of your audience.
- □ Listen to what your audiences say to you via social media and respond appropriately. This is your opportunity to ensure they are informed and gain useful information during the crisis.
- □ Search keywords surrounding the crisis and note what others are putting out. Are they talking about your command? Do they have the correct information? If not provide them the correct facts. In some cases you will find increased avenues to tell your command's stories, in other instances you may find yourself correcting the record.

AFTER

- □ Ask designated communicators for lessons learned and implement changes to your crisis plan.
- □ Continue to provide interesting updates and information to your audiences to maintain interest in your page.
- □ Thank your community members for spreading the word, helping and supporting each other through this crisis.

Resources

DoD and the Navy have a number of Social Media resources available to you. If there is a specific document, policy, or training product that you are interested in and can't find please contact CHINFO.

POLICY

□ **DTM 09-026 RESPONSIBLE AND EFFECTIVE USE OF INTERNET-BASED CAPABILITIES**
(www.defense.gov/news/dtm%2009-026.pdf)

□ **ALNAV 057/10 INTERNET-BASED CAPABILITIES GUIDANCE – UNOFFICIAL INTERNET POSTS**
(http://www.npc.navy.mil/NR/rdonlyres/CB77304E-B380-4844-9558-536F6BC72157/0/ALN10057.txt)

□ **ALNAV 056/10 INTERNET-BASED CAPABILITIES GUIDANCE – OFFICIAL INTERNET POSTS**
(http://www.npc.navy.mil/NR/rdonlyres/AD9DB957-11CC-4118-92F8-6CB2CD54D768/0/ALN10056.txt)

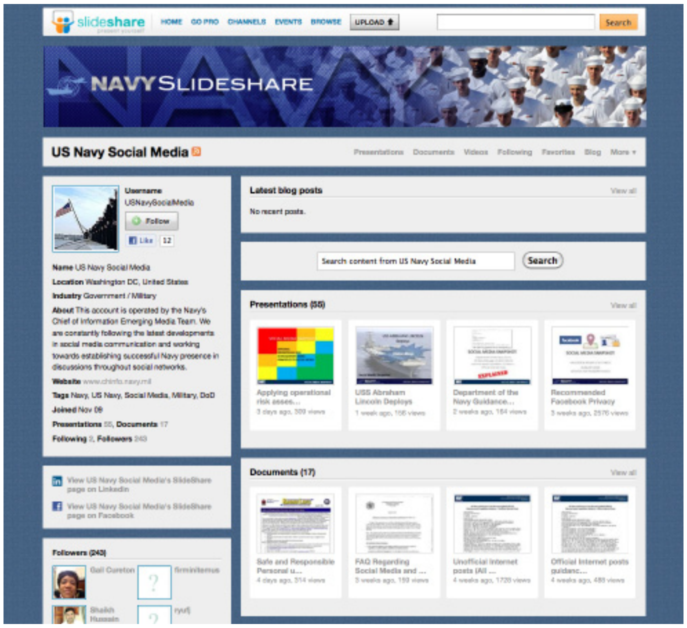
SITES:

□ **DOD SOCIAL MEDIA HUB**
(http://socialmedia.defense.gov/)
A resource page containing policy, training, and guidance

□ **NAVY SOCIAL MEDIA DIRECTORY**
(www.navy.mil/socialmedia)
The Navy's directory of approved social media presences. Command's can submit their social media presence here for approval.

□ **CHINFO SOCIAL MEDIA RESOURCES PAGE**
(available on www.chinfo.navy.mil)
The Navy's social media resource page for links to policy, training, and guidance

□ **NAVY SOCIAL MEDIA ON SLIDESHARE**
(www.slideshare.net/USNavySocialMedia)
A document hosting service that the Navy's Social Media team uses to host training, how-to's, guidance and best practice briefs and documents.



US Navy Social Media

Username USNavySocialMedia

Name US Navy Social Media
Location Washington DC, United States
Industry Government / Military
About This account is operated by the Navy's Chief of Information Emerging Media Team. We are constantly following the latest developments in social media communication and working towards establishing successful Navy presence in discussions throughout social networks.
Website www.chinfo.navy.mil
Tags Navy, US Navy, Social Media, Military, DoD
Joined Nov 09
Presentations 55, Documents 17
Following 2, Followers 243

View US Navy Social Media's SlideShare page on LinkedIn
View US Navy Social Media's SlideShare page on Facebook

Followers (243)

Latest blog posts
No recent posts.

Search content from US Navy Social Media

Presentations (55)
Applying operational risk asses... 3 days ago, 309 views
USS Abraham Lincoln Deploys 1 week ago, 156 views
Department of the Navy Guidance... 2 weeks ago, 164 views
Recommended Facebook Privacy 3 weeks ago, 2576 views

Documents (17)
Safe and Responsible Personal u... 4 days ago, 314 views
FAQ Regarding Social Media and ... 3 weeks ago, 159 views
Unofficial Internet posts (All ... 4 weeks ago, 1728 views
Official Internet posts guidanc... 4 weeks ago, 488 views

U.S. Navy Social Media SlideShare account, www.slideshare.net/usnavysocialmedia

Enclosure (1)

DEPARTMENT OF THE NAVY GUIDANCE ON OFFICIAL POSTS

R 192027Z AUG 10
FM SECNAV WASHINGTON DC
TO ALNAV
ALNAV 056/10 SUBJ/INTERNET-BASED CAPABILITIES GUIDANCE - OFFICIAL INTERNET POSTS//
REF/A/DESC:DIRECTIVE-TYPE MEMORANDUM (DTM) 09-026/DEPSECDEF/25FEB2010//
REF/B/DESC:DOD DIRECTIVE 5230.09/DA&M, DOD/22AUG2008//
REF/C/DESC:DOD 5500.7-R/GC, DOD/23MAR2006//
REF/D/DESC:SECNAVINST 5720.44B/OI-5/1NOV2005//
REF/E/DESC:SECNAVINST 5720.47B/CHINFO/28DEC2005//
REF/F/DESC:SECNAVINST 5211.5E/DNS-36/28DEC2005//
REF/G/DESC:SECNAVINST 5239.3B/DON CIO/17JUN2009//
REF/H/DESC:DODMAN 5205.02-M/USD-I/03NOV2008//
REF/I/DESC:5 U.S.C. 552a, THE PRIVACY ACT OF 1974-AS AMENDED//
REF/J/DESC:U.S. NAVY REGULATIONS//
REF/K/DESC:DOD DIRECTIVE 1344.10/USD(P&R)/19FEB2008//
NARR/REF A IS DOD POLICY FOR THE RESPONSIBLE AND EFFECTIVE USE OF INTERNET-BASED CAPABILITIES. REF B IS DOD POLICY FOR CLEARANCE OF DOD INFORMATION FOR PUBLIC RELEASE. REF C IS THE JOINT ETHICS REGULATION. REF D IS DON PUBLIC AFFAIRS POLICY AND REGULATIONS. REF E IS DON POLICY FOR CONTENT OF PUBLICLY ACCESSIBLE WORLD WIDE WEB SITES. REF F IS DON PRIVACY ACT PROGRAM. REF G IS THE DON INFORMATION ASSURANCE POLICY. REF H IS THE DOD OPERATIONS SECURITY (OPSEC) PROGRAM MANUAL. REF I IS THE PRIVACY ACT OF 1974, AS AMENDED. REF J IS U.S. NAVY REGULATIONS. REF K IS THE DOD POLICY FOR POLITICAL ACTIVITIES BY MEMBERS OF THE ARMED FORCES.//
POC/ANN ANDREW/CIV/DON CIO/TEL: 703-607-5608/EMAIL: ANN.ANDREW(AT)NAVY.MIL//
POC/ALAN GOLDSTEIN/CIV/CHINFO POLICY/TEL:703-695-1887/ EMAIL: ALAN.P.GOLDSTEIN(AT)NAVY.MIL//
POC/JULIANA ROSATI/CDR/OPNAVN2N6C3/TEL: 703-601-1717/EMAIL: JULIANA.ROSATI(AT)NAVY.MIL//
POC/GREG REEDER/CIV/UNIT: DMA (MARINE CORPS)/TEL: 703-602-2001/EMAIL: GREGORY.REEDER(AT)AFN.DMA.MIL//
GENTEXT/REMARKS/ 1. THIS ALNAV PROVIDES GUIDANCE TO ALL DEPARTMENT OF NAVY (DON) PERSONNEL REGARDING OFFICIAL POSTS ON INTERNET-BASED CAPABILITIES. A SEPARATE ALNAV PROVIDES GUIDANCE REGARDING UNOFFICIAL POSTS ON INTERNET-BASED CAPABILTIES.

2. DEFINITIONS: PER REF A, THE FOLLOWING DEFINITIONS APPLY:

A. INTERNET-BASED CAPABILITIES (IBC) – PUBLICLY ACCESSIBLE INFORMATION CAPABILITIES AND APPLICATIONS AVAILABLE ACROSS THE INTERNET IN LOCATIONS NOT OWNED, OPERATED, OR CONTROLLED BY THE DEPARTMENT OF DEFENSE OR THE FEDERAL GOVERNMENT. INTERNET-BASED CAPABILITIES INCLUDE COLLABORATIVE TOOLS SUCH AS SOCIAL NETWORKING SERVICES, SOCIAL MEDIA, USER-GENERATED CONTENT, SOCIAL SOFTWARE, WEB-BASED E-MAIL, INSTANT MESSAGING, AND DISCUSSION FORUMS (E.G., YOUTUBE, FACEBOOK, MYSPACE, TWITTER, GOOGLE APPS).

B. OFFICIAL USES OF INTERNET-BASED CAPABILITIES

(1) EXTERNAL OFFICIAL PRESENCES – OFFICIAL PUBLIC AFFAIRS ACTIVITIES CONDUCTED ON NON-DOD SITES ON THE INTERNET (E.G., THE ‘U.S. NAVY’ AND ‘MARINE CORPS NEWS’ FACEBOOK PAGES, INDIVIDUAL COMMAND TWITTER ACCOUNTS). THESE PRESENCES FUNCTION AS EXTENSIONS OF, NOT IN LIEU OF, OFFICIAL DON WEB SITES.

