From: Shirley Steven SES DC3
Sent: Tue, 28 Aug 2012 12:24:41 -0400
To: (b)(6)
Cc: (b)(6) DC3;(b)(6) DC3;'Carey, Robert J SES DoD CIO';Hale, Richard A SES DoD CIO;(b)(6) DoD CIO';(b)(6) DoD OGC;(b)(6) DC3/DCFX
Subject: (U) INFO - DC3 IDENTITY EXPLOITED IN ON-LINE FRAUD SCHEME
Attachments: smime.p7s

FOR OSD/PA (b)(6)

BLUF: FYSA.

*DC3's logo has apparently been harvested by unidentified persons to perpetrate a fraud scheme against persons surfing web sites.

* Since 24 Aug / Fri, three men have contacted DC3 to complain they've received a pop-up placard on their computer that displays the DC3 logo & notifies the recipient they've been identified as downloading music illegally or surfing porn sites. The placard is described as occupying the entire screen & locking the computer. To unlock their computer, it instructs the recipient to obtain a VISA gift card from Wal-Mart or Walgreens & to send the card data to a designated email address. We infer one of the three callers was military affiliated (USCM, Camp LeJeune).

* We estimate there are probably considerably more than 3 recipients & would expect there is a fair probability this could get picked up by the techie &/or mainstream press as it is fairly inventive/amusing. Our working plan is to place a disclaimer on DC3's website that our GC is currently drafting.

BACKGROUND:

* At present it appears DC3 is a collateral victim in terms of reputational impact vice literal criminal offense. Our surmise is the perpetrators have infected the music &/or porn site(s) in question & are identifying their targets from among those who accessed the site(s).

Sincerely,

Steve Shirley

Steven D. Shirley, SES, DAF
Executive Director
DoD Cyber Crime Center (DC3)
(b)(6)

DoD Identity Theft
(Response to Query Only)
Jan. 2, 2004

QUESTION: What can you tell me about an alleged theft of personal identification information from military personnel?

ANSWER: The Department of Defense is actively investigating a possible case of illegal downloading and distribution of personal identification information.

The Justice Department received an anonymous communication in late November claiming that personal identifications were downloaded, to include name, date of birth and social security number, and subsequently sold to an "identity broker." A list of 155 names, which were all at one time Department of Defense personnel, was attached.

The Defense Department was first informed of the alleged theft on December 12 and began an immediate investigation. A full investigation by the Department of Defense and the FBI is underway to determine the validity of this claim. Active measures are being employed to ensure the security of beneficiary personal identification information.

Identified individuals in the anonymous claim are being contacted directly regarding this possible compromise.

Source: (b)(6) U.S. Navy Bureau of Medicine and Surgery, (b)(6)

Coordination: (b)(6) DoD IG

AO/Telephone #: (b)(6)

Approved:

Q&A:

Q – WHAT HAPPENED?

A – AN ANONYMOUS COMMUNICATION WAS RECEIVED BY THE DEPARTMENT OF HEALTH AND HUMAN SERVICES FROM SOMEONE WHO CLAIMED TO HAVE ILLEGALLY DOWNLOADED PERSONAL IDENTIFICATION INFORMATION. ATTACHED TO THAT COMMUNICATION WAS A THREE-PAGE LIST OF 155 PERSONAL IDENTIFICATIONS – IDENIFICATIONS THAT WERE LIMITED TO NAME, DATE OF BIRTH AND SOCIAL SECURITY NUMBER. ALTHOUGH WE HAVE NO INFORMATION ABOUT THE MOTIVE FOR THE CRIME, OR WHETHER THE INFORMATION WILL EVER BE ACCESSED OR MISUSED, WE WANTED TO ADVISE BENEFICIARIES OF THIS SITUATION SO THEY COULD BEGIN TAKING PRECAUTIONS TO WATCH OUT FOR ANY UNAUTHORIZED USE OF PERSONAL INFORMATION. WE ARE CONTINUING TO COOPERATE WITH THE FEDERAL GOVERNMENT AND THE INVESTIGATING AGENCIES.

Q - WHEN WAS THE DEFENSE DEPARTMENT NOTIFIED?

A – THE ANONYMOUS COMMUNICATION WAS FIRST RECEIVED IN LATE NOVEMBER BY THE DEPARTMENT OF HEALTH AND HUMAN SERVICES. THIS INCIDENT WAS REFERRED TO DEFENSE DEPARTMENT OFFICIALS ON 12 DECEMBER. INVESTIGATIONS CONTINUE BY SEVERAL AGENCIES TO DETERMINE THE VALIDITY AND EXTENT OF THIS POTENTIAL CRIME.

Q – WHERE WAS THIS INFORMATION OBTAINED?

A – THE FOCUS OF THE INVESTIGATION INVOLVES THE DETERMINATION OF MANY FACTORS, INCLUDING ORIGIN OF THE POTENTIAL BREACH. IT WOULD BE INAPPROPRIATE TO COMMENT FURTHER AS THE INVESTIGATION IS ONGOING.

Q - HOW COULD IT AFFECT DOD BENEFICIARIES?

A- IN THE WRONG HANDS, SSN'S COULD BE USED FOR IDENTITY THEFT. ACTIVE STEPS SHOULD BE TAKEN TO SAFEGUARD AGAINST IMPROPER USE OF PERSONAL INFORMATION. RECOMMENDATIONS BY THE FEDERAL TRADE COMMISSION AS NOTED IN THEIR FREE

COPY OF THE COMPREHENSIVE CONSUMER GUIDE, "ID THEFT: WHEN BAD THINGS HAPPEN TO YOUR GOOD NAME, ARE AVAILABLE AT WWW.CONSUMER.GOV/IDTHEFT OR BY CALLING1-877-IDTHEFT (1-877-438-4338).

Q - HAVE THERE BEEN ANY ACTUAL INCIDENTS OF IDENTITY THEFT FROM THIS EVENT?

A – AN INVESTIGATION IS UNDERWAY AT THIS TIME. WE HAVE NO REPORTS OF ANY CASES OF IDENTITY THEFT IN THE CASES OF THE 155 PEOPLE NOTED IN THE ANONYMOUS COMMUNICATION.

Q – WERE THERE MORE THAN 155 PEOPLE INVOLVED? HOW DO WE KNOW MORE PEOPLE WEREN'T AFFECTED?

A – AN INVESTIGATION IS ONGOING, AND IT WOULD BE INAPPROPRIATE TO SPECULATE ABOUT WHETHER OTHER INDIVIDUALS HAVE BEEN AFFECTED.

Q - HOW ARE THE AFFECTED INDIVIDUALS BEING NOTIFIED?

A - LETTERS WERE MAILED TO ALL POTENTIALLY AFFECTED BENEFICIARIES. THE LETTERS INFORMED THEM ABOUT THE INCIDENT, THE POTENTIAL FOR IDENTITY THEFT, AND STEPS THEY COULD TAKE TO HELP PROTECT AGAINST THE UNAUTHORIZED USE OF THEIR INFORMATION.

Q – WOULD THIS TYPE OF PERSONAL INFORMATION BE ENOUGH FOR SOMEONE TO SUCCESSFULLY TAKE PART IN IDENTITY THEFT?

A – PERSONAL INFORMATION PRIVACY AND PROTECTION OF PERSONAL RECORDS AND INFORMATION ARE AT THE FOREFRONT OF DOD'S PRIORITIES. WHAT CRIMINAL PURPOSE ONE MIGHT HAVE IN ILLEGALLY ACCESSING THIS INFORMATION OR HOW SUCCESSFULLY THIS INFORMATION COULD BE IN IDENTITY THEFT CRIMES IS UNKNOWN.

Q - FROM WHICH DATABASE DID THESE NAMES COME?

A - AN INVESTIGATION IS ONGOING TO DETERMINE IF THIS POTENTIAL UNAUTHORIZED ACCESS OF PERSONAL IDENTIFICATIONS

ACTUALLY OCCURRED. IT IS DEFENSE DEPARTMENT POLICY TO ENSURE THAT PERSONAL RECORDS AND INFORMATION ARE SAFE AND PROTECTED FROM ANY KIND OF OUTSIDE THREAT.

Q – HOW EASY IS IT FOR HACKERS TO ACCESS INFORMATION LIKE THIS?

A – AN INVESTIGATION IS ONGOING TO DETERMINE IF THIS POTENTIAL UNAUTHORIZED ACCESS OF PERSONAL IDENTIFICATIONS ACTUALLY OCCURRED. IT IS DEFENSE DEPARTMENT POLICY TO ENSURE THAT PERSONAL RECORDS AND INFORMATION ARE SAFE AND PROTECTED FROM ANY KIND OF OUTSIDE THREAT.

Q – COULD THIS HAVE BEEN AN INSIDE JOB? WHO DID THIS?

A – IT WOULD BE INAPPROPRIATE TO COMMENT ON ANY DETAILS OF THE INVESTIGATION AS IT IS ONGOING.

CYBERSECURITY: 'ROBIN SAGE' FAKE PROFILE

CNN requested to interview someone on July 20 for DoD's response to the "Robin Sage" fake profile used to collect personal information from government people Facebook. CNN read about it from Wash Times Shaun Waterman's July 19 article,"Fictitious Femme Fatale Fooled Cybersecurity Intel, defense specialists fell for ruse in test." Wash Times quotes Mr Dave Wennergren Deputy Director NII/DoD-CIO, from last week's RTQ. Wash Times discovered the story from the DarkReading.Com's version of the story titled, "'Robin Sage' Profile Duped Military Intelligence, IT Security Pros."

Issue: Robin Sage does not exist. Her profile was a ruse, set up by security consultant Thomas Ryan (Co-Founder & Managing Partner Provide Security, LLC.) as part of an effort to expose weaknesses in the nation's defense and intelligence communities. Mr Ryan created this fake Facebook ID as a social networking 28-day experiment to reveal flaws in government cybersecurity.

The Pentagon Channel is also interested in doing a related story to remind our people of OPSEC.

Issue is Behavior, Not the Tool

- It's part of a bigger process to help ensure our folks are well trained on responsible use of the Internet (at work and home).
- We should address the behavior not abandon the tool.
- Similarly in the past, when long-distance phone abuse resulted in appropriate action against an individual, we didn't abandon the use of telephones.

Risk

- All access to the Internet (not just SNS) involves risk; even accessing web sites and the use of email involves risk.
- Risks should not prevent the Department from utilizing emerging technologies to accomplish its mission.

DoD DTM 09-026 (February 25, 2010) on Social Networking Services

- All access to SNS was not blocked prior to the DTM, military folks had access to some of these capabilities at work and at home.

- The point of the memo was to ensure we allowed our people to have the benefit of these capabilities, while ensuring we use them responsibly, effectively and appropriately.

More questions anticipated: Wasn't DoD safer when SNS was banned? What if anything is your office doing to update this policy in the light of the weaknesses revealed by "Robin Sage"? What will happen to the soldier who appears to have inadvertently disclosed information about troop locations? This is a breach of OPSEC, isn't it? Will he be disciplined/counseled/retrained etc?

Appendix – Snapshots of First Three Accounts

Fake Peter Cook @FakePeterCook · Sep 23

I don't have any comment about the reports of Syrian rebels defecting to al Qaeda because nobody tells me anything in this place.

1 1

Fake Peter Cook @FakePeterCook · Sep 23

That's all for now! I have a meeting I need to be very early to, but please Tweet me your questions and I'll get to them ASAP.

1

Fake Peter Cook @FakePeterCook · Sep 23

Q: Peter, do you like movies about gladiators? --Clarence (Los Angeles, CA)
A: I'm not sure. Gladiator was pretty cool. Why do you ask?

1

Fake Peter Cook @FakePeterCook · Sep 23

Q: Why'd it take you so long to start giving briefings?--Dawn (Hope, AR)
A: The art of talking w/o saying anything takes time to learn.

1

Fake Peter Cook @FakePeterCook · Sep 23

Q: What is your middle name? --Gregory (Des Moines, IA)
A: Cornelius. Well, I wish it was.

Fake Ashton Carter @lameducksecdef · Sep 22
AND @PentagonPresSec showed up late to his own presser and then demanded to leave early. That is the kind of asshole thing I would do.

