[redacted]

From: [redacted]
Sent: Tuesday, November 21, 2006 2:17 PM
To: [redacted]
LTC NETCOM
Subject: FW: FW: Army Revamps How Information Is Deemed Classified (UNCLASSIFIED)

Attachments: FW: Army Revamps How Information Is Deemed Classified

FW: Army Revamps How Informati...

Classification: UNCLASSIFIED

Caveats: NONE

FYI

[redacted]

Web Risk Assessment/Information Assurance Analyst

[redacted]

[redacted]

Sent: Tuesday, November 21, 2006 8:48 AM

[redacted]

Subject: Fwd: FW: Army Revamps How Information Is Deemed Classified

[redacted] - thought this might be of interest.

[redacted]

Classification: UNCLASSIFIED

Caveats: NONE

[redacted]

From: [redacted]
Sent: Tuesday, October 10, 2006 1:04 PM
To: [redacted]

Subject: FW: FW: OPSEC Concern (UNCLASSIFIED)

Classification: UNCLASSIFIED

Caveats: NONE

FYI

[redacted]
Web Risk Assessment/Information Assurance Analyst
[redacted]

[redacted]
Sent: Tuesday, October 10, 2006 12:09 PM
[redacted]
Subject: RE: FW: OPSEC Concern (UNCLASSIFIED)

Thank you for concern and notification. The document in question is our public version (unclassified and redacted) of a recent report. I will let publications know that the small lines through the "secret" markings should be more defined. The front cover of the report does list the correct designation of the document.

[redacted]
Information Systems Security Manager (ISSM)

DHS, Office of Inspector General

[redacted]

-----Original Message-----
[redacted]
Sent: Tuesday, October 10, 2006 11:55 AM
[redacted]

[redacted]

Subject: FW: FW: OPSEC Concern (UNCLASSIFIED)

[redacted]

I received the attached e-mail message from the Army Web Risk Assessment Cell. The below link containing a redacted Secret document was available on the internet. The Army Web Risk Assessment Cell found the link during an OPSEC sweep.

http://www.dhs.gov/interweb/assetlibrary/OIGr_06-58_Aug06.pdf

They wanted to inform DHS that the document was available for unrestricted access on the internet.

V/R

[redacted]

Information Systems Security Officer (ISSO)

DHS/Office of the CIO/Infrastructure Operations

Enterprise Applications Delivery & Operations Security Team Lead

DHS 202-447-0300

Mobile 540-903-3548

[redacted]

[redacted]

Sent: Sunday, October 08, 2006 2:59 PM

[redacted]

Subject: Fwd: FW: OPSEC Concern (UNCLASSIFIED)

Forward to IQ.

[redacted]

Classification: UNCLASSIFIED

Caveats: NONE

[redacted]

From: [redacted]
Sent: Thursday, October 12, 2006 5:19 PM
To: [redacted]
Subject: FW: Good Army News article today (UNCLASSIFIED)

Classification: UNCLASSIFIED

Caveats: NONE

I called [redacted] he Link has been corrected.

[redacted]
Web Risk Assessment/Information Assurance Analyst
[redacted]

[redacted]
Sent: Thursday, October 12, 2006 4:07 PM
[redacted]
Subject: Re: Good Army News article today

[redacted] -- I am going to refer you to the AWRAC government lead, [redacted] and the Lockheed Martin contractor who runs the mission, [redacted] I wrote the articles, but I was reassigned last month and no longer am directly involved with AWRAC. I did start the original AWRAC site on AKO, but it is now administered by [redacted] another LM contractor.

You can reach [redacted] at [redacted] or [redacted] at [redacted]. David can be reached at [redacted].

I have cc'd all of them, and I know they would be happy to answer your specific questions.

[redacted]

----- Original Message -----

From: [redacted]

Date: Thursday, October 12, 2006 3:23 pm

Subject: Good Army News article today

> [redacted] got your name from the AWRAC discussion forum page and
> I assume you are still part of the blog and website monitoring VA
> Guard team. I'm with the AKO program office Outreach office and always
> trying to get people off the .com world and into AKO for their
> operational requirements collaboration and into AKO-S for their
> classified work.
>
> When your team finds a .com site with OPSEC violations is the next
>
> step to tell them about AKO and how it can assist them in meeting
> their portal/collaboration requirement??
>
> PS not sure who wrote the article, but the link to the AKO page is
> incorrect and is being corrected. The correct link is seen when
> clicking on the "Send AKO Link" area on top of the Cyberpatrol page in
> AKO. This is correct format:
> https://www.us.army.mil/suite/page/
> 254224
>
> thanks
>
> [redacted]
> CherryRoad Technologies
> PEO-EIS-AKO Outreach
> [redacted]
>
>
>
>
>
>

Classification: UNCLASSIFIED

Caveats: NONE

[redacted]

From: [redacted]
Sent: Thursday, October 26, 2006 9:43 AM
To: [redacted]
Subject: FW: HOT! CNN Media Query re: Army blog policy (Desire response by 4 p.m. today) (UNCLASSIFIED)

Classification: UNCLASSIFIED

Caveats: NONE

[redacted]

I got this request while I was out yesterday; so no action has been taken. I think we need to get NETCOM PAO and your office on-line to field all questions from the media.