(2) OFFICIAL REPRESENTATION – ACTIVITIES SUCH AS AUTHORIZED COMMAND REPRESENTATIVES COMMENTING IN AN OFFICIAL CAPACITY ON FACEBOOK FAN PAGES, MILITARY INTEREST BLOGS (MILBLOGS), AND SIMILAR IBC.

(3) NON-PUBLIC AFFAIRS USE OF IBC – OFFICIAL USE OF AN IBC IS PERMITTED TO SUPPORT MISSION RELATED FUNCTIONS (E.G. USE OF A WIKI OR OTHER IBC FOR COLLABORATION WITH PARTNERS EXTERNAL TO THE DOD).

3. GUIDANCE.

A. PER REF A, OFFICIAL DON INFORMATION MAY BE DISSEMINATED VIA INTERNET-BASED CAPABILITIES, PROVIDED SUCH DISSEMINATION IS IN COMPLIANCE WITH REFS A THRU K. THE DON RECOGNIZES THE VALUE OF THESE COMMUNICATION CHANNELS IN POSTING CURRENT INFORMATION FOR OUR VARIOUS CONSTITUENTS AND SUPPORTING THE MORALE OF PERSONNEL, THEIR FAMILIES AND FRIENDS. THIS FREE FLOW OF INFORMATION CONTRIBUTES TO LEGITIMATE TRANSPARENCY OF THE DON TO THE U.S. PUBLIC WHOM WE SERVE.

B. THE DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER (DON CIO), CHIEF OF INFORMATION (CHINFO), MARINE CORPS DIRECTOR OF PUBLIC AFFAIRS (DIRPA), DEPUTY DON CIO (NAVY) AND DEPUTY DON CIO (MARINE CORPS) WILL COORDINATE A DETAILED POLICY SPECIFYING ROLES AND RESPONSIBILITIES TO ENSURE THE SAFE AND EFFECTIVE ADMINISTRATION OF OFFICIAL USE OF INTERNET-BASED CAPABILITIES TO INCLUDE EXTERNAL OFFICIAL PRESENCES. THIS WILL INCLUDE A CONSISTENT PROCESS FOR THE REGISTRATION, REVIEW, APPROVAL AND MONITORING OF ALL DON OFFICIAL PRESENCES ON INTERNET-BASED CAPABILITIES.

C. CURRENTLY, CHINFO AND USMC DIRPA MAINTAIN REGISTRIES OF EXTERNAL OFFICIAL PRESENCES ON INTERNET-BASED CAPABILITIES FOR NAVY AND USMC RESPECTIVELY. THESE REGISTRIES INCLUDE A PUBLICLY ACCESSIBLE DIRECTORY OF VALIDATED DON OFFICIAL

Enclosure (1)

EXTERNAL PRESENCES. UNTIL FUTURE POLICY IS RELEASED DETAILING A DON IBC REGISTRATION AND APPROVAL PROCESS, NAVY COMMANDS MUST SUBMIT THEIR EXTERNAL OFFICIAL PRESENCES FOR REVIEW AND APPROVAL TO WWW.NAVY.MIL/SOCIALMEDIA. USMC COMMANDS MUST SUBMIT THEIR EXTERNAL OFFICIAL PRESENCES FOR REVIEW AND APPROVAL TO WWW.MARINES.MIL/SOCIALMEDIA.

D. COMMANDS MUST DESIGNATE ADMINISTRATORS FOR OFFICIAL USE OF IBC TO INCLUDE EXTERNAL OFFICIAL PRESENCES. THE ADMINSTRATOR IS RESPONSIBLE TO ENSURE POSTINGS TO THE IBC COMPLY WITH CONTENT RESTRICTIONS AND THE IBC IS CONFIGURED SECURELY IN COORDINATION WITH THE COMMAND INFORMATION ASSURANCE MANAGER (IAM). COMMANDS THAT PERMIT POSTINGS BY OTHERS (E.G. FANS) MUST ENSURE THE SITE CONTAINS AN APPROVED USER AGREEMENT DELINEATING THE TYPES OF INFORMATION THAT ARE UNACCEPTABLE FOR POSTING TO THE SITE AND MUST REMOVE UNACCEPTABLE CONTENT. AT A MINIMUM, THE DON'S CURRENT SOCIAL MEDIA USER AGREEMENT IS REQUIRED. THIS AGREEMENT IS FOUND AT WWW.CHINFO.NAVY.MIL/SOCIALMEDIA/USER_AGREEMENT.DOC (NOTE UNDERSCORE BETWEEN THE WORDS OF THE FILE NAME).

E. EXTERNAL OFFICIAL PRESENCES SHALL LINK TO THE COMMAND/ACTIVITY'S OFFICIAL WORLD WIDE WEB SITE.

F. COMMANDS/ACTIVITIES MUST DEVELOP AND PUBLISH LOCAL PROCEDURES FOR THE APPROVAL AND RELEASE OF ALL INFORMATION, OF ANY MEDIA, POSTED ON COMMAND/ACTIVITY OFFICIAL USE OF INTERNET-BASED CAPABILITIES TO ENSURE POSTED INFORMATION MEETS REQUIREMENTS SET FORTH IN REFS (A) THROUGH (K).

G. COMMANDS MUST ACTIVELY MONITOR AND EVALUATE OFFICIAL USE OF IBC FOR COMPLIANCE WITH SECURITY REQUIREMENTS AND FOR FRAUDULENT OR OBJECTIONABLE USE.

H. OFFICIAL REPRESENTATIONS MAY BE POSTED ONLY BY THOSE AUTHORIZED TO RELEASE OFFICIAL INFORMATION TO THE PUBLIC. THIS MAY INCLUDE AN INDIVIDUAL WHO IS POSTING UNDER THE SUPERVISION OF THOSE AUTHORIZED TO RELEASE OFFICIAL INFORMATION. CONTRACTED PUBLIC AFFAIRS AND COMMUNICATIONS MANAGEMENT PERSONNEL ARE NOT AUTHORIZED TO PUBLISH CONTENT TO A COMMAND/ACTIVITY EXTERNAL OFFICIAL PRESENCE UNLESS A DON OFFICIAL WITH THE AUTHORITY FOR PUBLIC RELEASE OF INFORMATION APPROVES AND CONTROLS THE CONTENT.

I. INFORMATION POSTED IN AN OFFICIAL CAPACITY TO ANY INTERNET-BASED CAPABILITY MUST NOT INCLUDE:

(1) CLASSIFIED INFORMATION, PRE-DECISIONAL INFORMATION, PROPRIETARY INFORMATION, BUSINESS SENSITIVE INFORMATION, OPSEC INDICATORS, INFORMATION DESIGNATED AS FOR OFFICIAL USE ONLY (FOUO), OR PRIVILEGED INFORMATION, UNDER APPLICABLE LAW.

(2) INFORMATION PROTECTED BY THE PRIVACY ACT OF 1974 OR THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) OF 1996.

(3) INFORMATION, OTHER THAN AUTHORIZED RELEASES, ABOUT CASUALTIES PRIOR TO OFFICIAL CONFIRMATION THAT NEXT OF KIN HAVE BEEN NOTIFIED AND A COMPETENT AUTHORITY AUTHORIZES PUBLICATION OF SPECIFIC CASUALTY INFORMATION. COMMANDERS ARE REMINDED THAT CASUALTY INFORMATION IS TO BE TIGHTLY CONTROLLED AND HEAVILY SCRUTINIZED.

(4) INFORMATION, OTHER THAN AUTHORIZED RELEASES, REGARDING EVENTS OR INCIDENTS CURRENTLY UNDER INVESTIGATION.

(5) INFORMATION THAT IS UNDER COPYRIGHT OR TRADEMARK, WITHOUT PERMISSION OF THE HOLDER.

(6) UNIT OR OTHER PERSONNEL LISTS/ROSTERS, CHARTS OR DIRECTORIES, WITH THE NAMES, ADDRESSES AND TELEPHONE NUMBERS OF UNIT MEMBERS. THIS PROVISION DOES NOT APPLY TO THE NAME, RANK, OR BUSINESS CONTACT INFORMATION FOR A CO, XO, CMC OR COMMAND OMBUDSMEN OR AS OTHERWISE REQUIRED IN THIS DIRECTIVE.

(7) MATERIAL THAT IS POLITICAL IN NATURE OR TENDS TO ENDORSE POLITICAL PARTIES, CANDIDATES, CAMPAIGNS, REFERENDUMS, BALLOT INITIATIVES, OR OTHER POLITICAL CAUSES.

(8) MATERIAL THAT ENDORSES/PROMOTES NON-FEDERAL ENTITY (NFE) PRODUCTS, NFE SERVICES, OR NFE ENTERPRISES OTHER THAN THOSE OFFICIALLY ENDORSED BY THE DEPARTMENT OF THE NAVY.

(9) POSTED LINKS TO COMMERCIAL CONTENT WHICH MAY IMPLY ENDORSEMENT. THIS INCLUDES THOSE TO COMMERCIAL ENTITIES, CHARITIES OR CAUSES (EXCEPT THOSE AUTHORIZED BY STATUTE OR REFS C AND E).

J. LINKS TO ARTICLES OR POSTS ABOUT THE DOD, THE DON OR ANY COMPONENT THEREOF ARE PERMITTED.

K. INFORMATION POSTED IN AN OFFICIAL CAPACITY TO ANY INTERNET-BASED CAPABILITY MUST:

(1) BE CLEARLY IDENTIFIED AS BEING MADE BY AN AUTHORIZED MEMBER OF THE COMMAND/ACTIVITY TO INCLUDE NAME, RANK, AND TITLE OF THE AUTHOR UNLESS POSTED BY AN ADMINISTRATOR, WHERE IT IS CLEAR THE POST IS OFFICIAL IN NATURE.

(2) MAKE NO ATTEMPT TO DISGUISE, IMPERSONATE OR OTHERWISE MISREPRESENT THE IDENTITY OR AFFILIATION OF THE AUTHOR. ANONYMOUS POSTS ARE PROHIBITED.

(3) BE TRUTHFUL, ACCURATE, AND WRITTEN IN A PROFESSIONAL MANNER, INCLUDING CORRECT SPELLING AND GRAMMAR.

(4) NOT VIOLATE APPLICABLE U.S. NAVY REGULATIONS REGARDING COMMENTARY REFLECTING ON A SUPERIOR OR RELEASE OF INFORMATION ABOUT PRIVATE INDIVIDUALS.