Fake Ashton Carter @lameducksecdef · Sep 22
I love @PentagonPresSec! He looks pretty and never address any issue substantively...just like me.

Fake Ashton Carter @lameducksecdef · Sep 22
I'd like to take this opportunity to single out the finest member of the Pentagon Press Corps. @ACapaccio, you're a king among men. Like me.

Fake Ashton Carter @lameducksecdef · Sep 21
I would say I'm an absentee Cabinet secretary but can you be MIA if no one cares whether you are there or not?

Fake Ashton Carter @lameducksecdef · Sep 21
Hey gang!!! Who is ready to LEEEEAAANNN AWWAAAAY from dealing with Syria? See you the Fecebook event!

Fake Ashton Carter @lameducksecdef · Sep 18
Fake Ash is starting an "awkward hug" count by the esteemed SECDEF. Yesterday, 3, at heroes celebration; 1 today at CNO ceremony

Pinned Tweet

Ashley J. Carter @SecyOfDarkness · Sep 2

(Editor's note: Not sure how or why people are making this mistake, but this is NOT Ash Carter's real Twitter account. That would be weird.)

1

Ashley J. Carter @SecyOfDarkness · 18h

TWEEPS HAHAHAHAHA

Ashley J. Carter @SecyOfDarkness · 18h

IT's my birthday and Stephanie gave me too much wine! How's it GOING MY TWEEPS?

Ashley J. Carter @SecyOfDarkness · 23h

I'm starting to get the feeling that @GenDunford isn't much of a hugger. Maybe it's just me.

FACT SHEET
POTENTIAL CYBER-ATTACK/IDENTITY THEFT

PURPOSE

- To provide information on a potential case of criminal identity theft through access of a Defense Department database, provide the actions underway to address this matter, and offer steps that individuals whose personal information may have been compromised should take to protect misuse of this information.

FACTS

- In November, the US Department of Health and Human Services received an anonymous communication that claimed thousands of personal identifications were downloaded from a server located at the Naval Medical Information Management Center, to include name, date of birth, and social security number. The letter included a list of 155 names as "proof."

- After a series of communications between HHS and the Department of Justice, the Defense Department was first informed on December 12th and began an immediate investigation. A full investigation by the Department of Defense and the FBI is underway to determine the validity of this claim.

- The Navy has verified that all 155 names are confirmed as Department of Defense retired military members representing all Services, to include the Coast Guard.

ACTIONS UNDERWAY

- The Naval Criminal Investigative Services has opened a criminal investigation, assisted by the Defense Criminal Investigative Service and the Federal Bureau of Investigation.

- A full-scale technical security investigation has also commenced, led by the Navy, and assisted by TRICARE Management Activity Information Assurance personnel.

- A physical security assessment has been conducted. There is no evidence of a break-in.

- Telephone calls to all 155 individuals identified in the letter, informing them of the allegation began on December 30th. This outreach has been followed by a personal letter mailed today, January 2, 2004 to all 155 persons.

- A hotline has also been established (1-800-227-7921) for persons who need additional information or have questions.

Identity Theft Information Sheet

Because your personal information may have been misused to commit identity theft, take the following steps and keep a record of all your actions.

• FIRST, contact the fraud departments of each of the three major credit bureaus. Request that a "fraud alert" be placed in your file. Also ask them to place a statement that asks creditors to call you before opening any new accounts or changing any existing accounts. The credit bureau fraud departments are listed below. Their normal operating hours are Monday – Friday, 8:30 a.m. to 4:30 p.m.

Equifax Credit Information Services
www.equifax.com

Consumer Fraud Division
P.O. Box 105069
Atlanta, GA 30348

Phone: 800-525-6285

Experian
www.experian.com

Experian's National Consumer Assistance
P.O. Box 1017
Allen, TX 75013

Phone: 888-397-3742

TransUnion
www.transunion.com

Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834

Phone: 800-680-7289
Fax: 714-447-6034

• SECOND, after reviewing your credit reports for any irregularities, should you find that someone has created unauthorized accounts in your name, you should close or suspend any accounts you know or believe have been tampered with or opened fraudulently.

•THIRD, if your accounts have been misused or opened fraudulently, file a police report with your local police or the police in the community where the identity theft took place and you should contact the Defense Criminal Investigative Service at 703- 604- 8440. Obtain a copy of the local police report number for future reference.

•FOURTH, if your accounts have been misused or opened fraudulently, notify all banks, credit unions, creditors, and utilities that have extended you credit or otherwise have opened an account in your name. Be prepared to provide these companies with a copy of the police report. Change all PIN numbers and passwords.

•FIFTH, file a complaint with the FTC by contacting the FTC's Identity Theft Hotline. Their toll-free telephone is 1-877-IDTHEFT (438-4338) or by direct dial to: 202-326-2502. You may also write to them at:

Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

You can also access their web site at: www.consumer.gov/idtheft. A free comprehensive consumer guide to help you guard against and recover from identity theft is available on this website. It is entitled *ID Theft: When Bad Things Happen to Your Good Name.*

SIXTH, on an annual basis you should obtain a copy of your credit report from all three credit bureaus and review them for any unauthorized accounts or unauthorized activity.

Depending on the nature of the fraud, you may consider contacting the following agencies:

The Social Security Administration is an excellent source for information about Social Security Number theft or misuse. If you suspect that your SSN has been misused then you should call the SSA Fraud Hotline at **1-800-269-0271** or www.ssa.gov/oig/guidelin.htm. The SSA general website http://www.ssa.gov has several publications which may be useful including: Social Security: Your Number and Card (SSA Pub. No. 05-10002); and When Someone Misuses Your Number (SSA Pub. No. 05-10064). You should also periodically contact the SSA at 1-800-772-1213 to verify the accuracy of the earnings reported on your SSN, and may request a copy of your Social Security Statement.

The Internet Fraud Complaint Center (IFCC) should be contacted for any fraud or theft involving your Internet accounts. They can be contacted at: http://www.ifccfbi.gov.

For fraud involving your mail file a complaint with the U.S. Postal Service at http://www.usps.com/postalinspectors/fraud/MailFraudComplaint.htm or by telephone at (312) 669-5663.

If the fraud crosses state lines, then contact the Federal Bureau of Investigation (FBI) at http://www.fbi.gov/contact/fo/territory.htm [Consult your phone directory for office nearest you.]

If counterfeit checks are involved, contact the U. S. Secret Service at http://www.ustreas.gov/usss/ or by telephone at (202) 406-9042.

If the fraud affects your taxes, contact the Internal Revenue Service at http://www.irs.gov or by telephone at 1-800 829 0433.

V. RECOMMENDED QUESTIONS AND ANSWERS

TO BE USED IN RESPONSE TO MEDIA QUERY AND TALKING POINTS WHEN COMMUNICATING WITH BENEFICIARIES.

STATEMENT:

THE DEPARTMENT OF DEFENSE IS ACTIVELY INVESTIGATING A POSSIBLE CASE OF ILLEGAL DOWNLOADING AND DISTRIBUTION OF PERSONAL IDENTIFICATION INFORMATION.

THE JUSTICE DEPARTMENT RECEIVED AN ANONYMOUS COMMUNICATION CLAIMING THAT PERSONAL IDENTIFICATIONS WERE DOWNLOADED, TO INCLUDE NAME, DATE OF BIRTH AND SOCIAL SECURITY NUMBER, AND SUBSEQUENTLY SOLD TO AN "IDENTITY BROKER." A LIST OF 155 NAMES, WHO WERE ALL AT ONE TIME DEPARTMENT OF DEFENSE BENEFICIARIES, WAS ATTACHED AS PROOF.

A FULL INVESTIGATION BY THE DEPARTMENT OF DEFENSE AND THE FBI IS UNDERWAY TO DETERMINE THE VALIDITY OF THIS CLAIM, AND ACTIVE MEASURES ARE BEING EMPLOYED TO ENSURE THE CONTINUED SECURITY OF BENEFICIARY PERSONAL IDENTIFICATION INFORMATION. IDENTIFIED INDIVIDUALS IN THE ANONYMOUS CLAIM ARE BEING CONTACTED DIRECTLY REGARDING THIS POSSIBLE COMPROMISE.

Q – WHAT HAPPENED?

A – AN ANONYMOUS COMMUNICATION WAS RECEIVED BY THE JUSTICE DEPARTMENT FROM SOMEONE WHO CLAIMED TO HAVE ILLEGALLY DOWNLOADED PERSONAL IDENTIFICATION INFORMATION. ATTACHED TO THAT COMMUNICATION WAS A THREE-PAGE LIST OF 155 PERSONAL IDENTIFICATIONS – IDENIFICATIONS THAT WERE LIMITED TO NAME, DATE OF BIRTH AND SOCIAL SECURITY NUMBER. ALTHOUGH WE HAVE NO INFORMATION ABOUT THE MOTIVE FOR THE CRIME, OR WHETHER THE INFORMATION WILL EVER BE ACCESSED OR MISUSED, WE WANTED TO ADVISE BENEFICIARIES OF THIS SITUATION SO THEY COULD BEGIN TAKING PRECAUTIONS TO WATCH OUT FOR ANY UNAUTHORIZED USE OF PERSONAL INFORMATION. WE ARE CONTINUING TO COOPERATE WITH THE FEDERAL GOVERNMENT AND THE INVESTIGATING AGENCIES.

Q - WHEN WAS THE DEFENSE DEPARTMENT NOTIFIED?

A – THE ANONYMOUS COMMUNICATION WAS FIRST RECEIVED IN LATE NOVEMBER BY THE DEPARTMENT OF JUSTICE. THIS INCIDENT WAS REFERRED TO DEFENSE DEPARTMENT OFFICIALS ON 12 DECEMBER. IMMEDITE INVESTIGATIONS BEGAN AND CONTINUE BY SEVERAL AGENCIES TO DETERMINE THE VALIDITY AND EXTENT OF THIS POTENTIAL CRIME.

Q – WHERE WAS THIS INFORMATION OBTAINED?

A – THE FOCUS OF THE INVESTIGATION INVOLVES THE DETERMINATION OF MANY FACTORS, INCLUDING ORIGIN OF THE POTENTIAL BREACH. IT WOULD BE INAPPROPRIATE TO COMMENT FURTHER AS THE INVESTIGATION IS ONGOING.

Q - HOW COULD IT AFFECT DOD BENEFICIARIES?

A- IN THE WRONG HANDS, SSN'S COULD BE USED FOR IDENTITY THEFT. ACTIVE STEPS SHOULD BE TAKEN TO SAFEGUARD AGAINST IMPROPER USE OF PERSONAL INFORMATION. RECOMMENDATIONS BY THE FEDERAL TRADE COMMISSION AS NOTED IN THEIR FREE COPY OF THE COMPREHENSIVE CONSUMER GUIDE, "ID THEFT: WHEN BAD THINGS HAPPEN TO YOUR GOOD NAME, ARE AVAILABLE AT WWW.CONSUMER.GOV/IDTHEFT OR BY CALLING1-877-IDTHEFT (1-877-438-4338).

Q - HAVE THERE BEEN ANY ACTUAL INCIDENTS OF IDENTITY THEFT FROM THIS EVENT?

A – AN INVESTIGATION IS UNDERWAY AT THIS TIME. WE HAVE NO REPORTS OF ANY CASES OF IDENTITY THEFT IN THE CASES OF THE 155 PEOPLE NOTED IN THE ANONYMOUS COMMUNICATION.

Q – WERE THERE MORE THAN 155 PEOPLE INVOLVED? HOW DO WE KNOW MORE PEOPLE WEREN'T AFFECTED?

A – WE HAVE NO INFORMATION TO SUGGEST THAT ANYONE ELSE WAS AFFECTED BY THIS POTENTIAL COMPROMISE. AN INVESTIGATION IS ONGOING, AND IT WOULD BE INAPPROPRIATE TO SPECULATE ABOUT WHETHER OTHER INDIVIDUALS HAVE BEEN AFFECTED.

Q - HOW ARE THE AFFECTED INDIVIDUALS BEING NOTIFIED?