[redacted]
Web Risk Assessment/Information Assurance Analyst
[redacted]

[redacted]
Sent: Wednesday, October 25, 2006 2:43 PM
[redacted]
Subject: HOT! CNN Media Query re: Army blog policy (Desire response by 4 p.m. today) (UNCLASSIFIED)

Classification: UNCLASSIFIED

Caveats: NONE

Sir, request your assistance with the below media query from CNN regarding an Army News Ser article of 12 October. CNN desires to learn if this article was published as a threat or warning? Reporter also desires to learn more about AWRAC. This appears to be an opportunity to educa CNN on the AWRAC. Timeline is very short and I appreciate any assistance that you may offe

Very Respectfully,

[redacted]

[redacted]

[redacted]

Sent: Wednesday, October 25, 2006 2:24 PM

[redacted]

Subject: cnn - army blog policy

Hi Dave,

Thank you for the offer to help!

Here is the article below. I was looking for more info about AWRAC (but the link at the bottom is behind a password) and the VA National Guard Unit. And then it begs to question, was this article published as a notice or warning? (since it's not usual to report about intelligence ops from what I understand)

Thanks again!

[redacted]

CNN Internet Reporter

The Situation Room

[redacted]

http://www4.army.mil/OCPA/read.php?story_id_key=9707

Virginia National Guard eyes Web sites, blogs

By Maj. Pam Newbern
October 12, 2006

WASHINGTON (Army News Service, Oct. 12, 2006) – Big Brother is not watching you, but 10 members of a Virginia National Guard unit might be.

The Manassas-based Virginia Data Processing Unit activated a team in July for one year to scan official and unofficial Army Web sites for operational security violations.

The team, which works under the direction of the Army Web Risk Assessment Cell, Army Office of Information Assurance and Compliance, notifies webmasters and blog writers when they find documents, pictures and other items that may compromise security.

The team uses several scanning tools to monitor sites for OPSEC violations. The tools search for such key words as "for official use only" or "top secret," and records the number of times they are used on a site. Analysts review the results to determine which, if any, need further investigation.

For the 10 Virginia Guardsmen, the mission often becomes personal.

"I have friends over in Iraq, Kuwait and Afghanistan," said Sgt. Yaphet Benton, a network technician in civilian life. "Once I started this mission, I saw a lot of things that can endanger a lot of Soldiers. I see a lot of bios, pictures, names and birthdates. I consider that critical. Terrorists (and persons trying to steal your identity) can use that information."

Based in Arlington, Va., AWRAC was created in 2002 to monitor official Web sites. Its mission was expanded in August 2005 by order of the Army Chief of Staff to include unofficial sites written by servicemembers.

Lt. Col. Stephen Warnock, team leader and battalion commander of the Manassas unit, said his team combines Guardsmen, Reservists and active-duty Soldiers. It's a combination, he notes, that is rarely seen below the division or joint level.

"It's a full Army force – it's a more unique force," he said. "We have quite a flavor to it."

In addition to the Manassas unit, AWRAC works with members of the Guard and Reserve from Washington State, Texas and Maryland, as well as active-duty Soldiers and contractors.

"I see this expanding considerably with the communications tools that are out there now," said Sgt. [illegible] Irwin Walters, who oversees personnel issues for the Manassas unit, and works in the IT

procurement office for the IRS in his civilian life. "I have special concerns about Soldiers leaving their families vulnerable. They are giving up too much information that we know they (the terrorists) are capable of exploiting.

When a team member finds information that could be sensitive, he or she marks it for further investigation. Another team member reviews the item and determines if the webmaster or blog writer should be notified. Most notifications are made by e-mail, and the person responsible is given a few days to respond, depending on the severity of the issue.

When secret documents are found, the site owner is notified immediately by phone. Official sites are contacted through either the webmaster, or in some cases, the unit's chain of command.

The most common OPSEC violations found on official sites are For Official Use Only (FOUO) documents and limited distribution documents, as well as home addresses, birthdates and home phone numbers.

Unofficial blogs often show pictures with sensitive information in the background, including classified documents, entrances to camps or weapons. One Soldier showed his ammo belt, on which the tracer pattern was easily identifiable.

Although AWRAC contacts Soldiers who write unofficial blogs, the team does not review sites that lack public access. Team members identify themselves as AWRAC representatives, and work with a legal counsel to ensure their actions adhere to law and Army regulations.

Members of the DPU bring a variety of specialized skills to the job. Some, like Walters, have extensive technological backgrounds. Others, such as Spec. Shane Newell, are newer to the field, but no less dedicated.

"It's a good opportunity to get some real-world experience," said Newell, a former member of the Old Guard. "I think it's a good mission that needs to be done. It's an ongoing mission."

Benton agreed, saying he accepted the mission in an effort to gain greater technical experience. "It's also a way to contribute to the war on terrorism," he said.

For Sgt. 1st Class Lonny Paschal, the mission reminds him of his time in the Middle East.

"I was a contractor in Iraq, and I would see Soldiers coming back (with pictures of their compounds c weapons)," he said. "I would tell them – you can't publish that. You're compromising yourself and your fellow Soldiers. I do believe that we are saving lives in the long run here."