(5) IN CASES NECESSITATING A CORRECTION OF A PREVIOUS POST BY ANOTHER CONTRIBUTOR TO THE INTERNET-BASED CAPABILITY, BE DONE IN A RESPECTFUL, CLEAR AND CONCISE MANNER. PERSONAL ATTACKS ARE PROHIBITED.

4. ADDITIONAL INFORMATION ABOUT THE USE OF INTERNET-BASED CAPABILITIES FOR EXTERNAL OFFICIAL PRESENCES AND PUBLIC AFFAIRS POLICY, GUIDANCE, TRAINING, AND RECOMMENDED BEST PRACTICES IS AVAILABLE AT WWW.CHINFO.NAVY.MIL/SOCIALMEDIA.HTML (NAVY) OR WWW.MARINES.MIL/SOCIALMEDIA (MARINE CORPS). FOR QUESTIONS REGARDING THE USE OF INTERNET-BASED CAPABILITIES, NOT RELATED TO PUBLIC AFFAIRS ACTIVITIES IN THE DON, PLEASE CONTACT THE AFOREMENTIONED DON CIO POC.

5. RELEASED BY RAY MABUS, SECRETARY OF THE NAVY.//

Enclosure (2)

DEPARTMENT OF THE NAVY GUIDANCE ON UNOFFICIAL POSTS

R 192031Z AUG 10
FM SECNAV WASHINGTON DC
TO ALNAV
ALNAV 057/10 SUBJ/INTERNET-BASED CAPABILITIES GUIDANCE - UNOFFICIAL INTERNET POSTS//
REF/A/DESC: DIRECTIVE-TYPE MEMORANDUM (DTM) 09-26/DEPSECDEF/25FEB2010//
REF/B/DESC: DOD REGULATION 5500.7R/GC, DOD/23MAR2006//
REF/C/DESC: SECNAVINST 5211.5E/DNS-36/28DEC2005//
REF/D/DESC: SECNAVINST 5720.44B/OI-5/1NOV2005//

NARR/REF A IS DOD POLICY FOR THE RESPONSIBLE AND EFFECTIVE USE OF INTERNET-BASED CAPABILITIES. REF B IS THE DOD JOINT ETHICS REGULATION. REF C IS THE DON PRIVACY PROGRAM. REF D IS THE DON PUBLIC AFFAIRS POLICY AND REGULATIONS.//

POC/ANN ANDREW/CIV/DON CIO/TEL: 703-607-5608/EMAIL: ANN.ANDREW(AT)NAVY.MIL//
POC/ALAN GOLDSTEIN/CIV/CHINFO/TEL: 703-695-1887/EMAIL: ALAN.P.GOLDSTEIN(AT)NAVY.MIL//
POC/RAY LETTEER/CIV/HQMC(C4)/TEL:703-693-3490-X128/EMAIL:RAY.LETTEER(AT)USMC.MIL//
POC/JULIANA ROSATI/CDR/OPNAVN2N6C3/TEL: 703-601-1717/EMAIL: JULIANA.ROSATI(AT)NAVY.MIL//

GENTEXT/REMARKS/1. THIS ALNAV PROVIDES GUIDANCE TO ALL DEPARTMENT OF NAVY (DON) PERSONNEL REGARDING UNOFFICIAL POSTS ON THE INTERNET, INCLUDING THOSE PERTAINING TO DON-RELATED CONTENT AND DISCUSSIONS. IT ALSO PROVIDES GUIDANCE ABOUT BEST-PRACTICES FOR USE OF INTERNET-BASED CAPABILITIES (IBC) IN A PERSONAL CAPACITY. A SEPARATE ALNAV PROVIDES GUIDANCE FOR EXTERNAL OFFICIAL PRESENCES ON IBC ON BEHALF OF THE DON.

A. “DON PERSONNEL” IS DEFINED AS ACTIVE-DUTY AND RESERVE COMPONENT SAILORS AND MARINES AND CIVILIAN EMPLOYEES OF THE DON.

B. PER REF A, IBC ARE DEFINED AS PUBLICLY ACCESSIBLE INFORMATION CAPABILITIES AND APPLICATIONS AVAILABLE ACROSS THE INTERNET IN LOCATIONS NOT OWNED, OPERATED, OR CONTROLLED BY THE DEPARTMENT OF DEFENSE OR THE FEDERAL GOVERNMENT. IBC INCLUDES COLLABORATIVE TOOLS SUCH AS SOCIAL NETWORKING SERVICES, SOCIAL MEDIA, USER-GENERATED CONTENT, SOCIAL SOFTWARE, WEB-BASED E-MAIL, INSTANT MESSAGING, AND DISCUSSION FORUMS (E.G., YOUTUBE, FACEBOOK, MYSPACE, TWITTER, GOOGLE APPS).

C. OFFICIAL INTERNET POSTS INVOLVE CONTENT THAT HAS BEEN RELEASED IN AN OFFICIAL CAPACITY BY DON PUBLIC AFFAIRS PERSONNEL OR COMMANDERS DESIGNATED AS RELEASING AUTHORITIES.

D. “UNOFFICIAL INTERNET POSTS” IS DEFINED AS ANY CONTENT ABOUT THE DON OR RELATED TO THE DON THAT IS POSTED ON ANY INTERNET SITE BY DON PERSONNEL IN AN UNOFFICIAL AND PERSONAL CAPACITY. CONTENT INCLUDES, BUT IS NOT LIMITED TO, PERSONAL COMMENTS, PHOTOGRAPHS, VIDEO, AND GRAPHICS. INTERNET SITES INCLUDE SOCIAL NETWORKING SITES, BLOGS, FORUMS, PHOTO- AND VIDEO-SHARING SITES, AND OTHER SITES, TO INCLUDE SITES NOT OWNED, OPERATED OR CONTROLLED BY THE DON OR DEPARTMENT OF DEFENSE. UNOFFICIAL INTERNET POSTS ARE NOT ENDORSED BY ANY PART OF THE DON OR REVIEWED WITHIN ANY OFFICIAL DON APPROVAL PROCESS.

2. PER THE GUIDELINES PROVIDED IN THIS ALNAV, DON PERSONNEL ARE ENCOURAGED TO RESPONSIBLY ENGAGE IN UNOFFICIAL INTERNET POSTING ABOUT THE DON AND DON-RELATED TOPICS. THE NAVY AND MARINE CORPS PERFORM A VALUABLE SERVICE AROUND THE WORLD EVERY DAY AND DON PERSONNEL ARE FREQUENTLY IN A POSITION TO SHARE OUR SUCCESSES WITH A GLOBAL AUDIENCE VIA THE INTERNET.

3. GUIDELINES. DON PERSONNEL ARE RESPONSIBLE FOR ALL DON-RELATED CONTENT THEY PUBLISH ON SOCIAL NETWORKING SITES, BLOGS, OR OTHER IBC AND SHOULD ENSURE THAT THIS CONTENT IS ACCURATE, APPROPRIATE AND DOES NOT COMPROMISE MISSION SECURITY OR SUCCESS. IN ADDITION TO ENSURING DON-RELATED CONTENT IS ACCURATE AND APPROPRIATE, IT IS RECOMMENDED THAT DON PERSONNEL BE MINDFUL ABOUT THE NON-DEPARTMENT RELATED CONTENT THEY POST SINCE THE LINES BETWEEN PERSONAL AND PROFESSIONAL LIVES OFTEN BLUR IN THE ONLINE SPACE. ALSO, DON PERSONNEL MUST BE AWARE THAT ONCE THEY POST CONTENT TO THE INTERNET, THEY LOSE CONTROL OF IT; MANY SOCIAL MEDIA SITES HAVE POLICIES THAT GIVE THEM OWNERSHIP OF ALL CONTENT AND INFORMATION POSTED OR STORED ON THEIR SYSTEMS. THUS DON PERSONNEL SHOULD USE THEIR BEST JUDGMENT AT ALL TIMES AND KEEP IN MIND HOW THE CONTENT OF THEIR POSTS WILL REFLECT UPON THEMSELVES, THEIR SERVICE, AND THE DON. THE FOLLOWING GUIDELINES ARE ESTABLISHED TO ASSIST WITH THIS RESPONSIBILITY:

A. DON PERSONNEL ENGAGED IN UNOFFICIAL INTERNET POSTING ABOUT THE DON MAY IDENTIFY THEMSELVES AS DON PERSONNEL BY RANK, BILLET, MILITARY OCCUPATIONAL SPECIALTY, AND STATUS (ACTIVE, RESERVE, CIVILIAN, ETC.) IF DESIRED. HOWEVER, IF DON PERSONNEL DECIDE TO IDENTIFY THEMSELVES AS DON PERSONNEL, THEY MUST NOT DISGUISE, IMPERSONATE OR OTHERWISE MISREPRESENT THEIR IDENTITY OR AFFILIATION WITH THE DON. WHEN EXPRESSING DON-RELATED PERSONAL OPINIONS, DON

Enclosure (2)

PERSONNEL SHOULD MAKE CLEAR THAT THEY ARE SPEAKING FOR THEMSELVES AND NOT ON BEHALF OF THE DON.

B. USE OF PERSONAL EMAIL ADDRESSES IS STRONGLY ENCOURAGED WHEN ENGAGING IBC FOR UNOFFICIAL PURPOSES. THIS INCLUDES, BUT IS NOT LIMITED TO, REGISTRATION WITH SOCIAL NETWORKING SITES AND COMMENTING IN FORUMS AND BLOGS. WHEN IT IS NOT FEASIBLE TO MAKE USE OF PERSONAL EMAIL ADDRESSES FOR THESE PURPOSES, DON PERSONNEL MAY USE THEIR DON PROVIDED EMAIL ADDRESSES.

C. AS WITH OTHER FORMS OF COMMUNICATION, DON PERSONNEL ARE RESPONSIBLE FOR ADHERING TO DON REGULATIONS AND POLICIES WHEN MAKING UNOFFICIAL INTERNET POSTS. DON PERSONNEL SHOULD COMPLY WITH REGULATIONS AND POLICIES SUCH AS PERSONAL STANDARDS OF CONDUCT, OPERATIONS SECURITY, INFORMATION ASSURANCE, PERSONALLY IDENTIFIABLE INFORMATION (PII), JOINT ETHICS REGULATIONS, AND THE RELEASE OF INFORMATION TO THE PUBLIC. VIOLATIONS OF REGULATIONS OR POLICIES MAY RESULT IN DISCIPLINARY ACTION. SEE REFS B AND C.