A - LETTERS WERE MAILED TO ALL POTENTIALLY AFFECTED BENEFICIARIES. THE LETTERS INFORMED THEM ABOUT THE INCIDENT, THE POTENTIAL FOR IDENTITY THEFT, AND STEPS THEY COULD TAKE TO HELP PROTECT AGAINST THE UNAUTHORIZED USE OF THEIR INFORMATION.

Q – WOULD THIS TYPE OF PERSONAL INFORMATION BE ENOUGH FOR SOMEONE TO SUCCESSFULLY TAKE PART IN IDENTITY THEFT?

A – PERSONAL INFORMATION PRIVACY AND PROTECTION OF PERSONAL RECORDS AND INFORMATION ARE AT THE FOREFRONT OF DOD'S PRIORITIES. WHAT CRIMINAL PURPOSE ONE MIGHT HAVE IN ILLEGALLY ACCESSING THIS INFORMATION OR HOW SUCCESSFULLY THIS INFORMATION COULD BE IN IDENTITY THEFT CRIMES IS UNKNOWN.

Q – HOW EASY IS IT FOR HACKERS TO ACCESS INFORMATION LIKE THIS?

A – AN INVESTIGATION IS ONGOING TO DETERMINE IF THIS POTENTIAL UNAUTHORIZED ACCESS OF PERSONAL IDENTIFICATIONS ACTUALLY OCCURRED. IT IS DEFENSE DEPARTMENT POLICY TO ENSURE THAT PERSONAL RECORDS AND INFORMATION ARE SAFE AND PROTECTED FROM ANY KIND OF OUTSIDE THREAT.

Q – COULD THIS HAVE BEEN AN INSIDE JOB? WHO DID THIS?

A – IT WOULD BE INAPPROPRIATE TO COMMENT ON ANY DETAILS OF THE INVESTIGATION AS IT IS ONGOING.

RTQ Statement—Identity Theft

"The Department of Defense takes the issue of identity theft very seriously and makes every effort to protect the personal information of servicemembers. Further, we encourage servicemembers to safeguard personal information, especially social security numbers (SSN)."

"The Department has used SSNs as a means to identify servicemembers since the 1960s. The decision to use the SSN was made in order to avoid confusion by not using two separate personal identifiers within financial and personnel data systems. This is especially important when linking to external systems, such as the Veterans Administration, IRS, the Social Security Administration, and state tax authorities."

"While it does not appear that DoD policy has contributed to the misuse of personal information, we nevertheless have and will continue to take the strongest measures practical to protect our servicemembers and their families."

DoD IDENTITY THEFT PROTECTION MESSAGES

Attention current or former SC taxpayers:

Recently, the South Carolina Dept. of Revenue experienced a criminal cyber intrusion in which Personally Identifiable Information (PII) may have been compromised for anyone who filed a S.C. tax return since 1998. DoD personnel and their dependents who are current or former S.C. taxpayers are urged to do the following by Jan. 31, 2013:

- Visit **www.ProtectMyID.com/SCDOR** (code **SCDOR123**) or call **1-866-578-5422** (M-F 9am-9pm EST; S-S 11am-8pm EST) to enroll for one year of identity theft protection.

  Last US address must be used. Spouses must enroll themselves. Parents will be notified when children may enroll.

All services are free of charge. For more information, visit www.consumer.sc.gov.

Less than 300 Characters

Attention current/former SC taxpayers:

The South Carolina Dept. of Revenue recently experienced a criminal cyber intrusion in which Personally Identifiable Information (PII) may have been compromised. Anyone who paid SC taxes since 1998 is encouraged to acquire identity theft protection by Jan. 31, 2013.

- Visit **www.ProtectMyID.com/SCDOR** (code **SCDOR123**) or call **1-866-578-5422** to enroll for one year, free of charge.

Less than 190 Characters

Current/former SC taxpayers are encouraged to acquire ID theft protection:

- Visit **www.ProtectMyID.com/SCDOR** (code **SCDOR123**) or call **1-866-578-5422** to enroll for one year, free of charge.

DoD IDENTITY THEFT PROTECTION MESSAGES

Attention current or former SC taxpayers:

Recently, the South Carolina Dept. of Revenue experienced a cyber intrusion in which Personally Identifiable Information (PII) may have been compromised for anyone who filed a S.C. tax return since 1998. DoD personnel and their dependents who are current or former S.C. taxpayers are urged to do the following by Jan. 31, 2013:

- Visit **www.ProtectMyID.com/SCDOR** (code **SCDOR123**) or call **1-866-578-5422** (M-F 9am-9pm EST; S-S 11am-8pm EST) to enroll for one year of identity theft protection.

  Last US address must be used. Spouses must enroll themselves. Parents will be notified when children may enroll.

All services are free of charge. For more information, visit www.consumer.sc.gov.

Less than 300 Characters

Attention current/former SC taxpayers:

The South Carolina Dept. of Revenue recently experienced a cyber intrusion in which Personally Identifiable Information (PII) may have been compromised. Anyone who paid SC taxes since 1998 is encouraged to acquire identity theft protection by Jan. 31, 2013.

- Visit **www.ProtectMyID.com/SCDOR** (code **SCDOR123**) or call **1-866-578-5422** to enroll for one year, free of charge.

Less than 190 Characters

Current/former SC taxpayers are encouraged to acquire ID theft protection:

- Visit **www.ProtectMyID.com/SCDOR** (code **SCDOR123**) or call **1-866-578-5422** to enroll for one year, free of charge.

IDENTITY THEFT PROTECTION TWITTER/FACEBOOK MESSAGES FOR AFFECTED DOD SOUTH CAROLINA TAXPAYERS:

To: (b)(6) Department of Defense

From: Office of the Governor, State of South Carolina

Subject: ID Theft Protection Messages for Use by DOD for SC Taxpayers

Date: November 8, 2012

Less than 625 Characters
Attention current or former SC taxpayers: Recently, the SC Dept. of Revenue was breached in a criminal cyber attack. Anyone who has paid SC taxes since 1998 may have had their personal information compromised. By 31JAN13, current or former SC taxpayers should: • Visit **www.ProtectMyID.com/SCDOR** (code **SCDOR123**) or call **1-866-578-5422** (M-F 9am-9pm EST; S-S 11am-8pm EST) to enroll for one year of identity theft protection. Last US address must be used. Spouses must enroll themselves. Parents will be notified when children may enroll. All services are free of charge. For more information, visit www.consumer.sc.gov.

Less than 300 Characters
Attention current/former SC taxpayers: The SC Dept. of Revenue was breached in a cyberattack. Anyone who paid SC taxes since 1998 is encouraged to acquire ID theft protection by 31JAN13: • Visit **www.ProtectMyID.com/SCDOR** (code **SCDOR123**) or call **1-866-578-5422** to enroll for one year, free of charge.

Less than 190 Characters
Current/former SC taxpayers are encouraged to acquire ID theft protection: • Visit **www.ProtectMyID.com/SCDOR** (code **SCDOR123**) or call **1-866-578-5422** to enroll for one year, free of charge.

Prepared by: (b)(6)
Reviewed by

Updated: 2012-03-09/1500
Reviewed: 2012-03-09/1540

Army Recruiting Assistance Programs – Fraud Investigations

The U.S. Army Audit Agency (USAAA) has been conducting a forensic audit of numerous potential fraud cases. About 1,140 NG recruiters have been identified either associated with potentially suspicious or improper payments (suspicious activities that may indicate fraud) involving $87.5 million. OCPA has lead on this matter, and has been coordinating with all necessary organizations. All info has been close hold up to this point based on the sensitive nature of the investigation.

This week, Paul Weber, Associated Press Reporter, San Antonio queried National Guard Bureau Public Affairs and Army Public Affairs seeking more information regarding the Guard Recruiting Assistance Program (G-RAP) and Every Soldier a Recruiting Program (ESAR).

In order to maintain control of the message, all queries would be taken here at OCPA.

HQDA RESPONSE AP REQUEST FOR INFORMATION

"After internal Army investigations identified instances of fraud in Recruiting Assistance Programs, the Secretary of the Army immediately terminated those programs and their funding. He further directed a comprehensive investigation and review by the Army's Criminal Investigation Command (CID) and Army Audit Agency. That investigation of the program's use by the Army, Army National Guard and Army reserve is ongoing. If additional allegations of criminal conduct are found, the Army will take appropriate action. Because of the sensitivity of the criminal investigation, providing any further details or comment would be inappropriate."

Prepared by: (b)(6)
Reviewed by:

Updated: 2012-03-09/1500
Reviewed: 2012-03-09/1540

OCPA Questions & Answers

In order to maintain control of the message, all queries would be taken at OCPA.

Q: Can you provide data about these programs? (Number of soldiers successfully recruited under the program? Total referral applications received? Number of referrals denied? Total recruiting bonuses paid out? Amount, in dollars, of referral bonuses paid to date?
A: Recruiting Assistance Program recruit referral payments, constituting over $366.3 million in payments associated with 151,333 enlistments.

Q: Can you provide copies of annual reports submitted by Docupak to the ANG since the programs began?
A: These reports are not readily available and will take some time to obtain.

Q: Were these programs ever audited? If so, when? Who was the auditing entity? Where can I obtain copies of these audits?
A: Yes. June 2011. Army Audit Agency (AAA). The reports are not readily available and will take some time to obtain.

Q: Related, the Army Reserve Contracting Center also began a similar program with Docupak in 2007. I played it safe and just asked you about GRAP and ESAR - those that I know were programs of the ANG - but please advise if you can also speak to the ARCC arm of this effort.
A: No. I cannot speak on behalf of the Army Reserve. You will need to contact the Army Reserve Public Affairs Office to get information concerning them.

Prepared by: (b)(6)
Reviewed by:

Updated: 2012-03-09/1500
Updated: TBD)

Army Recruiting Assistance Programs – Fraud Investigations

The U.S. Army Audit Agency (USAAA) has been conducting a forensic audit of numerous potential fraud cases. About 1,140 NG recruiters have been identified either associated with potentially suspicious or improper payments (suspicious activities that may indicate fraud) involving $87.5 million. OCPA has lead on this matter, and has been coordinating with all necessary organizations. All info has been close hold up to this point based on the sensitive nature of the investigation.

This week, Paul Weber, Associated Press Reporter, San Antonio queried National Guard Bureau Public Affairs and Army Public Affairs seeking more information regarding the Guard Recruiting Assistance Program (G-RAP) and Every Soldier a Recruiting Program (ESAR).

In order to maintain control of the message, all queries would be taken here at OCPA.

HQDA RESPONSE AP REQUEST FOR INFORMATION

"After internal Army investigations identified instances of fraud in Recruiting Assistance Programs, the Secretary of the Army immediately terminated those programs and their funding. He further directed a comprehensive investigation and review by the Army's Criminal Investigation Command (CID) and Army Audit Agency. That investigation of the program's use by the Army, Army National Guard and Army reserve is ongoing. If additional allegations of criminal conduct are found, the Army will take appropriate action. Because of the sensitivity of the criminal investigation, providing any further details or comment would be inappropriate."

Prepared by: (b)(6)
Reviewed by:

Updated: 2012-03-12/1500
Reviewed: 2012-03-09/1540

Army Recruiting Assistance Programs – Fraud Investigations

The U.S. Army Audit Agency (USAAA) has been conducting a forensic audit of numerous potential fraud cases. About 1,140 NG recruiters have been identified either associated with potentially suspicious or improper payments (suspicious activities that may indicate fraud) involving $87.5 million. OCPA has lead on this matter, and has been coordinating with all necessary organizations. All info has been close hold up to this point based on the sensitive nature of the investigation.

Last week, Paul Weber, Associated Press Reporter, San Antonio queried National Guard Bureau Public Affairs and Army Public Affairs seeking more information regarding the Guard Recruiting Assistance Program (G-RAP) and Every Soldier a Recruiting Program (ESAR).

Today, Bob O'Harrow of Washington Post contacted Army Public Affairs and was provided HQDA response.

In order to maintain control of the message, all queries would be taken here at OCPA.