For more on AWRAC or to request a courtesy scan of a blog, go to the team's Web site on Army Knowledge Online at https://www.us.army.mil/suite/page/254224.

Caveats: NONE

Classification: UNCLASSIFIED

Caveats: NONE

[redacted]

From: [redacted]
Sent: Thursday, October 12, 2006 12:00 PM
To: [redacted]
Subject: FW: IAPM List (UNCLASSIFIED)

Attachments: IAPM List Current.xls

IAPM List Current.xls

Classification: UNCLASSIFIED

Caveats: NONE

[redacted]here is the link to the IAPMs for when you do your notifications.

[redacted]

Web Risk Assessment/Information Assurance Analyst

[redacted]

[redacted]

Sent: Thursday, October 12, 2006 11:50 AM

[redacted]

Subject: IAPM List (UNCLASSIFIED)

Classification: UNCLASSIFIED

Caveats: NONE

\\HQDADFS\Data\Agencies\DISC4\Pnt\Data\C2 Protect Division\OIAC\2b Operations Division\1 Admin\OIA&C Smartbook Files\Rosters and Org Charts\IAPM List Current.xls <file:///\\HQDADFS\Data\Agencies\DISC4\Pnt\Data\C2%20Protect%20Division\OIAC\2b%20Operations%20Division\1 20Admin\OIA&C%20Smartbook%20Files\Rosters%20and%20Org%20Charts\IAPM%20List% 20Current.xls>

[redacted]

Office of Information Assurance and Compliance

Army CIO/G-6, NETCOM

[redacted]

Classification: UNCLASSIFIED

Caveats: NONE

Classification: UNCLASSIFIED

Caveats: NONE

[redacted]

From: [redacted]
Sent: Thursday, February 01, 2007 3:15 PM
To:
Cc: [redacted]

Subject:
Signed By:

Importance: High

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

This is what we suggest as a response to [redacted] (OCPA) reference a media query she received. Do you see any issues with this response.

PROPOSED RESPONSE: The Army Web Risk Assessment Cell's (AWRAC) goal is to review all Army information that is publicly available for violations of Operational Security (OPSEC) which may put Army assets, operations, or people at risk and the posting of privacy information that may lead to identity theft and/or endanger Army personnel or their families.

Do you want to deal with her or do you want us to contact her. Thanks.

[redacted]

-----Original Message-----
[redacted]
Sent: Wednesday, January 31, 2007 5:46 PM
To: NETCOM Army Web Risk Assessment Cell
Subject: Media query on AWRAC (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

I received a query asking about the AWRAC and if it screens opinion or editorial essay-type material of Soldier blogs. I would think yes, but I wanted to check to make sure. Do you have any guidance on this?

[redacted]

[redacted]
Army Public Affairs
1500 Pentagon, RM 1E475
[redacted]

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

From: [redacted]
Sent: Tuesday, August 15, 2006 12:51 PM
To: [redacted]

Subject: FW: Rapid Action Revision of the text changes to DA Pam 25-1-1, Information Technology Support and Services S:31 Aug (UNCLASSIFIED)

Classification: UNCLASSIFIED

Caveats: NONE

FYI

I did a quick review and it looks good. Please see if you have any comments.

[redacted]

Sent: Tuesday, August 15, 2006 11:33 AM

[redacted]

CIO/G-6/SAIC
Subject: Rapid Action Revision of the text changes to DA Pam 25-1-1, Information Technology Support and Services S:31 Aug (UNCLASSIFIED)

Classification: UNCLASSIFIED

Caveats: NONE

ALCON:

Located on AKO for your review/comment(s), is the rapid action revision of the text changes to DA Pam 25-1-1, Information Technology Support and Services. View the text changes and comment sheet by going to the AKO link provided below.

https://www.us.army.mil/suite/folder/6032440

Please provide your comments NLT 31 August 06.

[redacted] of the fields on the comment sheet, being specific to list the page, paragraph, and

line to which you refer and return comment sheet via email to the undersigned. If your organization has no comments, a negative reply is still required in order to confirm that you received / reviewed this publication. For reference purposes, the current version of DA Pam 25-1-1 can be viewed at the following link:

http://www.army.mil/usapa/epubs/pdf/p25_1_1.pdf

If you have any questions regarding the document please don't hesitate to contact me.

V/R

[redacted]@hqda.army.mil

CIO Policy Division, Army CIO/G6

Support Contractor SAIC

[redacted]

Classification: UNCLASSIFIED

Caveats: NONE

Classification: UNCLASSIFIED

Caveats: NONE

[redacted]

From: [redacted]
Sent: Tuesday, May 16, 2006 10:57 AM
To: [redacted]
Subject: FW: The Cell (UNCLASSIFIED)

Attachments: The Cell.doc

The Cell.doc

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]
Information Assurance Directorate NETC-EST-A
Army Web Risk Assessment Cell
[redacted]

-----Original Message-----
[redacted]
Sent: Monday, November 21, 2005 11:33 AM
[redacted]
Subject: FW: The Cell

Final version

-----Original Message-----
[redacted]
Sent: Monday, November 21, 2005 7:34 AM
[redacted]
Subject: The Cell

Resend.
<<The Cell.doc>>
Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

From: [redacted]
Sent: Thursday, October 26, 2006 1:37 PM
To: [redacted]
NETCOM/LMH
Subject: FW: Waiver Issue?: (UNCLASSIFIED)
Signed By: [redacted]

Attachments: Army Chief of Staff Urges Increased Vigilance on Operational Security.htm

Army Chief of Staff Urges Incr...