D. THE POSTING OR DISCLOSURE OF INTERNAL DON DOCUMENTS OR INFORMATION THAT THE DON HAS NOT OFFICIALLY RELEASED TO THE PUBLIC IS PROHIBITED. THIS INCLUDES CLASSIFIED, CONTROLLED UNCLASSIFIED INFORMATION (CUI), OR SENSITIVE INFORMATION (FOR EXAMPLE, TACTICS, TROOP MOVEMENTS, FORCE SIZE, WEAPON SYSTEM DETAILS, ETC). THIS POLICY APPLIES NO MATTER HOW DON PERSONNEL COME INTO POSSESSION OF THE INFORMATION OR DOCUMENT. EXAMPLES INCLUDE, BUT ARE NOT LIMITED TO, MEMOS, E-MAILS, MEETING NOTES, MESSAGE TRAFFIC, WHITE PAPERS, PUBLIC AFFAIRS GUIDANCE, PRE-DECISIONAL MATERIALS, INVESTIGATORY INFORMATION, AND PROPRIETARY INFORMATION. DON PERSONNEL ARE ALSO PROHIBITED FROM RELEASING OTHER THAN THEIR OWN DON E-MAIL ADDRESSES, TELEPHONE NUMBERS, OR FAX NUMBERS NOT ALREADY AUTHORIZED FOR PUBLIC RELEASE. WHEN IN DOUBT, DON PERSONNEL SHOULD CONTACT THEIR OPERATIONS SECURITY OFFICER, INTELLIGENCE OFFICER, FREEDOM OF INFORMATION ACT (FOIA) OFFICIAL, OR PUBLIC AFFAIRS OFFICER FOR GUIDANCE.

E. WHEN CORRECTING ERRORS AND MISREPRESENTATIONS MADE ABOUT THE DON, PERSONNEL ARE ENCOURAGED TO BE PROFESSIONAL AND RESPECTFUL. DON PERSONNEL SHOULD REFER TO THE CHAIN OF COMMAND OR PUBLIC AFFAIRS FOR GUIDANCE IF UNCERTAIN ABOUT THE NEED FOR, OR APPROPRIATENESS OF, A RESPONSE.

F. DON PERSONNEL SHOULD BE AWARE THAT THE INTERNET IS OFTEN USED TO GAIN INFORMATION FOR CRIMINAL ACTIVITIES SUCH AS IDENTITY THEFT. BY PIECING TOGETHER INFORMATION PROVIDED ON DIFFERENT WEBSITES, CRIMINALS CAN USE INFORMATION TO, AMONG OTHER THINGS, IMPERSONATE DON PERSONNEL, STEAL PASSWORDS, AND COMPROMISE DON NETWORKS. THEREFORE, WHEN USING THE INTERNET AND SOCIAL MEDIA, DON PERSONNEL SHOULD BE CAUTIOUS AND GUARD AGAINST CYBER CRIMINALS AND ATTACKERS BY ADHERING TO THE FOLLOWING SECURITY PROCEDURES.

(1) DON PERSONNEL SHOULD BE MINDFUL OF RELEASING PII THAT COULD BE USED TO DISTINGUISH THEIR INDIVIDUAL IDENTITY OR THAT OF ANOTHER INDIVIDUAL. EXAMPLES OF PII INCLUDE SOCIAL SECURITY NUMBER, ADDRESS, BIRTHDAY, BIRTH PLACE, DRIVER'S LICENSE NUMBER, ETC.

(2) DON PERSONNEL SHOULD BE CAREFUL WHEN RESPONDING VIA EMAIL TO IBC AUTOMATIC NOTIFICATIONS, SINCE THIS MAY INADVERTENTLY EXPOSE PERSONAL AND WORK RELATED CONTACT INFORMATION CONTAINED IN THE EMAIL SIGNATURE LINE.

(3) DON PERSONNEL SHOULD NOT CLICK LINKS OR OPEN ATTACHMENTS UNLESS THEY TRUST THE SOURCE. CYBER CRIMINALS OFTEN PRETEND TO BE PEOPLE THEY ARE NOT IN ORDER TO DECEIVE INDIVIDUALS INTO PERFORMING ACTIONS THAT LAUNCH CYBER ATTACKS, DOWNLOAD VIRUSES, AND INSTALL MALWARE AND SPYWARE ONTO COMPUTERS. TO HELP MITIGATE THESE THREATS, DON PERSONNEL SHOULD INSTALL AND MAINTAIN CURRENT ANTI-VIRUS AND ANTI-SPYWARE SOFTWARE ON THEIR PERSONAL COMPUTERS. MILITARY AND CIVILIAN EMPLOYEES OF THE DON MAY OBTAIN ANTI-VIRUS SOFTWARE FOR HOME USE, FROM HTTPS://INFOSEC.NAVY.MIL/AV OR HTTPS://WWW.JTFGNO.MIL/ANTIVIRUS/ANTIVIRUS_HOMEUSE.HTM. YOU MUST ACCESS THESE SITES FROM A .MIL DOMAIN.

(4) DON PERSONNEL SHOULD ALWAYS USE THE STRONGEST PASSWORD COMBINATIONS ALLOWED, COMPRISED OF AS MANY OF THE COMBINATIONS OF LOWER- AND UPPER-CASE LETTERS, NUMBERS, AND SYMBOLS POSSIBLE. CHANGE PASSWORDS FREQUENTLY. USE DIFFERENT PASSWORDS FOR BANKING AND FINANCIAL SITES AND PERSONAL WEB-BASED EMAIL THAN THOSE FOR ANY OTHER SITE.

(5) DON PERSONNEL SHOULD BE THOUGHTFUL ABOUT WHO THEY ALLOW TO ACCESS THEIR SOCIAL MEDIA PROFILES (E.G. "FRIENDS" OR "FOLLOWERS" ON SITES SUCH AS FACEBOOK, MYSPACE, OR TWITTER) AND THUS ALLOW ACCESS TO THEIR PERSONAL INFORMATION. DON PERSONNEL SHOULD ALSO RECOGNIZE THAT SOCIAL NETWORK "FRIENDS" AND "FOLLOWERS" MAY POTENTIALLY CONSTITUTE RELATIONSHIPS THAT COULD AFFECT DETERMINATIONS IN BACKGROUND INVESTIGATIONS AND PERIODIC REINVESTIGATIONS ASSOCIATED WITH SECURITY CLEARANCES.

(6) DON PERSONNEL SHOULD BE CAREFUL ABOUT USE OF THIRD PARTY APPLICATIONS ASSOCIATED WITH SOCIAL NETWORKING SITES, SINCE SUCH APPLICATIONS OFTEN HAVE ACCESS TO A USER'S PERSONAL INFORMATION.

(7) DON PERSONNEL ARE ENCOURAGED TO LEARN ABOUT AND USE THE PRIVACY SETTINGS ON SOCIAL MEDIA SITES, IN ORDER TO LIMIT THE INFORMATION THAT MIGHT BE UNINTENTIONALLY SHARED WITH "FRIENDS" AND THE BROADER SOCIAL NETWORKING COMMUNITY.

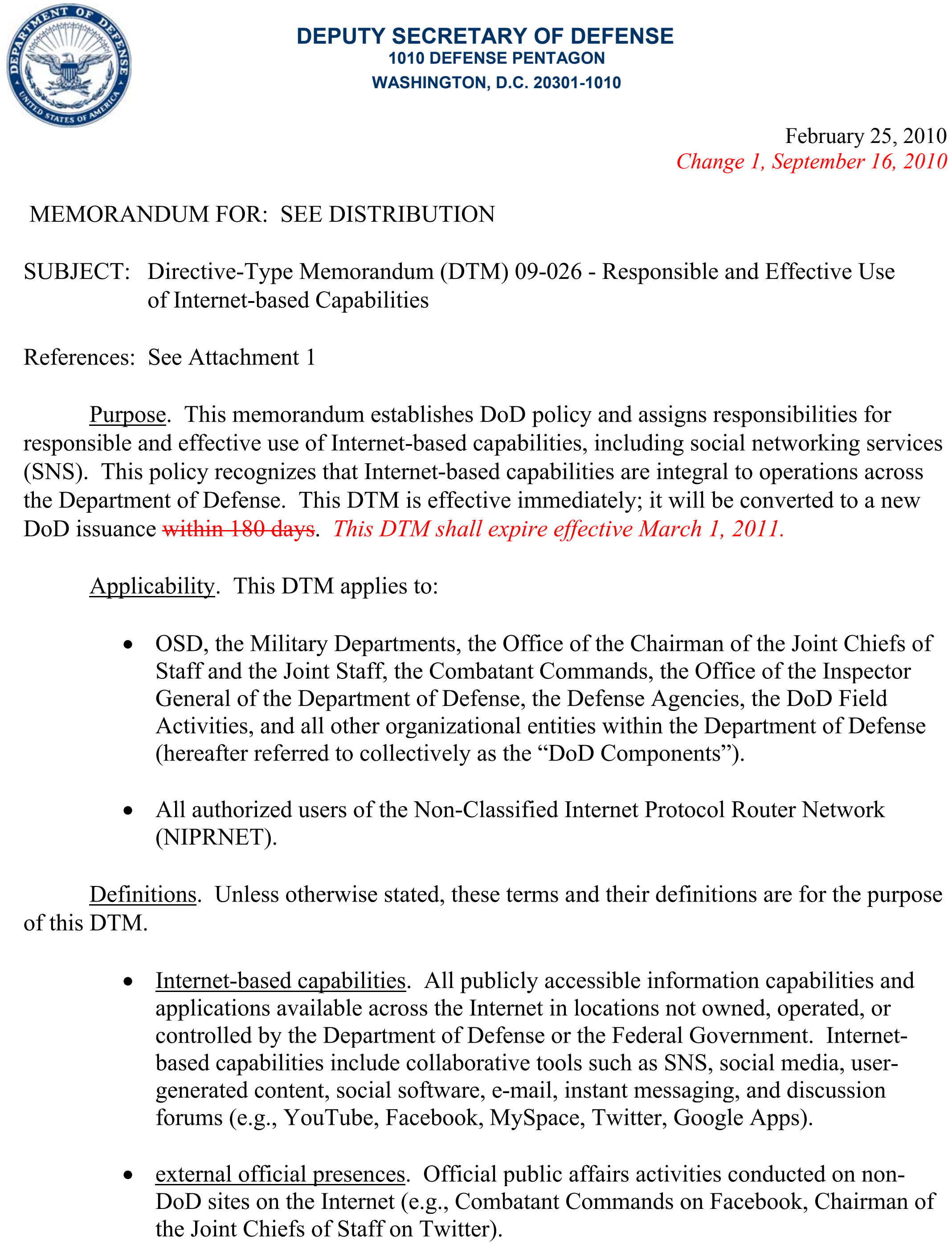
(8) DON PERSONNEL SHOULD REVIEW THEIR ACCOUNTS ON A REGULAR BASIS FOR POSSIBLE USE OR CHANGES BY UNAUTHORIZED USERS.