HQDA STATEMENT - RESPONSE TO QUERY

"After internal Army investigations identified instances of fraud in Recruiting Assistance Programs, the Secretary of the Army immediately terminated those programs and their funding. He further directed a comprehensive investigation and review by the Army's Criminal Investigation Command (CID) and Army Audit Agency. That investigation of the program's use by the Army, Army National Guard and Army reserve is ongoing. If additional allegations of criminal conduct are found, the Army will take appropriate action. Because of the sensitivity of the criminal investigation, providing any further details or comment would be inappropriate."

Prepared by: (b)(6)
Reviewed by:

Updated: 2012-03-12/1500
Reviewed: 2012-03-09/1540

OCPA Questions & Answers

In order to maintain control of the message, all queries would be taken at OCPA.

Q: Can you provide data about these programs? (Number of soldiers successfully recruited under the program? Total referral applications received? Number of referrals denied? Total recruiting bonuses paid out? Amount, in dollars, of referral bonuses paid to date?
A: Recruiting Assistance Program recruit referral payments, constituting over $366.3 million in payments associated with 151,333 enlistments.

Q: Can you provide copies of annual reports submitted by Docupak to the ANG since the programs began?
A: These reports are not readily available and will take some time to obtain.

Q: Were these programs ever audited? If so, when? Who was the auditing entity? Where can I obtain copies of these audits?
A: Yes. June 2011. Army Audit Agency (AAA). The reports are not readily available and will take some time to obtain.

Q: Related, the Army Reserve Contracting Center also began a similar program with Docupak in 2007. I played it safe and just asked you about GRAP and ESAR - those that I know were programs of the ANG - but please advise if you can also speak to the ARCC arm of this effort.
A: No. I cannot speak on behalf of the Army Reserve. You will need to contact the Army Reserve Public Affairs Office to get information concerning them.

Prepared by: (b)(6)
Reviewed by:

Updated: 2012-03-14/1500
Reviewed: 2012-03-09/1540

Army Recruiting Assistance Programs – Fraud Investigations

The U.S. Army Audit Agency (USAAA) has been conducting a forensic audit of numerous potential fraud cases. About 1,140 NG recruiters have been identified either associated with potentially suspicious or improper payments (suspicious activities that may indicate fraud) involving $87.5 million. OCPA has lead on this matter, and has been coordinating with all necessary organizations. All info has been close hold up to this point based on the sensitive nature of the investigation.

The story was covered today by the Washington Post and by MSNBC.

All queries would be referred to OCPA.

HQDA STATEMENT - RESPONSE TO QUERY

"After internal Army investigations identified instances of fraud in Recruiting Assistance Programs, the Secretary of the Army immediately terminated those programs and their funding. He further directed a comprehensive investigation and review by the Army's Criminal Investigation Command (CID) and Army Audit Agency. That investigation of the program's use by the Army, Army National Guard and Army reserve is ongoing. If additional allegations of criminal conduct are found, the Army will take appropriate action. Because of the sensitivity of the criminal investigation, providing any further details or comment would be inappropriate."

Prepared by: (b)(6)
Reviewed by:

Updated: 2012-03-14/1500
Reviewed: 2012-03-09/1540

OCPA Questions & Answers

In order to maintain control of the message, all queries would be taken at OCPA.

Q: Can you provide data about these programs? (Number of soldiers successfully recruited under the program? Total referral applications received? Number of referrals denied? Total recruiting bonuses paid out? Amount, in dollars, of referral bonuses paid to date?
A: Recruiting Assistance Program recruit referral payments, constituting over $366.3 million in payments associated with 151,333 enlistments.

Q: Can you provide copies of annual reports submitted by Docupak to the ANG since the programs began?
A: These reports are not readily available and will take some time to obtain.

Q: Were these programs ever audited? If so, when? Who was the auditing entity? Where can I obtain copies of these audits?
A: Yes. June 2011. Army Audit Agency (AAA). The reports are not readily available and will take some time to obtain.

Q: Related, the Army Reserve Contracting Center also began a similar program with Docupak in 2007. I played it safe and just asked you about GRAP and ESAR - those that I know were programs of the ANG - but please advise if you can also speak to the ARCC arm of this effort.
A: No. I cannot speak on behalf of the Army Reserve. You will need to contact the Army Reserve Public Affairs Office to get information concerning them.

Prepared by: (b)(6)
Reviewed by:

Updated: 2012-03-15/1300
Reviewed: 2012-03-09/1540

Army Recruiting Assistance Programs – Fraud Investigations

The U.S. Army Audit Agency (USAAA) has been conducting a forensic audit of numerous potential fraud cases. About 1,140 NG recruiters have been identified either associated with potentially suspicious or improper payments (suspicious activities that may indicate fraud) involving $87.5 million. OCPA has lead on this matter, and has been coordinating with all necessary organizations. All info has been close hold up to this point based on the sensitive nature of the investigation.

All queries would be referred to OCPA.

HQDA STATEMENT - RESPONSE TO QUERY

"After internal Army investigations identified instances of fraud in Recruiting Assistance Programs, the Secretary of the Army immediately terminated those programs and their funding. He further directed a comprehensive investigation and review by the Army's Criminal Investigation Command (CID) and Army Audit Agency. That investigation of the program's use by the Army, Army National Guard and Army reserve is ongoing. If additional allegations of criminal conduct are found, the Army will take appropriate action. Because of the sensitivity of the criminal investigation, providing any further details or comment would be inappropriate."

Prepared by: (b)(6)
Reviewed by:

Updated: 2012-03-15/1300
Reviewed: 2012-03-09/1540

OCPA Questions & Answers

In order to maintain control of the message, all queries would be taken at OCPA.

Q: Can you provide data about these programs? (Number of soldiers successfully recruited under the program? Total referral applications received? Number of referrals denied? Total recruiting bonuses paid out? Amount, in dollars, of referral bonuses paid to date?
A: Recruiting Assistance Program recruit referral payments, constituting over $366.3 million in payments associated with 151,333 enlistments.

Q: Can you provide copies of annual reports submitted by Docupak to the ANG since the programs began?
A: These reports are not readily available and will take some time to obtain.

Q: Were these programs ever audited? If so, when? Who was the auditing entity? Where can I obtain copies of these audits?
A: Yes. June 2011. Army Audit Agency (AAA). The reports are not readily available and will take some time to obtain.

Q: Related, the Army Reserve Contracting Center also began a similar program with Docupak in 2007. I played it safe and just asked you about GRAP and ESAR - those that I know were programs of the ANG - but please advise if you can also speak to the ARCC arm of this effort.
A: No. I cannot speak on behalf of the Army Reserve. You will need to contact the Army Reserve Public Affairs Office to get information concerning them.

Prepared by: (b)(6)
Reviewed by:

Updated: 2012-03-16/1300
Reviewed: 2012-03-09/1540

Army Recruiting Assistance Programs – Fraud Investigations

The U.S. Army Audit Agency (USAAA) has been conducting a forensic audit of numerous potential fraud cases. About 1,140 NG recruiters have been identified either associated with potentially suspicious or improper payments (suspicious activities that may indicate fraud) involving $87.5 million. OCPA has lead on this matter, and has been coordinating with all necessary organizations. All info has been close hold up to this point based on the sensitive nature of the investigation.

All queries would be referred to OCPA.

HQDA STATEMENT - RESPONSE TO QUERY

"After internal Army investigations identified instances of fraud in Recruiting Assistance Programs, the Secretary of the Army immediately terminated those programs and their funding. He further directed a comprehensive investigation and review by the Army's Criminal Investigation Command (CID) and Army Audit Agency. That investigation of the program's use by the Army, Army National Guard and Army reserve is ongoing. If additional allegations of criminal conduct are found, the Army will take appropriate action. Because of the sensitivity of the criminal investigation, providing any further details or comment would be inappropriate."

Prepared by: (b)(6)
Reviewed by:

Updated: 2012-03-16/1300
Reviewed: 2012-03-09/1540

OCPA Questions & Answers

In order to maintain control of the message, all queries would be taken at OCPA.

Q: Can you provide data about these programs? (Number of soldiers successfully recruited under the program? Total referral applications received? Number of referrals denied? Total recruiting bonuses paid out? Amount, in dollars, of referral bonuses paid to date?
A: Recruiting Assistance Program recruit referral payments, constituting over $366.3 million in payments associated with 151,333 enlistments.

Q: Can you provide copies of annual reports submitted by Docupak to the ANG since the programs began?
A: These reports are not readily available and will take some time to obtain.

Q: Were these programs ever audited? If so, when? Who was the auditing entity? Where can I obtain copies of these audits?
A: Yes. June 2011. Army Audit Agency (AAA). The reports are not readily available and will take some time to obtain.

Q: Related, the Army Reserve Contracting Center also began a similar program with Docupak in 2007. I played it safe and just asked you about GRAP and ESAR - those that I know were programs of the ANG - but please advise if you can also speak to the ARCC arm of this effort.
A: No. I cannot speak on behalf of the Army Reserve. You will need to contact the Army Reserve Public Affairs Office to get information concerning them.

- DoD is working to protect service members from deceptive or predatory sales practices. The July 20 New York Times Article on the topic cited numerous instances of insurance and investment companies conducting captive briefings.

- However, the Department does not intend to prohibit personal insurance solicitation on DoD installations.

- Changes to the commercial solicitation directive will help ensure past abuses are not repeated:

    - Solicitation feedback form to detect violations.
    - Suspension reports of solicitation privileges to higher headquarters.
    - Control of who can provide financial education;.
    - Prevention of commercial sponsorship from being used to obtain personal contact information.

Source: (b)(6) J. Molino, DUSD (MC&FP)
A/O:

INSURANCE SCAMS

DoD is working to protect service members from deceptive or predatory sales practices.

- However, the department does not intend to prohibit personal insurance solicitation on DoD installations.

- Changes to the commercial solicitation directive will help ensure past abuses are not repeated:

    - Solicitation feedback form to detect violations.
    - Suspension reports of solicitation privileges to higher headquarters.
    - Control of who can provide financial education;.
    - Prevention of commercial sponsorship from being used to obtain personal contact information.

Source: (b)(6) ; J. Molino, DUSD (MC&FP)
A/O:

INSURANCE SCAM

July 23, 2004

Insurance Scams – 23 July 04

Insurers and their agents are authorized to solicit on DoD installations provided they are licensed under the insurance laws of the state in which the installation is located.

- The conduct of all insurance business on DoD installations shall be by specific appointment. When establishing the appointment, insurance agents must identify themselves to the prospective purchaser as an agent for a specific company.

- Installation commanders shall designate areas where interviews by appointment may be conducted. Invitations to conduct interviews shall be extended to all agents on an equitable basis. Where space and other considerations limit the number of agents using the interviewing area, the installation commander may develop and publish local policy consistent with this concept.

- Installation commanders shall make disinterested third-party counseling available to DoD personnel desiring counseling.

INSURANCE SCAM

- The Department does not intend to prohibit personal insurance solicitation on DoD installations but must protect Service members from deceptive or predatory sales practices

- DoD efforts to implement policy to strengthen enforcement of personal solicitation policies have been unfortunately delayed as a result of congressional interest. We conducted an open forum in Aug 2003, to obtain public comments on existing personal commercial solicitation policy and will conduct another open forum in the near future to obtain public comments on proposed policy changes.

- Changes to the commercial solicitation directive to require a solicitation feedback form to detect violations, to report suspension of solicitation privileges to higher headquarters, to control who can provide financial education, and to prevent commercial sponsorship from being used to obtain personal contact information will help ensure past abuses are not repeated.

Source: (b)(6) ; J. Molino, ADUSD (MC&FP)
A/O:

INSURANCE SCAMS ON SOLDIERS

From: (b)(6)
Sent: 24 Jul 2014 17:28:01 +0000
To: (b)(6)
Cc: (b)(6)
Subject: Re: UAC scams

Yes, the New York Times ran a piece on it. Here is info from the FBI:
http://www.acf.hhs.gov/programs/orr/news/new-fraud-schemes-targeting-families-of-unaccompanied-children

On Jul 24, 2014, at 12:42 PM, (b)(6) (b)(6) wrote:

Gents, one of my DASDs heard that there are folks trying to obtain UAC information, contacting families of UACs and seeking payment with a promise to reunite the family with the UAC (basically a scam). Anything you have on that would be helpful as it may come up at the DC this afternoon.
My guy wants to get smart on that topic.
VR
(b)(6) (b)(6)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

NATIONAL GUARD BUREAU
111 SOUTH GEORGE MASON ROAD
ARLINGTON VA 22202-3231

NGB-PA 12 JUNE 14

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Social Media Guidance for National Guard Members

1. References.

a. Deputy Secretary of Defense Instruction 8550.01 DoD Internet Services and Internet-Based Capabilities, September 11, 2012.

b. Army Social Media Handbook, Version 3.1, JAN 13.

c. Air Force Social Media Guide, 4th Edition, 01 JUN 13.