Classification: UNCLASSIFIED

Caveats: NONE

FY I

[redacted]
Web Risk Assessment/Information Assurance Analyst
[redacted]

[redacted]
Sent: Thursday, October 26, 2006 1:25 PM
[redacted]
CIO/G6
Subject: RE: Waiver Issue?: (U) (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

In answer to your question regarding the web risk assessment to the Army, I have compiled th following information. Attached you will find a CSA memo that specifically identifies that need for web risk assessment. "HQDA G-6 (IN COORDINATION WITH G-2) IS DIRECTED TO TRACK AI REPORT, ON A QUARTERLY BASIS, OPEN SOURCE OPSEC VIOLATIONS."

The Army views all open source web pages that are available to the public for any security violations. We use the NIPRNet (DISN) to complete a google search. One reason for using the NIPRNet is it is financially economical for the Army.

The Air Force uses both the NIPRNet and commercial ISP.

I can not speak for the Navy; however, it is my understanding that they have chosen to use the ".com" means for the same purpose. I do not know of their justification for the commercial vice DISN capability. If OSD is looking for consistency - I would say that the Navy can also use the NIPRNet for their web risk assessment the same as the USAF and Army.

<<...>>

Regards,

[redacted]
US Army CIO/G6 FCI
[redacted]

[redacted]
Sent: Wednesday, October 25, 2006 2:20 PM
To: [redacted] DISA GIG-CS
Subject: Waiver Issue?: (U)

UNCLASSIFIED

[redacted]

"The Army Web Risk Assessment Cell, Army Office of Information Assurance and Compliance, opened a Virginia Data Processing Unit that has activated a team to scan official and unofficial Army Web sites for operational security violations."

Are either of you aware of how the Army is conducting their web risk assessment. The Navy has a team doing the same thing but they require a waiver. Is the Army performing that function on the DISN? Seems to be an inconsistency there and/or a best practices that needs to be shared.

[redacted]

Classification: UNCLASSIFIED
Caveats: NONE

Classification: UNCLASSIFIED

Caveats: NONE

[redacted]

From: [redacted]
Sent: Monday, July 17, 2006 8:52 AM
To: [redacted]
Subject: letters (UNCLASSIFIED)
Signed By: [redacted]

Attachments: new web letter.doc; Memorandum web site findings.doc


new web letter.doc


Memorandum web site findings.d...

Classification: UNCLASSIFIED

Caveats: NONE

<<...>> <<...>>

Classification: UNCLASSIFIED
Caveats: NONE

1. The Army Web Risk Assessment Cell (AWRAC) is currently reviewing U.S. Army Web sites for OPSEC and security compliance. An OPSEC concern was found on your organization's website. The OPSEC concern for your organization's website has been classified as a Major finding. Major findings are generally defined as information that in itself or in aggregation is or should be FOR OFFICIAL USE ONLY (FOUO), or is typically FOUO as defined in Part V of the DoD Web Site Administration Policies and Procedures Guide. Notification to affected unit/organization is within the next duty day. Required response time for website managers is 72 hours.

2. You have been identified as the commander/ supervisor/ POC for the website in question. We recommend you review the attached OPSEC finding SITREP assessment and take appropriate remedial actions e.g., questionable material is removed or password protected. In addition to the SITREP you received from the ARWAC, we highly recommend you initiate an immediate review of all material on your website for Operations Security (OPSEC) and proper security procedures IAW DoD and Army policy so that your command is not providing information depicting unit capabilities, limitations and intentions. Army Regulation 25-1 specifies a quarterly review for OPSEC be conducted. Commanders have been directed by HQDA Message (122240Z MAR 03) to ensure their websites do not provide questions about friendly intentions and military capabilities likely to be asked by enemy planners and decision makers.

3. To assist in the OPSEC review process for web content, we recommend a review of the "Web Site Policies http://www.defenselink.mil/webmasters/ and the Webmaster Training Course at https://iatraining.us.army.mil

4. Please acknowledge receipt of this email NLT 15 DEC 2004, and forward to your respective commander/supervisor or their designated representative responsible for the site. Let us know if you have any questions concerning our review and/or current DA or OSD directives and policies concerning OPSEC, FTP and Web site administration. Thank you for your assistance.

DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

Office, Chief Information Officer / G6

NETC-EST-A

S: March 22, 2002

March 11, 2002

MEMORANDUM FOR WEB SITE ACTIVITY COMMANDER/SUPERVISOR

SUBJECT: Web Risk Assessment Findings

1. References:

a. DoDI 5230.29 Security and Policy Review of DoD Information for Public Release, 6 March 1996
b. Memorandum, Deputy Secretary of Defense, dated 24 September 1998, Information Vulnerability and the World Wide Web.
c. Memorandum, Assistant Secretary of Defense, dated 28 December 2001, Removal of Personally Identifying Information of DOD Personnel from Unclassified Websites

2. On 9-10 March 2002, the Headquarters, Department of the Army, Information Assurance Office (NETC-EST-A) Web Risk Assessment Cell conducted an assessment of -your web site (WWW...). Also evaluated was your required registration with the Government Information Locator Service (GILS). GILS Identifies public information resources throughout the U.S. Federal Government, describe the information available in those resources, and provide assistance in obtaining the information. The following registration and security concerns were noted and rated by category (see below).