(9) DON PERSONNEL SHOULD REVIEW OTHER RESOURCES FOR SAFE USE OF SOCIAL NETWORKING SITES, AVAILABLE FROM

Enclosure (2)

HTTP://WWW.IOSS.GOV/SNS_SAFETY_CHECK.PDF, AND ARE REQUIRED TO TAKE MANDATORY ANNUAL INFORMATION ASSURANCE (IA) TRAINING, WHICH PROVIDES ADDITIONAL GUIDANCE, DIRECTION, AND BEST-PRACTICES ASSOCIATED WITH THE USE OF IBC.
4. THERE IS VALUE TO THE ACCESS AND USE OF IBC. FOLLOWING THE ABOVE GUIDELINES WILL HELP PREVENT THE COMPROMISE OF THE SAFETY AND SECURITY OF MISSIONS, PERSONNEL, AND NETWORKS.
5. RELEASED BY RAY MABUS, SECRETARY OF THE NAVY.//

Enclosure (3)



DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-1010

February 25, 2010
Change 1, September 16, 2010

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Directive-Type Memorandum (DTM) 09-026 - Responsible and Effective Use of Internet-based Capabilities

References: See Attachment 1

Purpose. This memorandum establishes DoD policy and assigns responsibilities for responsible and effective use of Internet-based capabilities, including social networking services (SNS). This policy recognizes that Internet-based capabilities are integral to operations across the Department of Defense. This DTM is effective immediately; it will be converted to a new DoD issuance ~~within 180 days~~. *This DTM shall expire effective March 1, 2011.*

Applicability. This DTM 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 the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the "DoD Components").

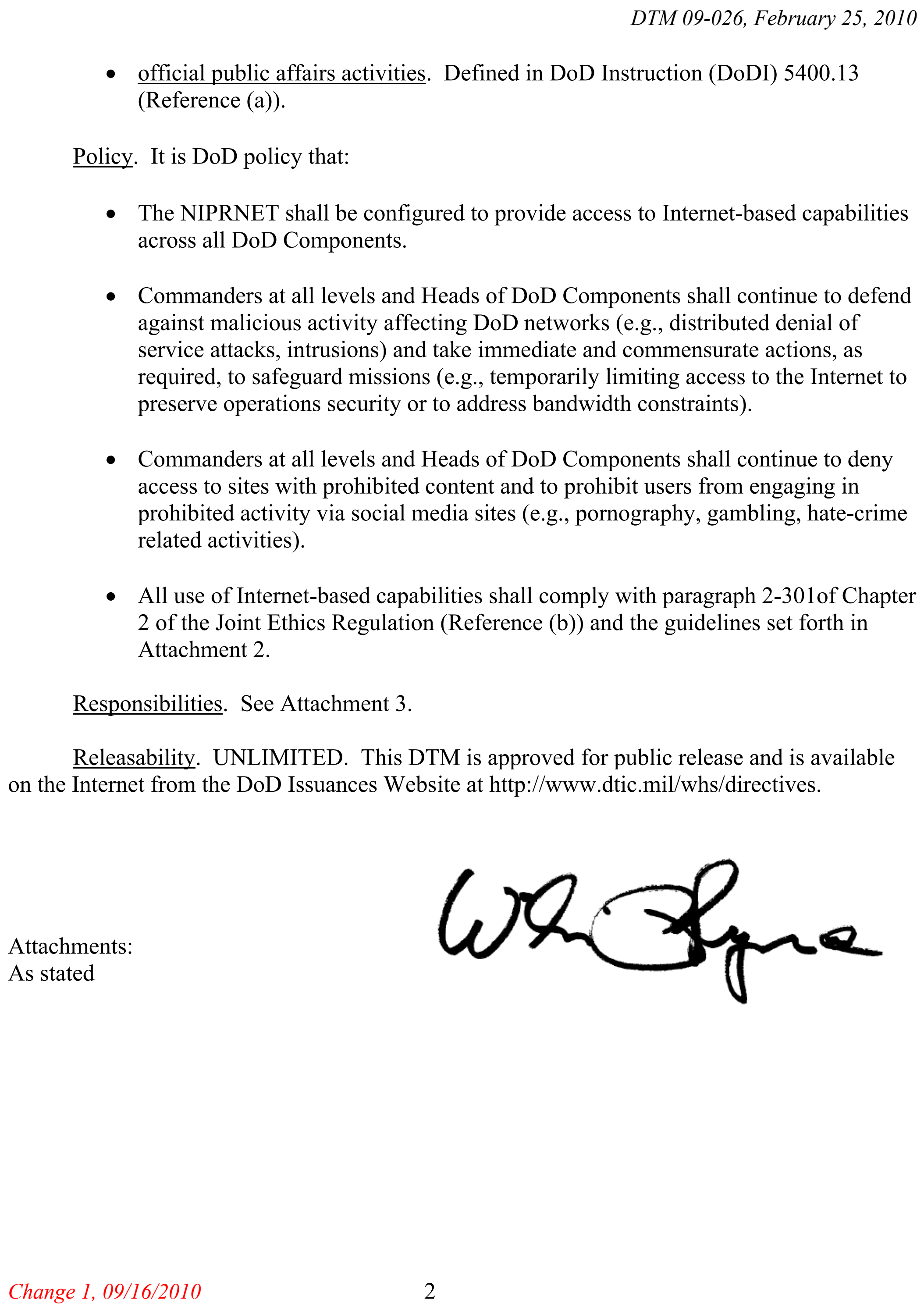
- All authorized users of the Non-Classified Internet Protocol Router Network (NIPRNET).

Definitions. Unless otherwise stated, these terms and their definitions are for the purpose of this DTM.

- Internet-based capabilities. All publicly accessible information capabilities and applications available across the Internet in locations not owned, operated, or controlled by the Department of Defense or the Federal Government. Internet-based capabilities include collaborative tools such as SNS, social media, user-generated content, social software, e-mail, instant messaging, and discussion forums (e.g., YouTube, Facebook, MySpace, Twitter, Google Apps).

- external official presences. Official public affairs activities conducted on non-DoD sites on the Internet (e.g., Combatant Commands on Facebook, Chairman of the Joint Chiefs of Staff on Twitter).

Enclosure (3)



- official public affairs activities. Defined in DoD Instruction (DoDI) 5400.13 (Reference (a)).

Policy. It is DoD policy that:

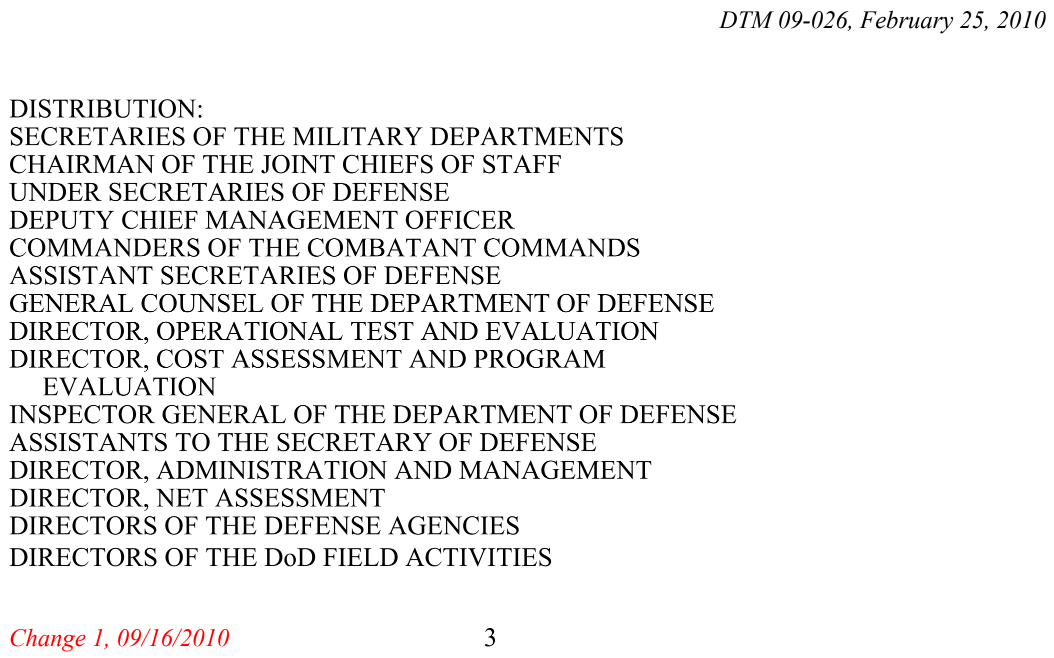
- The NIPRNET shall be configured to provide access to Internet-based capabilities across all DoD Components.
- Commanders at all levels and Heads of DoD Components shall continue to defend against malicious activity affecting DoD networks (e.g., distributed denial of service attacks, intrusions) and take immediate and commensurate actions, as required, to safeguard missions (e.g., temporarily limiting access to the Internet to preserve operations security or to address bandwidth constraints).
- Commanders at all levels and Heads of DoD Components shall continue to deny access to sites with prohibited content and to prohibit users from engaging in prohibited activity via social media sites (e.g., pornography, gambling, hate-crime related activities).
- All use of Internet-based capabilities shall comply with paragraph 2-301of Chapter 2 of the Joint Ethics Regulation (Reference (b)) and the guidelines set forth in Attachment 2.

Responsibilities. See Attachment 3.