2. Purpose. This memorandum provides simple, easy-to-follow tips that will help you use social media in your professional and personal life. This guide is for amplification purposes and does not replace official DoD, Service-specific nor State and Local Command policies.

3. Background. National Guard military and civilian members are encouraged to use social media to share their experiences and to conduct themselves online in a safe and professional manner worthy of their status and calling to support and defend the American people.

4. Official Use. Official online posts involve content released in an official capacity by a National Guard public affairs office. Official contact information, such as official duty telephone numbers or postal and email addresses, should be used to establish official-use accounts when such information is required. Posting internal documents or information that the National Guard has not officially released to the public is prohibited, including memos, emails, meeting notes, message traffic, white papers, public affairs guidance, drill weekend or other training guidance, pre-decisional materials, investigatory information and proprietary information.

5. Personal Use. National Guard members are personally responsible for all content that they publish on social networking sites, blogs or other websites. Personal contact information, such as personal telephone numbers or postal and email address, should be used with discretion to establish personal-use social media accounts. Guard members must comply with their State, Territory or District guidelines and with Army or Air Force guidelines for use of social media. When assigned to a federal mission, Guard

members are subject to disciplinary action under the Uniform Code of Military Justice. Guard members should be mindful that reviewing posts on public and social networking sites may be used as part of character evaluations and background checks for security clearances.

6. Tips on Using Social Media.

a. Guard members may identify themselves as and include their rank, military component and status. However, if they decide not to identify themselves as Guard members, they should not disguise, impersonate or misrepresent their identity or affiliation with the National Guard.

b. When expressing personal opinions, Guard members should make it clear that they are speaking for themselves and not on behalf of the National Guard. They are also encouraged to use a disclaimer such as: "The postings on this site are my own and don't represent the National Guard's positions or opinions."

c. As with other forms of personal public engagement, Guard members must avoid offensive and inappropriate behavior that could bring discredit upon themselves and the National Guard. This includes posting any defamatory, libelous, obscene, abusive, threatening, racially or ethnically hateful or otherwise offensive or illegal information or material.

d. Correcting errors and misrepresentations made by others about the National Guard should be done professionally and respectfully, not emotionally. Guard members should contact their chain of command or public affairs office for guidance if they are uncertain about the need for a response.

e. When posting political content, Guard members must adhere to policy in Department of Defense Directive 1344.10. They should also not imply National Guard endorsement of any opinions, products or causes other than those already officially endorsed by the National Guard.

f. Guard members should use privacy settings on social networking sites so only their “friends” can view their photos and updates. They should also recognize that social network "friends" and "followers" could affect determinations in background investigations for security clearances.

g. The National Guard, Army or Air Force logo and other symbols may be used in unofficial posts as long as the symbols are used in a manner that does not bring discredit upon the Guard, result in personal financial gain or give the impression of official or implied endorsement.

7. Safety.

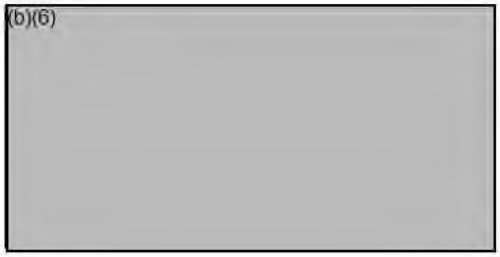
a. Guard members should not release personal identifiable information, such as Social Security number, home address or driver's license number that could be used to distinguish their individual identity or that of another Guardsman.

b. Guard members are also not allowed to release National Guard email addresses, telephone numbers or fax numbers not already authorized for public release. By piecing together information provided on different websites, criminals can use information to impersonate Guard members and steal passwords.

c. Guard members should not post information that would infringe upon the privacy, proprietary or personal rights of others or use any words, logos or other marks that would infringe upon the trademark, service mark, certification mark, or other intellectual property rights of the owners of such marks without the permission of the owners.

d. Finally, Guard members should review their accounts daily for possible use or changes by unauthorized users and should install and maintain current anti-virus and anti-spyware software on their personal computers.

8. Point of Contact. For answers to social media questions, Guard members should contact their local public affairs office or the National Guard Bureau Social Media Team at ngbpa.socialmedia@mail.mil.



DISTRIBUTION:
State PAOs

Department of Defense Public Affairs Guidance for Official Use of Social Media

References: (a) DoD Instruction 8550.01, "DoD Internet Services and Internet-Based Capabilities," September 11, 2012
(b) DoD Directive 5535.09, "DoD Branding and Trademark Licensing Program," December 19, 2007
(c) DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015
(d) DoD Administrative Instruction 15, "OSD Records and Information Management Program," May 3, 2013
(e) Office of Government Ethics' (OGE) Legal Advisory, LA-15-03, "The Standards of Conduct as Applied to Personal Social Media Use," April 9, 2015
(f) DoD 5500.7-R, "Joint Ethics Regulation (JER)," August 30 1993

This attachment contains OSD guidance and best practices for use by social media practitioners and PA staff who oversee and maintain official DoD accounts (e.g. a Uniformed Service's official Twitter page). The implementation of this guidance is effective immediately.

Social media platforms, technology and uses are dynamic and the ability to adapt to changing trends and technologies to will be imperative in order to take full advantage of social media as a communication tool and as part of a comprehensive strategy for the Department of Defense.

Guidance:

I. Establishing an Initial Presence:

A. Approval for official accounts (e.g. External Official Presence (EOP))

EOP activities should be conducted in compliance with the general requirements listed in DoD Instruction 8550.01 (Reference (a)). Before establishing an EOP, approval should be obtained from the responsible DoD Component Head.

Procedures for applying for an official social media account are provided in Enclosure 3 of DoD Instruction 8550.01 (Reference (a)).

It is recommended that only accounts with a dedicated Public Affairs Office (PAO) and a written strategy plan should apply for official verification (the "blue check mark") from specific social media sites. Applicants should submit verification requests to the Digital Engagement Lead for each Uniformed Service or combatant command in coordination with the OATSD(PA) Director of Digital Media.

B. Negotiated Terms of Service agreements

Before deciding to use a social media tool (e.g. Facebook, Instagram), one should seek the advice of the appropriate agency Terms of Service (TOS) Point of Contact (POC) to be sure the agency has already signed a federal-compatible TOS, that the product supports broader agency mission and goals, and that the TOS is legally appropriate for use by that agency. See complete implementation guidance on the main Terms of Service page.

C. Registering an account

All DoD owned and operated social media accounts should be registered at http://www.defense.gov/Sites/Register-A-Site and are encouraged to register with the U.S. Digital Registry at https://www.digitalgov.gov/services/u-s-digital-registry/. When possible, consider registering with an email address linked to the organization overseeing the account and not a specific person so that the email remains valid through personnel changes. Registrations in these sites make it possible to confirm the validity of a variety of government social media accounts.

II. Maintaining an Official Presence:

A. Clearly identify DoD affiliation

In maintaining an official presence, components should adhere to the following:

- Clear identification that a DoD component is supplying the content for the EOP should be provided.
- The DoD Component under which the EOP is managed, the mission of that Component, and the purpose of the EOP should be provided, as workable.
- Official branding should be in accordance with DoD Directive 5535.09 (Reference (b)).

B. Appropriate content

Although social media is more informal and conversational than conventional military communications, PA staff using social media must remain professional at all times and remember that each platform is simply another tool to achieve the DoD mission. The following are some examples to use as guidelines:

- Do not post graphic, obscene, explicit or racial comments, or comments that are abusive, hateful, vindictive or intended to defame anyone or any organization.
- As a general rule, do not post promotional material or advertisements for a non-federal entity, including its products, services, or sponsored events. Certain exceptions may apply, however, so consult with the appropriate ethics official.
- Do not post details about an ongoing investigation, legal or administrative proceeding that could prejudice the processes or interfere with an individual's rights.

- Avoid spamming or trolling which may be removed and may cause the author(s) to be blocked from the page without notice.

- Do not post copyrighted or trademarked content without permission of the copyright or trademark owner. Imagery posted on social media should be owned by the user. It is acceptable to link to trademarked content if an appropriate citation is provided.

- Be careful to not post comments, photos or videos that suggest or encourage illegal activity.

- Avoid politically oriented content. For additional guidance, see: https://osc.gov/Resources/FAQ%20Hatch%20Act%20Employees%20and%20Social%20Media%20Nov%202015.pdf

All information posted to social media sites should be unclassified. In addition information that is For Official Use Only (FOUO), pre-decisional, proprietary, business-sensitive, or protected by the Privacy Act should not be posted without explicit authorization. Ensure that posted information is marked appropriately, as necessary. Do not post personnel lists, rosters, or directories.

- Remember that use of a government or commercial social media site in an official capacity (related to organizational mission) constitutes official communication. Accuracy and propriety are imperative.

III. Additional Best Practices:

A. Handling social media mistakes

Extensive use of social media may result in occasional mistakes. Follow these steps in the event of a posting error or other mistake:

- Maintain all efforts to remain transparent; delete or edit the post and apologize for the mistake as appropriate, and explain that the material was posted in error and is not an official view.

- If the mistake was factual, post the factually correct information, making clear what has been clarified.

- Refer to the individual digital leads in the appropriate Uniformed Service or DoD component for further guidance.

B. Keeping social media sites safe

Social media access and content need to be defended and protected with vigilance. Cyber-attacks are a real and present threat to the security of government social media accounts. Below are some best practices for keeping social media sites safe:

- Use a strong password. At least 20 characters long, that is either randomly-generated (like LauH6maicaza1Neez3zi) or a random string of words (like "hewn cloths titles yachts refine"). Use a unique password for each website or service to ensure that if one account gets compromised the rest remain safe.

- Use a government e-mail address for official accounts, also with a strong password. A .mil or .gov account will generally be more secure than a personal account, and will reduce the possibility of unauthorized password-reset and interception of emails. Consider added precautions such as two-factor authentication.

- Do not give untrusted third parties, including those who promise more followers or financial returns, access to account usernames and passwords.

- Select third-party applications with care. There are thousands of applications built by external developers that allow an array of innovative functions with an account. Control of a government social media site account should not be given to anyone outside of the command or organization. Revoke access for any third-party application that is not recognized by visiting the Applications tab in the platform's account settings.

- Make sure all computers and operating systems are up-to-date with the most recent patches, upgrades, and anti-virus software, and that all computers and mobile devices are protected by secure passwords.

- Change social media account passwords at a regularly scheduled time (e.g. once a quarter). Never send passwords via email, even internally.

- **Use extra security features** to help keep accounts protected. For example, Facebook has such instructions here.

- **Minimize the number of people who have access to the account.** Even if a third-party platform is used to avoid sharing the actual account passwords, each person is a possible avenue for phishing or other compromise.

- Report all security violations (e.g. hacked accounts, impostors, etc.) through the appropriate DoD security channels and the Digital Engagement Leads, as well as appropriate social media provider channels (e.g. online forms). For example, to report a violation on Twitter, in addition to reporting through DoD channels, file a security ticket at https://support.twitter.com/forms/.

C. Making use of social media analytics (tracking and reporting)

The majority of social platforms offer more data, either through third party tools or internal "analytics," than has typically been available to PA practitioners. For example, Facebook offers analytics in their "insights page" and Twitter has an "analytics" page. This information is best used for two key purposes: guiding strategy and reporting impact.

Strategy

- Social platforms and audience methods of consumption change so rapidly that current effective posting strategies may become ineffective in a short period of time. Social media practitioners need to have an adaptable strategy. The best way to inform that strategy is to use the analytical tools available on each platform or seek a third party tool (e.g. Hootsuite, sprout social, Radian6).