CATEGORY	WEB ADDRESS	FINDING	REFERENCE	

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g., questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report

security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to acknowledge receipt via email to the AWRAC [redacted]da.army.mil) and forward the memorandum to the commander/ supervisor, or his/her designated representative, responsible for the website. Suspense dates for corrective actions/resolution of security concerns are provided in the memorandum. Copies of this memorandum will be furnished to the appropriate MACOM, PEO, IAPMs.

4. The Department of Defense has mandated that DoD websites be made available to the public and provide accurate and timely information relating to its activities, objectives, policies, and programs. At the same time we must ensure the information provided does not compromise the security of our nation or the privacy of service members and there families.

5. Definitions:

a. CRITICAL: Information that is either classified or, when combined with other sensitive information, may have significant operational impact. It is information that could put either personnel or facilities at risk.

b. MAJOR: Information in itself or in aggregation that is FOR OFFICIAL USE ONLY (FOUO).

c. MINOR: All other violations that do not fall in either of the above two categories. Information, which may not be posted, on official web sites open to public access. Also, information that is contrary to the web policy guidance. (Note: Commanders may elect to assume this level of risk.)

6. POC: Mr. [redacted] Army Web Risk Assessment Analyst, COM: 717-865-1785,
Email: [redacted]ARMY.MIL

THADDEUS A. DMUCHOWSKI
COL, GS
Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

SAIS-IOA
Subject: Web Risk Assessment Findings

WEB SITE CONTENT GUIDANCE

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures with 11January 2002 amendments

Memorandum, Office of the Secretary of Defense, July 13, 2000, Subject: Privacy Policies and Data Collection of DOD Public Web Sites

Memorandum, Deputy Secretary of Defense, 24 September 1996, Subject: Information Vulnerability and the World Wide Web

Memorandum, Office of Management and Budget, June 22, 2000, Subject: Policies and Data Collection of Federal Web Sites

DOD Directive 5230.29, "Security and Policy Review of DOD Information for Public Release," May 6, 1996

DOD Directive 5230.9, "Clearance of DOD Information for Public Release," April 9, 1996

Memorandum, Office of the Director of Information Systems for Command Control, Communications, and Computers (DISC4), 30 November 1998, Subject: Guidance for Management of Publicly Accessible U.S. Army Websites

Army Regulation (AR) 25-1, 4 August 1999, Army Information Management

Army Regulation (AR) 380-5, 29 September 2000, Department of the Army Information Security Program

Army Regulation (AR) 380-19, 27 February 1998, Information Systems Security

P 231903Z AUG 05
FM DA WASHINGTON DC//DACS-ZA//
TO ALARACT
ZEN/ADDRESS LISTS @ AL ALARACT(UC)
BT
UNCLAS ALARACT 156/2005

SUBJECT: CHIEF OF STAFF OF THE ARMY OPSEC GUIDANCE

CSA SENDS:
PASS TO ALL ARMY LEADERS.

REF//A//MSG/ALARACT/141637Z FEB 05/SUBJ: SENSITIVE PHOTOGRAPHS (U/FOUO)

1. (U//FOUO) OPSEC IS A CHAIN OF COMMAND RESPONSIBILITY. IT IS SERIOUS BUSINESS AND WE MUST DO A BETTER JOB ACROSS THE ARMY. THE ENEMY AGGRESSIVELY "READS" OUR OPEN SOURCE AND CONTINUES TO EXPLOIT SUCH INFORMATION FOR USE AGAINST OUR FORCES. SOME SOLDIERS CONTINUE TO POST SENSITIVE INFORMATION TO INTERNET WEBSITES AND BLOGS, E.G., PHOTOS DEPICTING WEAPON SYSTEM VULNERABILITIES AND TACTICS, TECHNIQUES, AND PROCEDURES. SUCH OPSEC VIOLATIONS NEEDLESSLY PLACE LIVES AT RISK AND DEGRADE THE EFFECTIVENESS OF OUR OPERATIONS.

2. (U//FOUO) THIS IS NOT THE FIRST TIME THIS ISSUE HAS SURFACED. THE VICE CHIEF OF STAFF OF THE ARMY PREVIOUSLY ADDRESSED THIS VIA MESSAGE IN FEBRUARY 2005. TAKE A HARD LOOK AT HIS GUIDANCE.