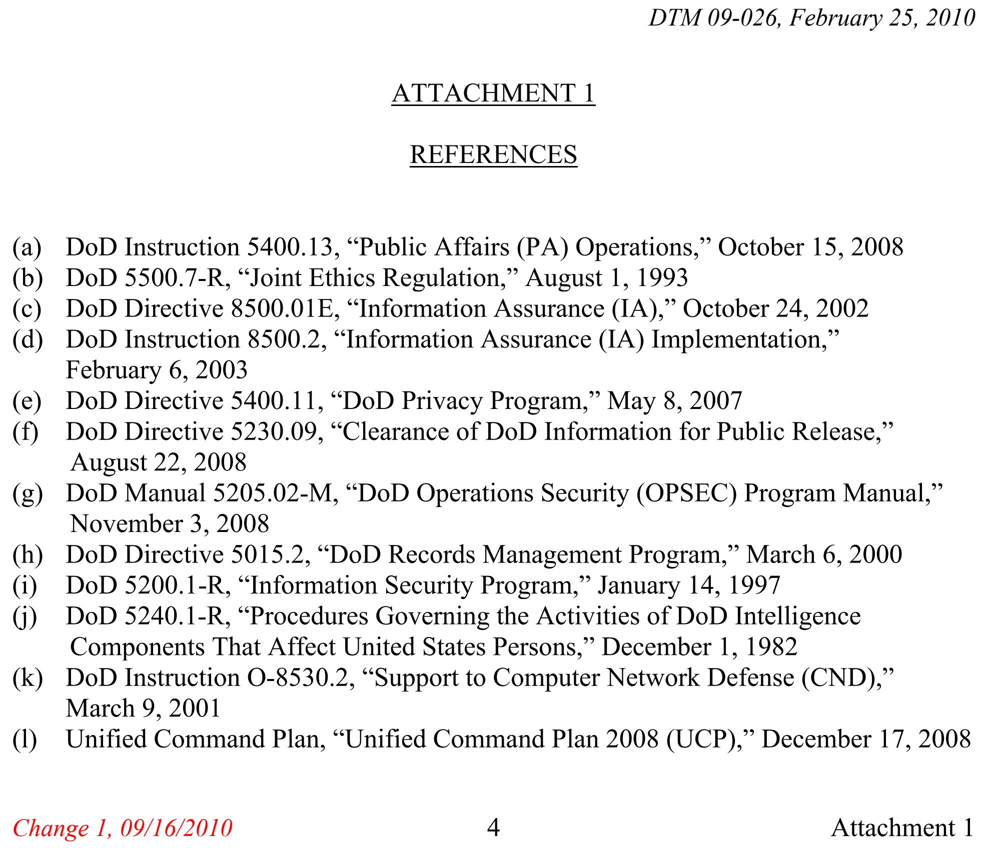
Releasability. UNLIMITED. This DTM is approved for public release and is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.

Attachments:
As stated

Enclosure (3)



DISTRIBUTION:
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DIRECTOR, COST ASSESSMENT AND PROGRAM
EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DoD FIELD ACTIVITIES

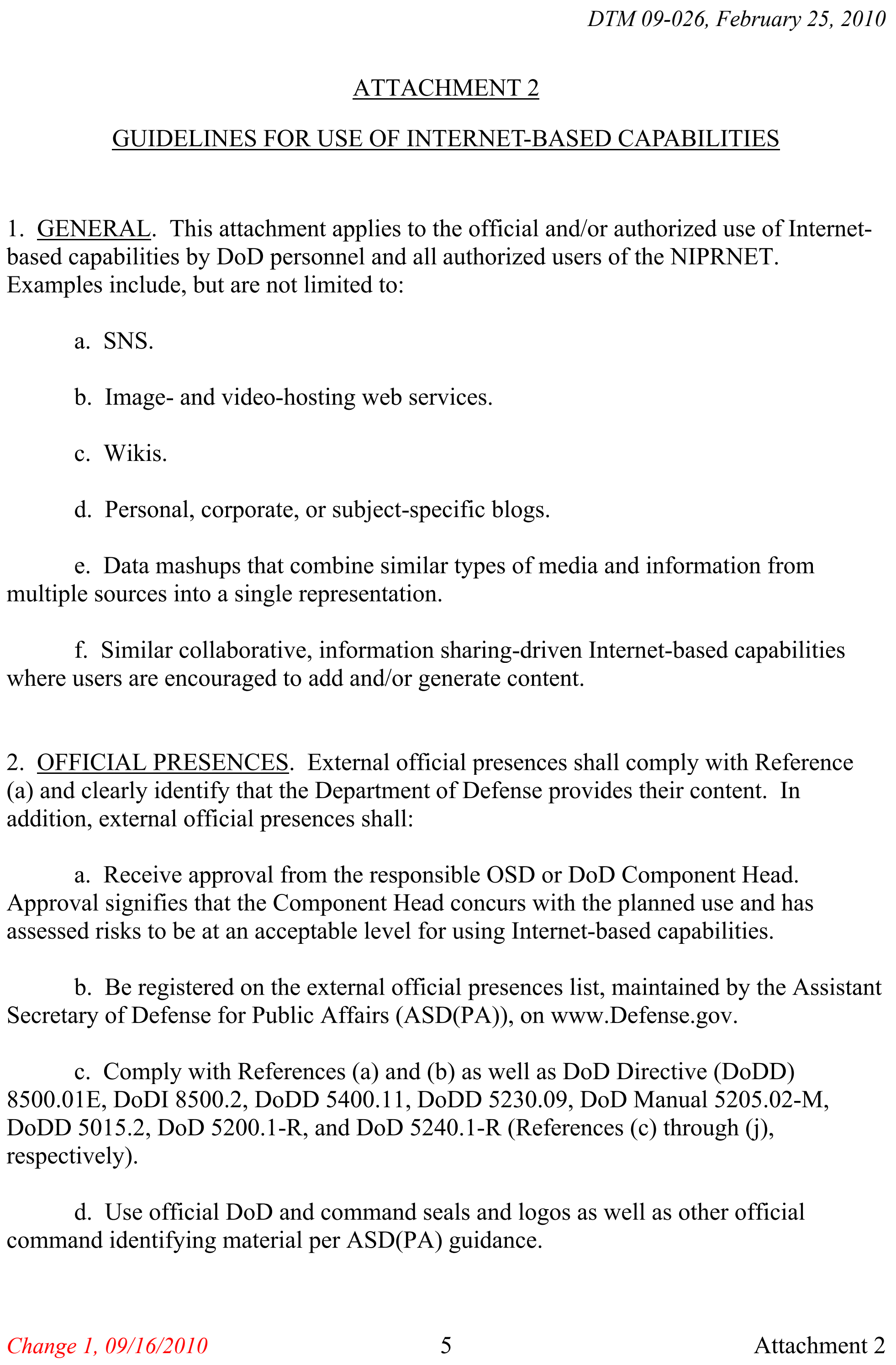


ATTACHMENT 1

REFERENCES

(a) DoD Instruction 5400.13, “Public Affairs (PA) Operations,” October 15, 2008
(b) DoD 5500.7-R, “Joint Ethics Regulation,” August 1, 1993
(c) DoD Directive 8500.01E, “Information Assurance (IA),” October 24, 2002
(d) DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003
(e) DoD Directive 5400.11, “DoD Privacy Program,” May 8, 2007
(f) DoD Directive 5230.09, “Clearance of DoD Information for Public Release,” August 22, 2008
(g) DoD Manual 5205.02-M, “DoD Operations Security (OPSEC) Program Manual,” November 3, 2008
(h) DoD Directive 5015.2, “DoD Records Management Program,” March 6, 2000
(i) DoD 5200.1-R, “Information Security Program,” January 14, 1997
(j) DoD 5240.1-R, “Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons,” December 1, 1982
(k) DoD Instruction O-8530.2, “Support to Computer Network Defense (CND),” March 9, 2001
(l) Unified Command Plan, “Unified Command Plan 2008 (UCP),” December 17, 2008

Enclosure (3)



ATTACHMENT 2

GUIDELINES FOR USE OF INTERNET-BASED CAPABILITIES

1. GENERAL. This attachment applies to the official and/or authorized use of Internet-based capabilities by DoD personnel and all authorized users of the NIPRNET. Examples include, but are not limited to:

a. SNS.

b. Image- and video-hosting web services.

c. Wikis.

d. Personal, corporate, or subject-specific blogs.

e. Data mashups that combine similar types of media and information from multiple sources into a single representation.

f. Similar collaborative, information sharing-driven Internet-based capabilities where users are encouraged to add and/or generate content.

2. OFFICIAL PRESENCES. External official presences shall comply with Reference (a) and clearly identify that the Department of Defense provides their content. In addition, external official presences shall:

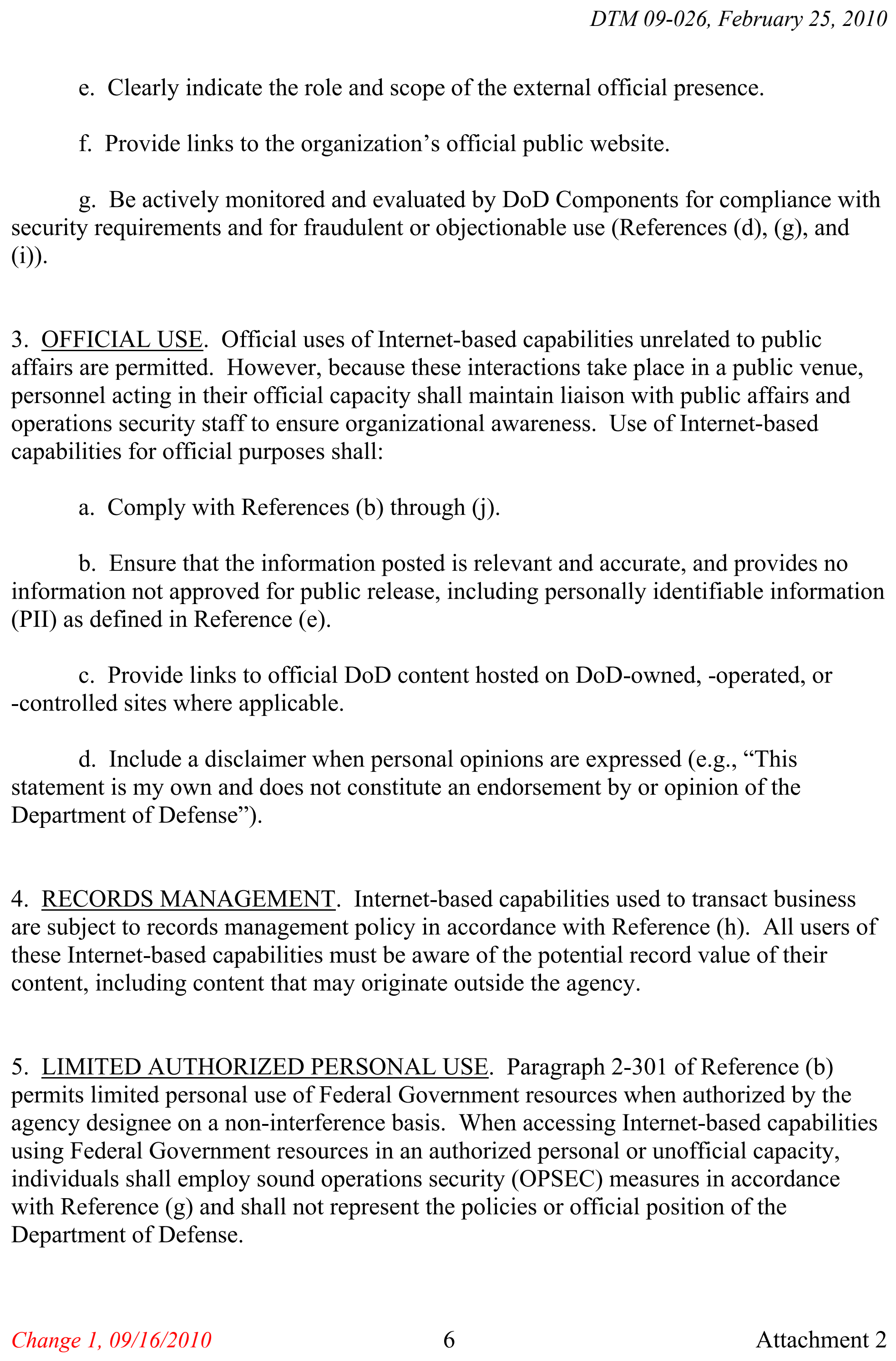
a. Receive approval from the responsible OSD or DoD Component Head. Approval signifies that the Component Head concurs with the planned use and has assessed risks to be at an acceptable level for using Internet-based capabilities.

b. Be registered on the external official presences list, maintained by the Assistant Secretary of Defense for Public Affairs (ASD(PA)), on www.Defense.gov.

c. Comply with References (a) and (b) as well as DoD Directive (DoDD) 8500.01E, DoDI 8500.2, DoDD 5400.11, DoDD 5230.09, DoD Manual 5205.02-M, DoDD 5015.2, DoD 5200.1-R, and DoD 5240.1-R (References (c) through (j), respectively).

d. Use official DoD and command seals and logos as well as other official command identifying material per ASD(PA) guidance.

Enclosure (3)



e. Clearly indicate the role and scope of the external official presence.

f. Provide links to the organization's official public website.

g. Be actively monitored and evaluated by DoD Components for compliance with security requirements and for fraudulent or objectionable use (References (d), (g), and (i)).

3. OFFICIAL USE. Official uses of Internet-based capabilities unrelated to public affairs are permitted. However, because these interactions take place in a public venue, personnel acting in their official capacity shall maintain liaison with public affairs and operations security staff to ensure organizational awareness. Use of Internet-based capabilities for official purposes shall:

a. Comply with References (b) through (j).

b. Ensure that the information posted is relevant and accurate, and provides no information not approved for public release, including personally identifiable information (PII) as defined in Reference (e).

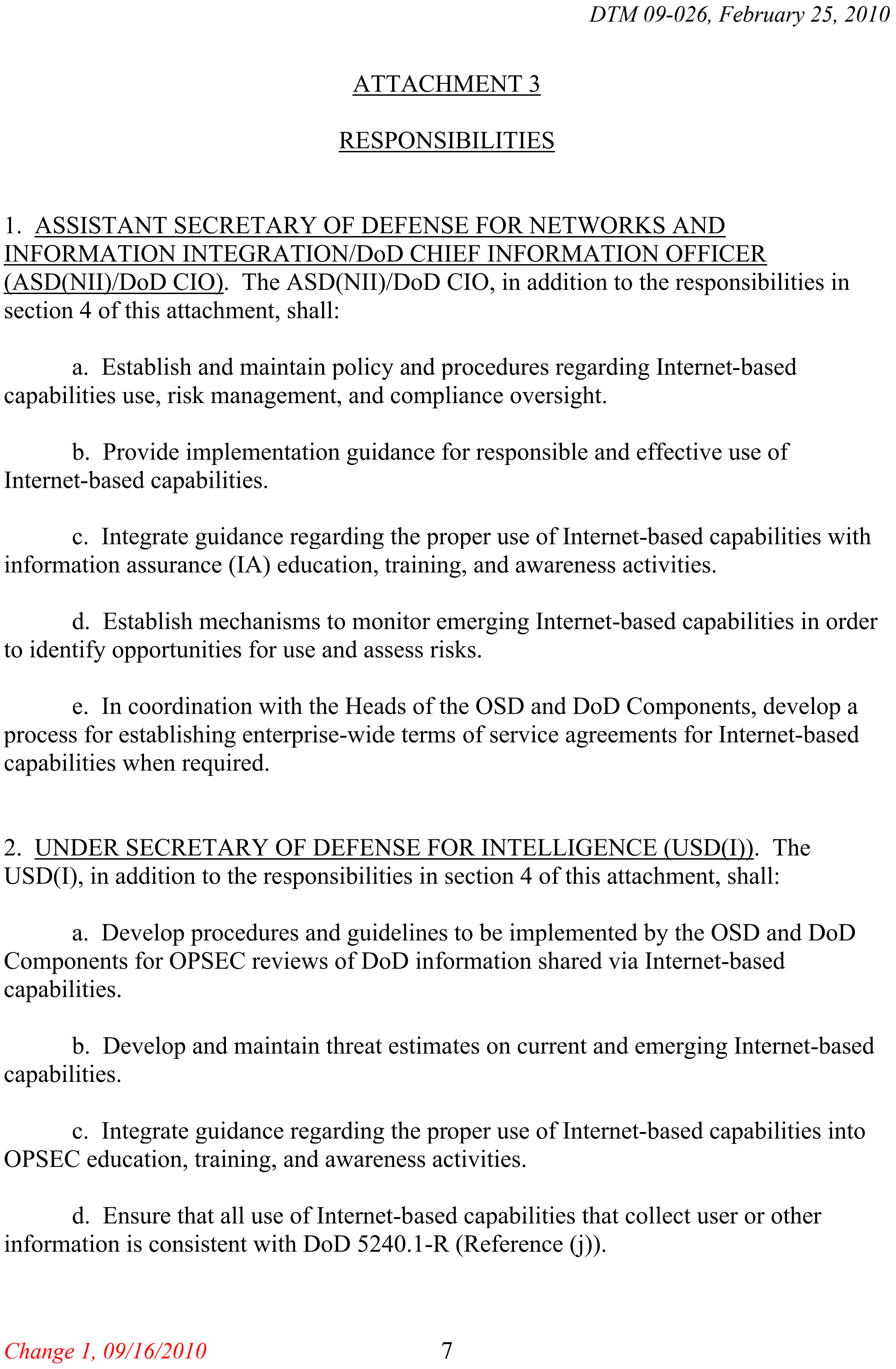
c. Provide links to official DoD content hosted on DoD-owned, -operated, or -controlled sites where applicable.

d. Include a disclaimer when personal opinions are expressed (e.g., "This statement is my own and does not constitute an endorsement by or opinion of the Department of Defense").

4. RECORDS MANAGEMENT. Internet-based capabilities used to transact business are subject to records management policy in accordance with Reference (h). All users of these Internet-based capabilities must be aware of the potential record value of their content, including content that may originate outside the agency.

5. LIMITED AUTHORIZED PERSONAL USE. Paragraph 2-301 of Reference (b) permits limited personal use of Federal Government resources when authorized by the agency designee on a non-interference basis. When accessing Internet-based capabilities using Federal Government resources in an authorized personal or unofficial capacity, individuals shall employ sound operations security (OPSEC) measures in accordance with Reference (g) and shall not represent the policies or official position of the Department of Defense.

Enclosure (3)



ATTACHMENT 3

RESPONSIBILITIES

1. ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION/DoD CHIEF INFORMATION OFFICER (ASD(NII)/DoD CIO). The ASD(NII)/DoD CIO, in addition to the responsibilities in section 4 of this attachment, shall:

a. Establish and maintain policy and procedures regarding Internet-based capabilities use, risk management, and compliance oversight.

b. Provide implementation guidance for responsible and effective use of Internet-based capabilities.

c. Integrate guidance regarding the proper use of Internet-based capabilities with information assurance (IA) education, training, and awareness activities.

d. Establish mechanisms to monitor emerging Internet-based capabilities in order to identify opportunities for use and assess risks.

e. In coordination with the Heads of the OSD and DoD Components, develop a process for establishing enterprise-wide terms of service agreements for Internet-based capabilities when required.

2. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). The USD(I), in addition to the responsibilities in section 4 of this attachment, shall:

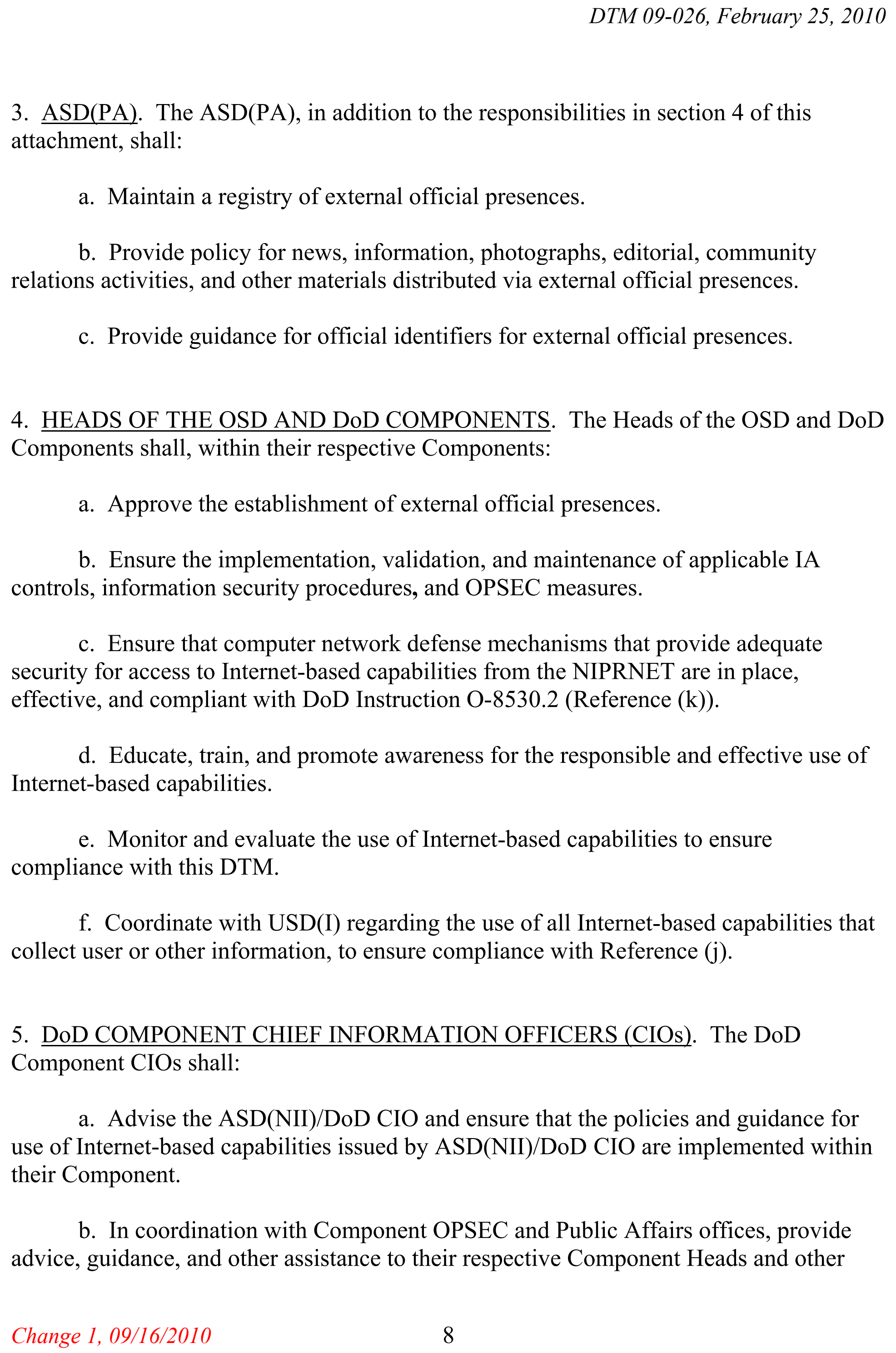
a. Develop procedures and guidelines to be implemented by the OSD and DoD Components for OPSEC reviews of DoD information shared via Internet-based capabilities.

b. Develop and maintain threat estimates on current and emerging Internet-based capabilities.

c. Integrate guidance regarding the proper use of Internet-based capabilities into OPSEC education, training, and awareness activities.

d. Ensure that all use of Internet-based capabilities that collect user or other information is consistent with DoD 5240.1-R (Reference (j)).

Enclosure (3)



3. ASD(PA). The ASD(PA), in addition to the responsibilities in section 4 of this attachment, shall:

a. Maintain a registry of external official presences.

b. Provide policy for news, information, photographs, editorial, community relations activities, and other materials distributed via external official presences.

c. Provide guidance for official identifiers for external official presences.

4. HEADS OF THE OSD AND DoD COMPONENTS. The Heads of the OSD and DoD Components shall, within their respective Components:

a. Approve the establishment of external official presences.

b. Ensure the implementation, validation, and maintenance of applicable IA controls, information security procedures, and OPSEC measures.

c. Ensure that computer network defense mechanisms that provide adequate security for access to Internet-based capabilities from the NIPRNET are in place, effective, and compliant with DoD Instruction O-8530.2 (Reference (k)).

d. Educate, train, and promote awareness for the responsible and effective use of Internet-based capabilities.

e. Monitor and evaluate the use of Internet-based capabilities to ensure compliance with this DTM.

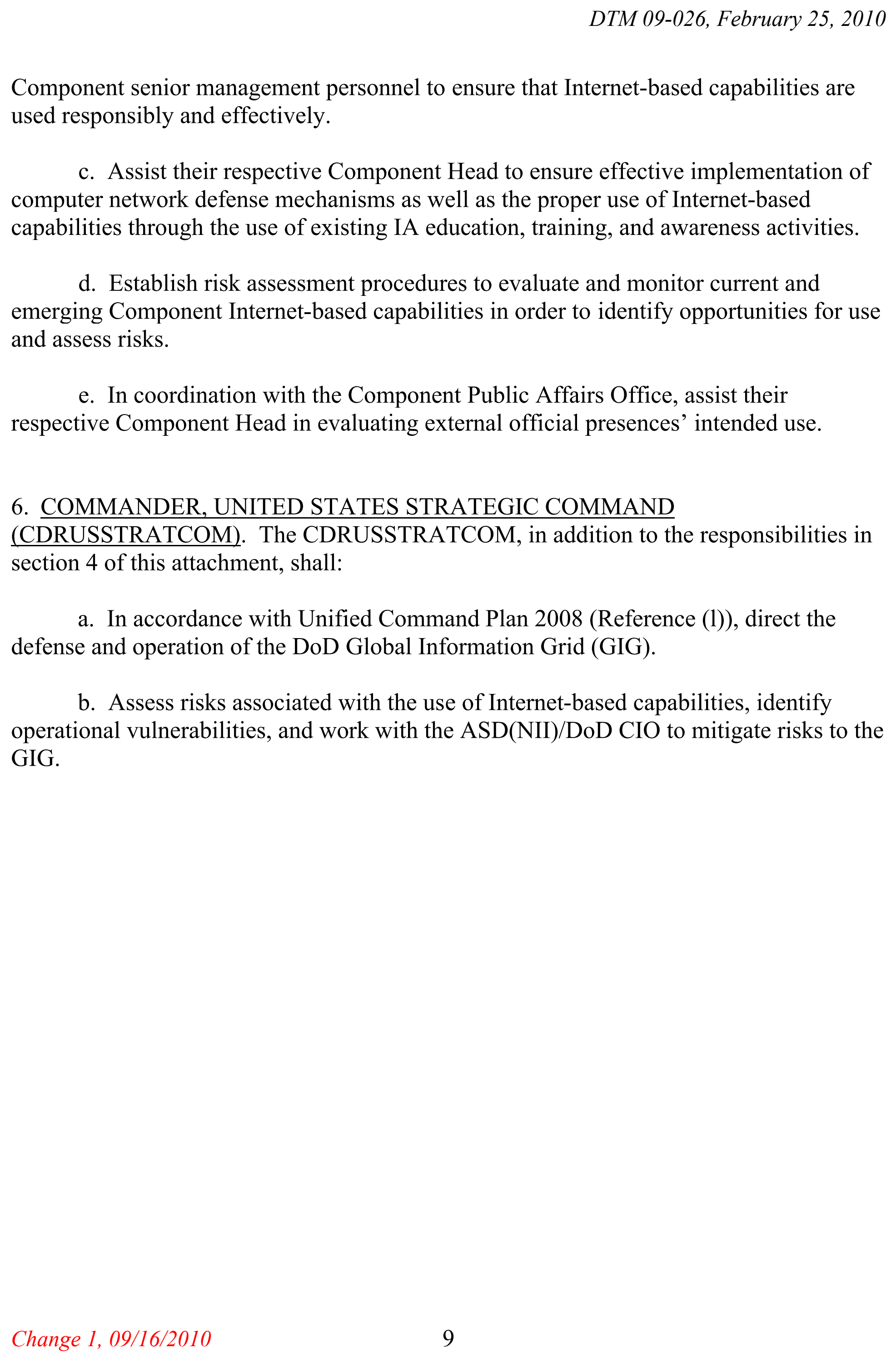
f. Coordinate with USD(I) regarding the use of all Internet-based capabilities that collect user or other information, to ensure compliance with Reference (j).

5. DoD COMPONENT CHIEF INFORMATION OFFICERS (CIOs). The DoD Component CIOs shall:

a. Advise the ASD(NII)/DoD CIO and ensure that the policies and guidance for use of Internet-based capabilities issued by ASD(NII)/DoD CIO are implemented within their Component.

b. In coordination with Component OPSEC and Public Affairs offices, provide advice, guidance, and other assistance to their respective Component Heads and other

Enclosure (3)



Component senior management personnel to ensure that Internet-based capabilities are used responsibly and effectively.

c. Assist their respective Component Head to ensure effective implementation of computer network defense mechanisms as well as the proper use of Internet-based capabilities through the use of existing IA education, training, and awareness activities.

d. Establish risk assessment procedures to evaluate and monitor current and emerging Component Internet-based capabilities in order to identify opportunities for use and assess risks.

e. In coordination with the Component Public Affairs Office, assist their respective Component Head in evaluating external official presences' intended use.

6. COMMANDER, UNITED STATES STRATEGIC COMMAND (CDRUSSTRATCOM). The CDRUSSTRATCOM, in addition to the responsibilities in section 4 of this attachment, shall:

a. In accordance with Unified Command Plan 2008 (Reference (l)), direct the defense and operation of the DoD Global Information Grid (GIG).

b. Assess risks associated with the use of Internet-based capabilities, identify operational vulnerabilities, and work with the ASD(NII)/DoD CIO to mitigate risks to the GIG.

CAPT Dave Werner
ACI for Communication
Integration & Strategy
Department of the Navy,
Office of Information
david.werner@navy.mil
(O)703-692-4728

CDR Scott McIlnay, APR
Director, Emerging Media Integration
Department of the Navy,
Office of Information
scott.mcilnay@navy.mil
(O)703-692-4718

LT Lesley Lykins
Deputy, Emerging Media Integration
Department of the Navy,
Office of Information
lesley.lykins@navy.mil
(O)703-695-6915

This guide is a creation of the Navy Office of Information