- Evaluate the intended audience. Review the data to track current followers, as well as whom the content reaches and who engages with it.

- Find patterns in successful posts. Analyze which posts achieve the best results and why. However, this step will become ineffective if posts are constructed the same way each time, so do not be afraid to test different tactics:
    - Experiment (develop a different type of post/campaign/presentation)
    - Engage (reply to a comment or create calls to action)
    - Measure (analyze impact)
    - Repeat (alter the post as necessary as informed by measurement).

Reporting

- While far from perfect, it is possible to measure the impact of one's communication efforts more than ever before. As communications professionals, it is important to provide easily understood, clearly focused reports to commanders.

- Be the translator. For example, explain what a "like" and an "engagement" are. Reports need to be clearly understood by non-social media practitioners. Be sure to provide context to reports.

- Focus on what is important. Avoid providing numbers for the sake of numbers. Reporting should be done when there is a measurable impact on a required objective, or actionable data can be provided to the commander. Reach, impressions, and engagements may have meaning to social media managers, but not to commanders.

- Be clear about what metrics will be prioritized and why. As an example, some organizations may prefer to focus on the number of "likes" as a measure of success. Others will choose to focus on shares.

D. Personal use of social media

For personal social media accounts, the user need not include DoD affiliation in a profile. Remember that even when posting in a personal capacity, others may still identify a poster's

DoD affiliation, even if not included in the public profile. Stating that one's views are personal does not remove the risk of negative media or other publicity. Social media practitioners should always keep in mind that posts can be shared outside of one's personal network.

Please follow Executive Branch-wide guidance for personal social media usage during work hours (*see Office of Government Ethics' (OGE) Legal Advisory, LA-15-03: The Standards of Conduct as Applied to Personal Social Media Use*, http://www.oge.gov/OGE-Advisories/Legal-Advisories/LA-15-03--The-Standards-of-Conduct-as-Applied-to-Personal-Social-Media-Use/ Reference (e)), in addition to pertinent guidance in DoD Instruction 8550.01 (Reference (a)) and the Joint Ethics Regulation (Reference (f)).

IV. Records Management:

DoD components should create an internal records management process and should work with their service component electronic records management office to establish this process, in accordance with DoD Instruction 5015.02 (Reference (c)) and DoD Administrative Instruction 15 (Reference (d)).

Department of Defense Public Affairs Guidance for Official Use of Social Media

References: (a) DoD Instruction 8550.01, "DoD Internet Services and Internet-Based Capabilities," September 11, 2012
(b) DoD Directive 5535.09, "DoD Branding and Trademark Licensing Program," December 19, 2007
(c) DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015
(d) DoD Administrative Instruction 15, "OSD Records and Information Management Program," May 3, 2013
(e) Office of Government Ethics' (OGE) Legal Advisory, LA-15-03, "The Standards of Conduct as Applied to Personal Social Media Use," April 9, 2015
(f) DoD 5500.7-R, "Joint Ethics Regulation (JER)," August 30 1993

This attachment contains OSD guidance and best practices for use by social media practitioners and PA staff who oversee and maintain official DoD accounts (e.g. a Uniformed Service's official Twitter page). The implementation of this guidance is effective immediately.

Social media platforms, technology and uses are dynamic and the ability to adapt to changing trends and technologies to will be imperative in order to take full advantage of social media as a communication tool and as part of a comprehensive strategy for the Department of Defense.

Guidance:

I. Establishing an Initial Presence:

A. Approval for official accounts (e.g. External Official Presence (EOP))

EOP activities should be conducted in compliance with the general requirements listed in DoD Instruction 8550.01 (Reference (a)). Before establishing an EOP, approval should be obtained from the responsible DoD Component Head.

Procedures for applying for an official social media account are provided in Enclosure 3 of DoD Instruction 8550.01 (Reference (a)).

It is recommended that only accounts with a dedicated Public Affairs Office (PAO) and a written strategy plan should apply for official verification (the "blue check mark") from specific social media sites. Applicants should submit verification requests to the Digital Engagement Lead for each Uniformed Service or combatant command in coordination with the OATSD(PA) Director of Digital Media.

B. Negotiated Terms of Service agreements

Before deciding to use a social media tool (e.g. Facebook, Instagram), one should seek the advice of the appropriate agency Terms of Service (TOS) Point of Contact (POC) to be sure the agency has already signed a federal-compatible TOS, that the product supports broader agency mission and goals, and that the TOS is legally appropriate for use by that agency. See complete implementation guidance on the main Terms of Service page.

C. Registering an account

All DoD owned and operated social media accounts should be registered at http://www.defense.gov/Sites/Register-A-Site and are encouraged to register with the U.S. Digital Registry at https://www.digitalgov.gov/services/u-s-digital-registry/. When possible, consider registering with an email address linked to the organization overseeing the account and not a specific person so that the email remains valid through personnel changes. Registrations in these sites make it possible to confirm the validity of a variety of government social media accounts.

II. Maintaining an Official Presence:

A. Clearly identify DoD affiliation

In maintaining an official presence, components should adhere to the following:

- Clear identification that a DoD component is supplying the content for the EOP should be provided.
- The DoD Component under which the EOP is managed, the mission of that Component, and the purpose of the EOP should be provided, as workable.
- Official branding should be in accordance with DoD Directive 5535.09 (Reference (b)).

B. Appropriate content

Although social media is more informal and conversational than conventional military communications, PA staff using social media must remain professional at all times and remember that each platform is simply another tool to achieve the DoD mission. The following are some examples to use as guidelines:

- Do not post graphic, obscene, explicit or racial comments, or comments that are abusive, hateful, vindictive or intended to defame anyone or any organization.
- As a general rule, do not post promotional material or advertisements for a non-federal entity, including its products, services, or sponsored events. Certain exceptions may apply, however, so consult with the appropriate ethics official.
- Do not post details about an ongoing investigation, legal or administrative proceeding that could prejudice the processes or interfere with an individual's rights.

- Avoid spamming or trolling which may be removed and may cause the author(s) to be blocked from the page without notice.

- Do not post copyrighted or trademarked content without permission of the copyright or trademark owner. Imagery posted on social media should be owned by the user. It is acceptable to link to trademarked content if an appropriate citation is provided.

- Be careful to not post comments, photos or videos that suggest or encourage illegal activity.

- Avoid politically oriented content. For additional guidance, see: https://osc.gov/Resources/FAQ%20Hatch%20Act%20Employees%20and%20Social%20Media%20Nov%202015.pdf

All information posted to social media sites should be unclassified. In addition information that is For Official Use Only (FOUO), pre-decisional, proprietary, business-sensitive, or protected by the Privacy Act should not be posted without explicit authorization. Ensure that posted information is marked appropriately, as necessary. Do not post personnel lists, rosters, or directories.

- Remember that use of a government or commercial social media site in an official capacity (related to organizational mission) constitutes official communication. Accuracy and propriety are imperative.

III. Additional Best Practices:

A. Handling social media mistakes

Extensive use of social media may result in occasional mistakes. Follow these steps in the event of a posting error or other mistake:

- Maintain all efforts to remain transparent; delete or edit the post and apologize for the mistake as appropriate, and explain that the material was posted in error and is not an official view.

- If the mistake was factual, post the factually correct information, making clear what has been clarified.

- Refer to the individual digital leads in the appropriate Uniformed Service or DoD component for further guidance.

B. Keeping social media sites safe

Social media access and content need to be defended and protected with vigilance. Cyber-attacks are a real and present threat to the security of government social media accounts. Below are some best practices for keeping social media sites safe:

- Use a strong password. At least 20 characters long, that is either randomly-generated (like LauH6maicaza1Neez3zi) or a random string of words (like "hewn cloths titles yachts refine"). Use a unique password for each website or service to ensure that if one account gets compromised the rest remain safe.

- Use a government e-mail address for official accounts, also with a strong password. A .mil or .gov account will generally be more secure than a personal account, and will reduce the possibility of unauthorized password-reset and interception of emails. Consider added precautions such as two-factor authentication.

- Do not give untrusted third parties, including those who promise more followers or financial returns, access to account usernames and passwords.

- Select third-party applications with care. There are thousands of applications built by external developers that allow an array of innovative functions with an account. Control of a government social media site account should not be given to anyone outside of the command or organization. Revoke access for any third-party application that is not recognized by visiting the Applications tab in the platform's account settings.

- Make sure all computers and operating systems are up-to-date with the most recent patches, upgrades, and anti-virus software, and that all computers and mobile devices are protected by secure passwords.

- Change social media account passwords at a regularly scheduled time (e.g. once a quarter). Never send passwords via email, even internally.

- **Use extra security features** to help keep accounts protected. For example, Facebook has such instructions here.

- **Minimize the number of people who have access to the account.** Even if a third-party platform is used to avoid sharing the actual account passwords, each person is a possible avenue for phishing or other compromise.

- Report all security violations (e.g. hacked accounts, impostors, etc.) through the appropriate DoD security channels and the Digital Engagement Leads, as well as appropriate social media provider channels (e.g. online forms). For example, to report a violation on Twitter, in addition to reporting through DoD channels, file a security ticket at https://support.twitter.com/forms/.

C. Making use of social media analytics (tracking and reporting)

The majority of social platforms offer more data, either through third party tools or internal "analytics," than has typically been available to PA practitioners. For example, Facebook offers analytics in their "insights page" and Twitter has an "analytics" page. This information is best used for two key purposes: guiding strategy and reporting impact.

Strategy

- Social platforms and audience methods of consumption change so rapidly that current effective posting strategies may become ineffective in a short period of time. Social media practitioners need to have an adaptable strategy. The best way to inform that strategy is to use the analytical tools available on each platform or seek a third party tool (e.g. Hootsuite, sprout social, Radian6).

- Evaluate the intended audience. Review the data to track current followers, as well as whom the content reaches and who engages with it.

- Find patterns in successful posts. Analyze which posts achieve the best results and why. However, this step will become ineffective if posts are constructed the same way each time, so do not be afraid to test different tactics:
    - Experiment (develop a different type of post/campaign/presentation)
    - Engage (reply to a comment or create calls to action)
    - Measure (analyze impact)
    - Repeat (alter the post as necessary as informed by measurement).

Reporting

- While far from perfect, it is possible to measure the impact of one's communication efforts more than ever before. As communications professionals, it is important to provide easily understood, clearly focused reports to commanders.

- Be the translator. For example, explain what a "like" and an "engagement" are. Reports need to be clearly understood by non-social media practitioners. Be sure to provide context to reports.

- Focus on what is important. Avoid providing numbers for the sake of numbers. Reporting should be done when there is a measurable impact on a required objective, or actionable data can be provided to the commander. Reach, impressions, and engagements may have meaning to social media managers, but not to commanders.

- Be clear about what metrics will be prioritized and why. As an example, some organizations may prefer to focus on the number of "likes" as a measure of success. Others will choose to focus on shares.

D. Personal use of social media

For personal social media accounts, the user need not include DoD affiliation in a profile. Remember that even when posting in a personal capacity, others may still identify a poster's

DoD affiliation, even if not included in the public profile. Stating that one's views are personal does not remove the risk of negative media or other publicity. Social media practitioners should always keep in mind that posts can be shared outside of one's personal network.

Please follow Executive Branch-wide guidance for personal social media usage during work hours (*see Office of Government Ethics' (OGE) Legal Advisory, LA-15-03: The Standards of Conduct as Applied to Personal Social Media Use*, http://www.oge.gov/OGE-Advisories/Legal-Advisories/LA-15-03--The-Standards-of-Conduct-as-Applied-to-Personal-Social-Media-Use/ Reference (e)), in addition to pertinent guidance in DoD Instruction 8550.01 (Reference (a)) and the Joint Ethics Regulation (Reference (f)).

IV. Records Management:

DoD components should create an internal records management process and should work with their service component electronic records management office to establish this process, in accordance with DoD Instruction 5015.02 (Reference (c)) and DoD Administrative Instruction 15 (Reference (d)).