3. (U//FOUO) LEADERS AT ALL LEVELS MUST TAKE CHARGE OF THIS ISSUE AND GET THE MESSAGE DOWN TO THE LOWEST LEVELS. TO ASSIST YOU, THE HQDA G-2 AND THE OPSEC SUPPORT ELEMENT ARE DEVELOPING A TRAINING MODULE AND ARE FORMING A MOBILE TRAINING TEAM TO ASSIST IN TRAINING YOUR SOLDIERS. DETAILS WILL BE PROVIDED NLT 2 SEPTEMBER 2005. HQDA G-6 (IN COORDINATION WITH G-2) IS DIRECTED TO TRACK AND REPORT, ON A QUARTERLY BASIS, OPEN SOURCE OPSEC VIOLATIONS. AN INTERIM CHANGE TO AR 530-1, OPERATIONS SECURITY, WILL BE PUBLISHED VIA MESSAGE WITHIN 30 DAYS WHICH WILL CONTAIN CLEAR POLICY CONCERNING THE POSTING OF SENSITIVE PHOTOS AND INFORMATION ON THE INTERNET.

4. (U//FOUO) GET THE WORD OUT AND FOCUS ON THIS ISSUE NOW. I EXPECT TO SEE IMMEDIATE IMPROVEMENT.

5. (U//FOUO) EXPIRATION DATE OF THIS ALARACT IS UNDETERMINED.

PETER J. SCHOOMAKER, GEN, CSA

==========

DTG: 141637Z Feb 05

SUBJECT: (U) SENSITIVE PHOTOS (U//FOUO)

PASS TO ALL ARMY LEADERS O5 (LTC) OR EQUIVALENT AND ABOVE.

1. (U//FOUO) THE ENEMY IS ACTIVELY SEARCHING THE UNCLASSIFIED NETWORKS FOR INFORMATION, ESPECIALLY SENSITIVE PHOTOS, IN ORDER TO OBTAIN TARGETING DATA, WEAPONS SYSTEM VULNERABILITIES, AND TTPs FOR USE

AGAINST THE COALITION. A MORE AGGRESSIVE ATTITUDE TOWARD PROTECTING FRIENDLY INFORMATION IS VITAL TO MISSION SUCCESS. THE ENEMY IS A PRO AT EXPLOITING OUR OPSEC VULNERABILITIES.

2. (U//FOUO) IT IS CRITICAL TO REMIND OUR PEOPLE THAT THE NEGLIGENT OR UNAUTHORIZED RELEASE OF SENSITIVE PHOTOS IS A SERIOUS THREAT TO OUR FORCES. LEADERS ARE ENCOURAGED TO:

2.A. (U//FOUO) REMIND ALL PERSONNEL THAT THE ENEMY WILL EXPLOIT SENSITIVE PHOTOS SHOWING THE RESULTS OF IED STRIKES, BATTLE SCENES, CASUALTIES, DESTROYED OR DAMAGED EQUIPMENT, AND ENEMY KIAs AS PROPAGANDA AND TERRORIST TRAINING TOOLS. FOR EXAMPLE, ANNOTATED PHOTOS OF AN ABRAMS TANK PENETRATED BY AN RPG ARE EASILY FOUND ON THE INTERNET. CAPTURED INSURGENT PAMPHLETS CONTAIN HAND DRAWINGS AND INSTRUCTIONS ON WHAT INSURGENTS BELIEVE ARE VULNERABLE PENETRATION POINTS ON TANKS, HMMWVS, BRADLEY FIGHTING VEHICLES, AND HELICOPTERS. RELEASING PHOTOS OUTSIDE OFFICIAL, PROTECTED CHANNELS MAY ALLOW THE ENEMY MATERIAL FOR HIS INFORMATION OPERATIONS AND TARGETING TTP AGAINST FRIENDLY FORCES. INSURGENTS ALSO USE WEBSITES TO COMMUNICATE, TRAIN, AND RECRUIT FOLLOWERS, OFTEN USING PHOTOS/VIDEO OF THEIR BATTLEFIELD SUCCESSES. WE CANNOT AFFORD TO HAVE OUR PHOTOS BECOME TRAINING AND RECRUITMENT TOOLS FOR THE ENEMY.

2.B. (U//FOUO) INFORM YOUR PERSONNEL THAT WE COULD UNWITTINGLY MAGNIFY ENEMY CAPABILITIES SIMPLY BY EXCHANGING PHOTOS WITH FRIENDS, RELATIVES, OR BY PUBLISHING THEM ON THE INTERNET OR OTHER MEDIA. WE ARE NOT LIMITING AUTHORIZED COMMUNICATION (TO INCLUDE THE APPROPRIATE USE OF PHOTOS) UNDER EXISTING PUBLIC AFFAIRS GUIDANCE, BUT WE MUST PROTECT PHOTOS THAT REVEAL TO THE ENEMY OUR BATTLE LOSSES, ONGOING FRIENDLY OPERATIONS, TTP, EQUIPMENT VULNERABILITIES, OR DISCLOSE INTELLIGENCE COLLECTION EFFORTS AND METHODS. MOREOVER, WE MUST PROTECT INFORMATION THAT MAY HAVE A NEGATIVE IMPACT ON FOREIGN RELATIONS WITH COALITION ALLIES OR WORLD OPINION.

3. (U//FOUO) OUR MISSION SUCCESS AND SOLDIERS LIVES DEPEND ON AGGRESSIVELY DENYING THE ENEMY ANY ADVANTAGE. I NEED YOUR FOCUS ON THIS CRITICAL ISSUE.

4. (U//FOUO) EXPIRATION DATE OF THIS ALARACT CANNOT BE DETERMINED.