Social Media

Social media is a way for people to communicate and interact online. It's called social media because users engage with (and around) it in a social context, which can include conversations, commentary, and other user-generated annotations and engagement interactions. Undoubtedly, Social Media is an integral part of the strategic communications and public affairs missions of the Department of Defense. However, like any asset, it is something to defend and protect with vigilance. Cyber attacks are a real and present threat to the security of government social media accounts.

In this guide you will find information about how to create and cultivate a social media presence, best practices for current platforms, and the steps needed in order to be protective, preventative, and proactive against cyber-attacks.

Platform Overview

The Department of Defense (Military Branches, COCOMS, OSD) uses several social media platforms to communicate the priorities of the military branches and the Secretary to its target audience, which includes civilians, veterans, active duty personnel, defense media and experts, and international allies.

The Department of Defense currently uses the following social media assets to communicate its message: Facebook, Twitter, Instagram, Vine, You tube, LinkedIn, Google +, and Flickr.

Facebook:
Facebook has become the most widely-used social network to date and has shaped online interaction as we know it. From connecting distant friends and family members, to bridging the gap between brands and their communities, Facebook has taken the way we interact online to a whole new level. Facebook is particularly popular among military families. According to a Blue Star Families 2014 report:

- Military families reported using Facebook at a higher rate (93%) than civilians (67%).
- 4 million people on Facebook are veterans or active duty members.
- 12.5 million people on Facebook are family members of a veteran or an active duty member.

Twitter:
Twitter's 140-character bite-size updates have transformed the world's access to real-time information. Its simple interface allows for sharing anything from breaking news to sports, to great content, to worldwide politics.

Instagram
Instagram is an online mobile photo-sharing, video-sharing and social networking service. It is owned by Facebook. You can post both videos up to 15 seconds in length, and you have a

whole bunch of extra filter options plus the ability to tweak and edit. You can configure your Instagram account to have photos posted on Facebook, Twitter, Tumblr or Flickr.

Flickr
Flickr is the best site for annotating, curating, storing, and managing photos. It supports an active and engaged community where people share and explore each other's photos. You can share and host hundreds of your own pictures on Flickr without paying a dime.

LinkedIn
LinkedIn is a business-oriented social networking service. Professionals at all levels—entry-level, middle management and executives—use it to search for jobs, keep in touch with current and former colleagues, and engage with their broader industry.

Youtube
YouTube has become more than just a place to watch cat videos. It has morphed into the world's second-largest search engine, a driver of online culture, and a springboard for Internet fame. There's still plenty of cat videos to go around, but YouTube has its sights on bigger, better ideas. Users can follow channels (which have gotten more sophisticated in their design and functionality over the years), upload their own content, comment on and discuss videos, and follow other users' content.

Vine
Vine is a short-form video sharing service where users can share six second-long looping video clips. Prior to 2015, Twitter did not support native video uploads so Vine was a way to upload short videos to your Twitter feed. With Twitter's addition of video upload capability, Vine has become less useful as a platform.

What/when can you post?

Social media is more conversational than standard military communications; however, you must remain professional at all times and remember that each platform is just another tool to achieve our mission.

Do not use social media as a one way newsfeed. Social Media requires a conversation and smaller pieces of digestible, transportable information. Not every article can or should be posted to your Social Media channels.

Examples of Best Practices:

- Spread your posts/comments throughout the day.
- Videos perform better when uploaded directly to FB or Twitter, rather than sharing a link to YouTube
- Update your cover photos regularly.

- Do not comment for the sake of commenting; ensure your posts are relevant and interesting.
- Do not post any defamatory, libelous, vulgar, obscene, abusive, profane, threatening, hateful, racially, ethnically, or otherwise offensive or illegal information or material.
- Do not post any information or other material protected by copyright without the permission of the copyright owner.
- Do not use any words, logos or other marks that would infringe upon the trademark, service mark, certification mark, or other intellectual property rights of the owners of such marks without the permission of such owners.
- Do not post classified or sensitive information.
- Do not post any information that would infringe upon the proprietary, privacy, or personal rights of others.
- Do not forge or otherwise manipulate identifiers in posts in an attempt to disguise, impersonate, or otherwise misrepresent their identity or affiliation with any other person or entity.
- Identify to readers of a personal social media site or post that the views expressed are yours alone and that they do not necessarily reflect the views of the Air Force. Use a disclaimer such as: "The postings on this site are my own and don't necessarily represent Air Force positions, strategies, or opinions."
- Use a strong Profanity Filter on Facebook: located in settings under Page Moderation on Facebook. You can add words that should be blocked from your page.

Be mindful of a concept known as "social media weather". The ebb and flow of information shared and received on social media is subject to constant change, often without warning or notice. These storms and swells will affect your social media interaction, especially if it is a big news story. You cannot always predict the social media weather, but all content strategists should be mindful of these unknown variables, and the role they will play on your content and interaction on your platforms.

How to write a good tweet:

Write engaging content that speaks to your audience

The first part of your Tweet should be around 90-100 characters. This text should be engaging, show off your brand personality, and include a call to action. Yes, Twitter's character limit is

140; however, if you're going to ask people to retweet your Tweet, make sure you leave enough room for them to add 'RT' to the body of the Tweet.

Include a URL (or a shortened URL)

For a majority of users, Twitter is used to drive traffic to a website. You are not a news outlet or brand, so much of your content will be commentary/opinion. However, there will be times when you want to send users to the OIR web special, or reference an article. In these instances, make sure to include a URL in your Tweet. Better yet, include a shortened URL, using a URL shortener like bit.ly or go.usa.gov, so you can track click-through rate. It also makes the tweet look cleaner.

Wrap up your Tweet with a hashtag

Increase the reach of your Tweet by using a relevant hashtag. Hashtags will increase your Tweet's visibility on the network, and help you join the bigger discussion going on around the topic. For example, if your Tweet is about ISIL, include the hashtag #ISIL (or #ISIS).

Include an image or a video

Still images and videos can dramatically increase the engagement rate for your Tweets. Make sure the images that accompany your Tweet are relevant and high-quality.

Tag (Verified) Accounts

Feel free to tag other users in your posts, especially verified users like @DeptofDefense or @USArmy. This will alert the user that you mentioned them and encourage them to reply.

Tracking/Reporting – Analytics

It is important to track how well you are doing. You can do this with a third party tool, like Engagor, Meltwater, etc, or most platforms have their own "analytics" section. Analytics tracks impressions, engagement, and engagement rate. **Impressions** is the number of times your tweet was delivered to someone's feed. **Engagement** tracks the number of RTs, Favorites, replies, or clicks on your tweet and the **Engagement Rate** is engagement divided by impressions.

Keeping your social media sites safe

Use a strong password. At least 20 characters long, that is either randomly-generated (like LauH6maicaza1Neez3zi) or a random string of words (like "hewn cloths titles yachts refine"). Use a unique password for each website or service you use; that way, if one account gets compromised, the rest are safe.

Use a government e-mail address, also with a strong password. A .gov or other private-domain account will generally be more secure than a public service, and will reduce the possibility of password-reset and other emails being intercepted. If you must use a public email provider, consider added precautions such as Gmail's two-factor authentication.

Don't give your username and password out to untrusted third parties, especially those promising to get you followers or make you money.

Select third-party applications with care. There are thousands of applications built by external developers that allow you to do an array of neat things with your account. However, you should be cautious before giving up control of your account to someone else. Revoke access for any third-party application that you don't recognize by visiting the Applications tab in your account settings.

Make sure your computer and operating system is up-to-date with the most recent patches, upgrades, and anti-virus software, and that all your computers and mobile devices are protected by secure passwords.

Change your Twitter account passwords at a regularly scheduled time (ie: once a quarter). Never send passwords via email, even internally.

Keep your email accounts secure. Twitter, Facebook, Google+, etc use email for password resets and official communication. Change your email passwords, and use a password different from your social media account passwords.

Review your authorized applications. Log in to Twitter or Facebook and review the applications authorized to access your accounts. If you don't recognize any of the applications on Twitter, contact them immediately by filing a security ticket and emailing hacked@twitter.com.

Use extra security features. This will help keep your accounts protected. **Facebook has a whole section on how to do that located here**.

Talk with your security team about ensuring that your email system is as safe as possible.

Minimize the number of people who have access to the account. Even if you use a third-party platform to avoid sharing the actual account passwords, each of these people is a possible avenue for phishing or other compromise.

Social Media Crisis Plan

Evaluate your position and risk level - Get all the details down internally. Know all the facts you will be hit with and assume the worst case scenario. Assess the threat quickly by asking: is this a hack (high threat level) or a troll (lowest threat level)?

Maintain updated contact information for anyone who could be contacted for a crisis.

Get it out first and on your terms. The minute something goes public is the best opportunity to define the terms of the engagement. The first response should always be "We know something happened and we are tracking it. We will update you with information when we have it."

Fight Social Media Fire with Social Media Water: Once you have some information, you should respond first in the venue where the crisis first broke. **If the crisis initiated on Facebook, respond first on Facebook,** then circle around and respond in other venue that have picked up on the crisis.

Pull down all auto- or pre-scheduled content: Any content that was pre-loaded onto our social media platforms should be removed until the crisis is resolved.

Arm the team: Any talking points that are developed by the Social Crisis Team should be disseminated to all social media and public affairs account holders as soon as available through a pre-approved distribution list.

Create a Crisis FAQ
Create a Web page or microsite and put all the information about the crisis in one place**.** This will allow you to respond to questions with a link instead of an answer. This saves times and prevents misinterpretation of your responses.

This Crisis FAQ should include:

- Acknowledgement of the crisis
- Details about the occurrence
- Photos or videos, if available
- How you found out
- Who was alerted, when, and how
- Specific actions taken in response
- Steps taken to prevent future occurrence
- Contact information as appropriate

Constantly reevaluate status. Crises move very quickly, so frequent evaluation of your tactics' success in moving towards win are important. If things aren't working, is it time to elevate to a higher-up voice? What are your available tactics?

AAR: After the crisis subsides, reconstruct and deconstruct the crisis. Document every facet:

- Make copies of all tweets, status updates, blog comments, etc.
- Save copies of all emails
- Analyze website traffic patterns

- Where did the crisis break, and when? Where did it spread, and how?
- How did the internal notification work?
- How did the response protocol work?
- Did specific customers rise to your defense? (consider thanking them)
- Were the appropriate staff members informed throughout the process?
- How did the online crisis intersect with traditional media coverage

Launching a Facebook Page for an Air Force Senior Leader

Develop communications plan prior to site activation

1. Set goals and strategies
2. Identify target audiences
3. Messaging
    a. Content to reach audiences
        i. Consider interests and preferences for obtaining and retaining followers and methods to drive traffic to the page
    b. Ensure info posted is approved for public release; remember OPSEC, propriety, Privacy Act considerations etc
4. Recommend Facebook page versus Facebook profile
    a. Recommend naming the page "Chief Master Sgt of the Air Force" instead of "CMSAF James Roy" – allows easy transition to successor
    b. Okay to personalize page with CMSgt Roy's photo and other info
    c. Designate admins to help control the page
    d. Each admin must have a FB profile first
    e. Success increased when site is personalized and uses informal, conversational language – *personal involvement of the principal is critical*
    f. Examples: http://www.facebook.com/generalrayjohns http://www.facebook.com/admiralmikemullen
5. Plan for feedback and negative comments/posts
    a. Include SWOT analysis
    b. Work with PA advisor to review content prior to posting to ensure consistency with security and policy
    c. Have a legal contact on stand-by as situations arise
    d. Establish a disclaimer indicating that personal opinions do not necessarily reflect the official views of the USAF or DOD; likewise appearance of links to outside content do not imply endorsement by USAF or DOD
    e. Establish a comment policy may help prevent inappropriate feedback/negative posts
        i. Define the page's rules of engagement with enlisted force
        ii. Consider reminding Airmen to use their chain of command for issues or problems
        iii. Build comment policy from United States Air Force Facebook page then customize as needed
6. Refer to *Social Media the Air Force* for guidelines

Official accounts

Official accounts allow us to target key audiences, deliver our messages and information directly,

engage and be open to challenge, opening up access to our officials and Ministers.

If you wish to apply for an o

fficial social media account please refer to the

online guidance

and

complete this

application form

.

Official social media channels should provide relevant, useful information on UK Government

activity; promote the FCO, HMG and relevant par

tner content in line with FCO objectives.

More specifically official accounts should have a clear purpose and audience and be evaluated

against those criteria.

Below is a framework on when to seek clearance before publishing content on official channels:

Go ahead

Established policy and press lines within your

area of expertise.

Seek guidance from head of team and/or Media

Office & Digital Transformation Unit.

Breaking news where there is no press line.

The interpretation of a change of policy where

the l

ine is being agreed.

Ministerial movements.

Rebuttal.

Don't do it

Subjects not in your area of expert

ise or direct

responsibility.

A

ny classified data.

U

pdate social media channels regularly or it is not worth doing at all

–

tailor frequency, length

and

type of updates to audience needs and expectations.

You are encouraged to share interesting third party content e.g. media articles, NGO blogs, foreign

government information but only if you are sure that it is appropriate and it is politically imparti

al.

Take into account cultural sensitivities and avoid posting anything that could be considered offensive

by anyone who may see the page (including audiences from other countries)

Debate is good, a protracted online argument is not. Take discussion best d

ealt with in private

offline.

Do not post or share anything which breaches Copyright or that could be construed as advertising or

promoting a commercial company.

Do not disclose information that is classified or privileged, or that may put you or your

colleagues at

risk, whether from crime, terrorism, or espionage.

As with any form of communication, if in doubt, seek advice from a colleague or do not post at all.

Personal use of social media

We have no bar on staff using social media channels, but there

are some rules.

Where your social media accounts are personal, you do not need to say you work for the FCO or Civil

Service.

It is important to remember that when posting in a personal capacity you may still easily be

identified by others as working for t

he FCO even if you don't state it.

Stating that your views are personal is no insurance against negative media or other publicity.

On personal social networks

–

even closed ones like Facebook

–

you should be aware that posts can

be shared outside your netw

ork.

You should avoid taking part in any political or public activity which compromises, or might be seen

to compromise, your impartial service to the government. The precise restrictions are specific to

different staff (e.g. politically restricted grades)

and you should know them already as they apply to

you offline too.

See the safety information above.

Dealing with mistakes

In making full use of social media, mistakes will occasionally happen.

How the FCO deals with a particular mistake will depend on th

e nature of the error. Your online

conduct is subject to the same disciplinary rules as your offline conduct.

There are a few steps you should take if you make a mistake:

Delete the post and apologise for the mistake, explaining that the material was

posted by mistake

and is not an official view.

Post the correct information if the mistake was factual, making clear what you've corrected.

Inform your line manager and the

Digital Transformation Unit

for advice on further handling.

If you work for FCO Services, please consult the FCO Services Social Media Policy which can be found

on 'One Way' (accessible only to FCO Services staff).

Social Media Guidance for Unofficial Posts

ONLINE SOCIAL MEDIA GUIDANCE
For
UNOFFICIAL INTERNET POSTS

1. Overview

a. This guidance is provided for Marines who, in their personal capacity, desire to make unofficial posts online, regarding Marine Corps-related topics. (The term "Marines" on this guidance refers to active-duty and reserve Marines and sailors).

"Unofficial Internet posts," referred to below, are considered any content about the Marine Corps or related to the Marine Corps that are posted on any Internet site by Marines 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 Marine Corps or Department of Defense.

b. Unofficial Internet posts are not initiated by any part of the Marine Corps or reviewed within any official Marine Corps approval process. By contrast, official Internet posts involve content released in an official capacity by public affairs Marines, Marine Corps Community Services marketing directors, or commanders designated as releasing authorities. Policy for Family Readiness Officers will be provided in separate guidance.

c. In accordance with these guidelines, Marines are encouraged to responsibly engage in unofficial Internet posts about the Marine Corps and Marine Corps-related topics. The Marine Corps performs a valuable service around the world every day and Marines are often in the best position to share the Marine Corps' story with the domestic and foreign publics.

2. Guidelines

a. Marines are **personally responsible** for all content they publish on social networking sites, blogs, or other websites. In addition to ensuring Marine Corps content is accurate and appropriate, Marines also must be thoughtful about the non-Marine related content they post, since the lines between a Marine's personal and professional life often blur in the online space. Marines **must be acutely aware that they lose control over content they post on the Internet** and that many social media sites have policies that give these sites ownership of all content and information posted or stored on those systems. Thus Marines should **use their best judgment at all times and keep in mind how the content of their posts will reflect upon themselves, their unit, and the Marine Corps.**

b. As with other forms of communication, Marines are responsible for adhering to Federal law, Marine Corps regulations and governing policies when making unofficial Internet posts. Marines must abide by certain restrictions and policy to ensure good order and discipline. Federal law, regulations and policies that directly impact a Marine's conduct mandate personal standards of conduct, operational security, information assurance, release of personally identifiable information, ethics regulations, and the release of information to the public. **A Marine who violates Federal law, regulations or policies through inappropriate personal online activity is subject to disciplinary action under the Uniform Code of Military Justice (UCMJ).** See the references listed below for more details.

c. Marines who communicate online about the Marine Corps in unofficial Internet posts may identify themselves as Marines, to include their rank, military component (e.g., Captain Smith, USMC), and status (active or reserve) if desired. However, if Marines decide not to identify themselves as Marines, they should not disguise, impersonate or otherwise misrepresent their identity or affiliation with the Marine Corps. **When expressing personal opinions, Marines should make clear that they are speaking for themselves and not on behalf of the Marine Corps.** Use a disclaimer such as: "the postings on this site are my own and don't represent Marine Corps' positions or opinions."

d. As with other forms of personal public engagement, **Marines should avoid offensive and inappropriate behavior that could bring discredit upon themselves and the Marine Corps. This behavior includes posting any defamatory, libelous, obscene, abusive, threatening, racially or ethnically hateful, or otherwise offensive or illegal information or material.**

e. Marines shall not post classified, controlled unclassified information (CUI), or sensitive information (for example, tactics, troop movements, force size, weapon system details, etc). When in doubt, Marines should contact the unit operations officer, security officer, intelligence officer, or public affairs officer for guidance.

f. Marines should be extremely judicious when disclosing personal details on the Internet, and should not release personal identifiable information (PII) that could be used to distinguish their individual identity or that of another Marine. Examples of PII include a Marine's social security number, home address, birthday, birth place, driver's license number, etc. Marines must be aware that criminals use the Internet to gain information for unscrupulous activities such as identity theft. **By piecing together information provided on different websites, criminals can use information to, among other things, impersonate Marines and steal passwords.** In addition, Marines should utilize privacy settings on social networking sites so posted personal information and photos can be viewed only by designated people. **Remember, what happens online, is available to everyone, everywhere.** There is no immediate assumption of privacy once users begin to interact with others online.

g. Marines should not post information that would infringe upon the privacy, proprietary, or personal rights of others.

h. Marines should not use any words, logos or other marks that would infringe upon the trademark, service mark, certification mark, or other intellectual property rights of the owners of such marks without the permission of such owners.

i. Marines may use the eagle, globe and anchor; coat of arms (ega in the center, encircled with words "United States – Marine Corps"); and other symbols in unofficial posts so long as the symbols are used in a manner that does not bring discredit upon the Corps, does not result in personal financial gain, or does not give the impression of official or implied endorsement. Marines should contact HQMC Division of Public Affairs Trademark and Licensing office for further clarification or contact their local legal office for an ethics determination prior to engaging in Internet activity that could violate the standards of conduct. **Marines who violate the Marine Corps' symbols (ega and/or coat of arms) are potentially subject to legal proceedings.**

j. **The posting or disclosure of internal Marine Corps documents or information that the Marine Corps has not officially released to the public is prohibited. This policy applies no matter how a Marine comes into possession of a**

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. **Marines are also prohibited from releasing Marine Corps e-mail addresses, telephone numbers, or fax numbers not already authorized for public release.**

k. Marines should only discuss Marine Corps issues related to their professional expertise, personal experiences, or personal knowledge.

l. Marines are encouraged to professionally and respectfully correct errors and misrepresentations made, by others, about the Marine Corps. **Marines must remember however, to respond and act with their minds and not their emotions when posting content.** Marines should refer to the chain of command or public affairs for guidance if uncertain about the need for or appropriateness of a response.

m. Marines must adhere to policy in Department of Defense Directive 1344.10 when posting political content. Marines also should take care not to express or imply Marine Corps endorsement of any opinions, products or causes other than those already officially endorsed by the Marine Corps.

n. Marines should be cautious and guard against cyber criminals and attackers by following sound security procedures (Questions regarding security issues can be directed to HQMC C4 Information Assurance personnel). When using the Internet and social media, Marines should not click links or open attachments unless the source can be trusted. Oftentimes, **cyber criminals pretend to be people they are not in order to deceive Marines into performing actions that launch cyber attacks, download viruses, and install malware and spyware onto computers.**

o. Marines should always use strong passwords (10-digit passwords comprised of lower- and upper-case letters, numbers, and symbols) to protect their online / social media accounts from getting hacked. Marines also should frequently change their passwords.

p. Marines should be thoughtful about who they allow to access their social media profiles and personal information (e.g., who Marines allow to be their "friend" on Facebook and thus allow access to their personal information). Marines 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.**

q. Marines must be careful about which online applications they use, since such applications often have access to a user's personal information (e.g., third-party applications on Facebook).

r. Marines should learn about and use the privacy settings on social media sites.

s. Marines should review their accounts daily for possible use or changes by unauthorized users.

t. Marines should install and maintain current anti-virus and anti-spyware software on their personal computers.

u. For answers to social media questions, Marines should contact their local public affairs office; top level guidance, support and questions can be directed to the appropriate and applicable points of contact listed below:

3. **Points of Contact.** To reduce the likelihood of email spam bot action, the "@" symbol in the e-mail addresses below is represented instead by the word "AT". To email the points of contact below, use the @ symbol instead when pasting the address into your email client.

a. Marine Corps Social Media Office
703-602-3013 or 5193
Marines AT afn.dma.mil

b. Marine Corps Trademark and Licensing Office
703-614-7678
Trademark_Licensing AT USMC.MIL

c. HQMC C4, Information Assurance
703-693-3490
Diane.Clarke AT USMC.MIL

4. **References:**

a. Responsible and Effective Use of Internet-based Capabilities
Directive Type Memorandum 09-026 (DTM 09-026)
http://www.dtic.mil/whs/directives/corres/pdf/DTM-09-026.pdf

b. Joint Ethics Regulation
Department of Defense 5500.7-R
http://www.dod.mil/dodgc/defense_ethics/ethics_regulation/jer1-6.doc

c. Political Activities by Members of the Armed Forces
Department of Defense Directive 1344.10
http://www.dtic.mil/whs/directives/corres/pdf/134410p.pdf

d. Handling Dissident and Protest Activities Among Members of the Armed Forces
Department of Defense Directive 1325.06
http://www.dtic.mil/whs/directives/corres/pdf/132506p.pdf

e. Department of the Navy Privacy Program
Secretary of Navy Instruction 5211.5E
http://doni.daps.dla.mil/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-200%20Management%20Program%20and%20Techniques%20Services/5211.5E.pdf

f. Marine Corps Information Assurance Program

Marine Corps Order 5239.2
http://www.Marines.mil/news/publications/Documents/MCO%205239.2.pdf

g. Clearance of DoD Information for Public Release
Marine Corps Order 5230.18
http://www.Marines.mil/news/publications/Documents/MCO 5230.18.pdf

h. Marine Corps Operations Security Program
Marine Corps Order 3070.2
http://www.Marines.mil/news/publications/Documents/MCO 3070.2.pdf

i. Immediate Ban of Social Networking Sites on the Marine Corps Enterprise Network
MARADMIN 0458/09
http://www.Marines.mil/news/messages/Pages/MARADMIN0458-09.aspx

j. Responsible and Effective Use of Internet Based Capabilities
MARADMIN 181/10
http://www.Marines.mil/news/messages/Pages/MARADMIN181-10.aspx

k. Social Networking Sites Best Practices

http://www.marines.mil/usmc/Documents/SocialMedia/USMC_Social_Networking_Sites_Best_Practices.pdf