RICHARD A. CODY, GEN, VCSA

DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

Office, Chief Information Officer / G6

SAIS-IOA

S: March 22,2002

March 11, 2002

MEMORANDUM FOR WEB SITE ACTIVITY COMMANDER/SUPERVISOR

SUBJECT: Web Risk Assessment Findings

1. References:

a. DoDI 5230.29 Security and Policy Review of DoD Information for Public Release, 6 March 1996
b. Memorandum, Deputy Secretary of Defense, dated 24 September 1998, Information Vulnerability and the World Wide Web.
c. Memorandum, Assistant Secretary of Defense, dated 28 December 2001, Removal of Personally Identifying Information of DOD Personnel from Unclassified Websites

2. On 9/10 March 2002, the Headquarters, Department of the Army, Chief Information Officer (CIO)/G-6 Web Risk Assessment Cell conducted an assessment of your web site (WWW...). Also evaluated was your required registration with the Government Information Locator Service (GILS). GILS Identifies public information resources throughout the U.S. Federal Government, describes the information available in those resources, and provides assistance in obtaining the information. The following registration and security concerns were noted and rated by category (see below).

CATEGORY	WEB ADDRESS	FINDING	REFERENCE	

3. The AWRAC program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g., questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report security concerns via e-mail

SAIS-IOA
Subject: Web Risk Assessment Findings
memorandum to the point of contact (POC) posted on the website. Website POCs are directed to acknowledge receipt via email to the AWRAC (XXXXXXXXXXXXXXXXXXXX) and forward the memorandum to the commander/ supervisor, or his/her designated representative, responsible for the website. Suspense dates for corrective actions/resolution of security concerns are provided in the memorandum. Copies of this memorandum will be furnished to the appropriate MACOM, PEO, PM IAPMs

4. The Department of Defense has mandated that DoD websites be made available to the public and provide accurate and timely information relating to its activities, objectives, policies, and programs. At the same time we must ensure the information provided does not compromise the security of our nation or the privacy of service members and there families.

5. Definitions:

a. CRITICAL: Information that is either classified or, when combined with other sensitive information, may have significant operational impact. It is information that could put either personnel or facilities at risk.

b. MAJOR: Information in itself or in aggregation that is FOR OFFICIAL USE ONLY (FOUO).

c. MINOR: All other violations that do not fall in either of the above two categories. Information, which may not be posted, on official web sites open to public access. Also, information that is contrary to the web policy guidance. (Note: Commanders may elect to assume this level of risk.)

6. POC: Mr. [redacted] Army Web Risk Assessment Analyst, COM: 703-602-2500 (DSN: 332), Email: [redacted].ARMY.MIL

THADDEUS A. DMUCHOWSKI
COL, GS
Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

M-05-04
MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES
FROM: Clay Johnson III
Deputy Director for Management
SUBJECT: Policies for Federal Agency Public Websites

The efficient, effective, and appropriately consistent use of Federal agency public websites is important to promote a more citizen centered government. This memorandum and attachment fulfill the requirements of section 207(f) of the E-Government Act of 2002 (Pub. L. No. 107-347). Overall, the management of agencies' public websites should be in compliance with Federal information resource management law and policy.

Publicly accessible Web site (or public Web site) on the World Wide Web
Army Web site with access unrestricted by password or PKI user authorization. "Public" refers to the at-large audience on the Internet; anyone who can access a Web site through a browser.

Federal agency public websites are information resources funded in whole or in part by the Federal government and operated by an agency, contractor, or other organization on behalf of the agency. They present government information or provide services to the public or a specific non-Federal user group and support the proper performance of an agency function. Federal agency public websites are also information dissemination products as defined in Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources." Agencies must manage Federal agency public websites as part of their information resource management program following guidance in OMB Circular A-130, OMB "Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies" (67 FR 5365), this memorandum, and other information policy issuances.

OMB expects prompt and orderly implementation of the policies in this memorandum and its attachment. OMB expects agencies to become fully compliant with new requirements by 12/31/05 and continue to adhere to existing requirements. OMB will monitor agency compliance with these policies as part of its oversight of agency information resource management programs. The recommendations and best practices published by the Interagency Committee on Government Information (http://www.webcontent.gov) will aid your implementation of the policies outlined in the attachment.

If you have any questions regarding this memorandum, please contact Kimberly Nelson (202) 395-3787 Knelson@omb.eop.gov, or Daniel Costello (202) 395-7857 Dcostell@omb.eop.gov, Policy Analysts, Information Policy and Technology Branch, Office of Management and Budget.
Attachment

Attachment

Policies for Federal Agency Public Websites

2-1 e. Implement the policy and procedures mandated by—
(1) P. L. 105–277 (Title XVII—The Government Paperwork Elimination Act).
(2) Title 15, Section 7001, United States Code (15 USC 7001) (2000), Electronic Signatures in Global and National
Commerce Act (also known as the "E–Sign Act").
(3) 44 USC, Chapter 35, Coordination of Federal Information Policy (P.L. 104–13, Paperwork Reduction Act of 1995).
(8) P.L. 107–347, E–Government Act of 2002.

3–9. Registry for major information systems inventory, reduction, webification, and security AR25-1c(1) *Information system inventory. c. Information system inventory.*
(1) Per the E–Government Act of 2002 (P.L. 107–347), the Army is required to annually maintain an inventory of
mission critical (MC) and mission essential (ME) systems and certify its accuracy and completeness. This list of
systems becomes part of the DOD IT registry, which is used by OSD and entities outside of OSD for budget and other
Congressional issues.

1. Establish and Maintain Information Dissemination Product Inventories, Priorities, and Schedules

   A. Your agency is already required under OMB Circular A-130 and the Paperwork Reduction Act to disseminate information to the public in a timely, equitable, efficient, and appropriate manner1 and to maintain inventories of information dissemination products.

   B. Section 207 of the E-Government Act2 requires your agency to develop priorities and schedules for making Government information available and accessible to the public, in accordance with public comment, and to post this information on your agency's website. Section 207 also requires your agency to report to OMB, as part of the agency's annual E-Government Act report, the final determinations of inventories, priorities, and schedules your agency has made.

   C. Your agency must also post to your agency's website any updates to your agency's final determination of inventories, priorities, and schedules, and include this information in your agency's annual E-Government Act report.

2. Ensure Information Quality

1–12. Ensuring quality of information disseminated to the public
AR25-1-12a

   A. Your agency is already required under the Information Quality Act and associated guidelines3 to maximize the quality, objectivity, utility, and integrity of information and services provided to the public. This includes making information and services available on a timely and equitable basis.

B. Agencies must reasonably assure suitable information and service quality, consistent with the level of importance of the information. Reasonable steps include: 1) clearly identifying the limitations inherent in the information dissemination product (e.g., possibility of errors, degree of reliability, and validity) so users are fully aware of the quality and integrity of the information or service, 2) taking reasonable steps to remove the limitations inherent in the information, and 3) reconsidering delivery of the information or services.

3. Establish and Enforce Agency-wide Linking Policies Covered in AR25-1 6-4
n. Internet (World Wide Web (WWW)), intranets, and extranets.
AR25-1 6-4n(15)

A. Agencies must now establish and enforce explicit agency-wide linking policies describing management controls for linking within and beyond the agency.
B. These policies must appropriately limit external linking to information or services necessary for the proper performance of an agency function.
C. Agency linking policies must also include reasonable management controls to assure external links remain active or otherwise continue to provide the level of quality (including objectivity, utility, and integrity) as intended by the agency and expected by users.
1 OMB Circular A-130, "Management of Federal Information Resources," section 8 (a)(5) available at http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf; see also, The Paperwork Reduction Act available at http://www.archives.gov/federal_register/public_laws/paperwork_reduction_act/3501.html
2 E-Government Act of 2002, Pub. L. No. 107-347, section 207(f)(2).
3 Information Quality Act, Pub. L. No. 106-554, section 515; see also, "Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies" (67 FR 5365) and your agency's Information Quality Act guidelines.

D. OMB's Information Quality guidelines exclude hyperlinks from the definition of information. This exclusion does not remove agency responsibility to exercise due diligence when determining whether to link externally. Therefore, when an agency determines external links are necessary for and material to the presentation of agency information or the delivery of services in the proper performance of an agency function, they must take reasonable steps to ensure the presentation is accurate, relevant, timely, and complete.
E. Agencies must reasonably assure suitable information and service quality, consistent with the level of importance of the information. Reasonable steps include: 1) clearly identifying the limitations inherent in the information dissemination product (e.g., possibility of errors, degree of reliability, and validity) so users are fully aware of the quality and integrity of the information or service, 2) taking reasonable steps to remove the limitations inherent in the information, and 3) reconsidering linking to the information or services. Agency links to commercial organizations or interest groups present special challenges with respect to maintaining agency objectivity and thus must be used judiciously.

F. Agency linking policies must identify mandatory links and post (or link to) the following information on their principal website and any known major entry points to their sites: 1) the agency's strategic plan and annual performance plans; 2) descriptions of agency organizational structure, mission and statutory authority; 3) information made available under the Freedom of Information Act; 4); specific website privacy policies; 5) FirstGov.gov; 6) summary statistical data about equal employment opportunity complaints filed with the agency and written notification of "Whistleblower" rights and protections as required by the No Fear Act of 2002; 7) the agency point of contact for small businesses as required by the Small Business Paperwork Relief Act of 2002; and 8) other cross-government portals or links required by law or policy.

4. Communicate with the Public, State, and Local Governments.

A. Your agency is already required under OMB Circular A-1304 to establish and maintain communications with members of the public and with State and local governments to ensure your agency creates information dissemination products meeting their respective needs.

B. Your agency is already required under the Paperwork Reduction Act to manage information collections from the public or State and local governments (including website surveys or questionnaires) in the manner prescribed in OMB's guidance in 5 CFR section 1320. For additional information see: http://www.access.gpo.gov/nara/cfr/waisidx_99/5cfr1320_99.html

5. Search Public Websites.

Covered in AR25-1 **8–6g. General policies May need to add site map requirement**

A. You are already required under OMB Circular A-130 to assist the public in locating government information.5

B. You must now ensure your agency's principal public website and any major entry point include a search function. However, agencies may determine in limited circumstances (e.g., for small websites) site maps or subject indexes are more effective than a typical search function.

4 OMB Circular A-130, "Management of Federal Information Resources," section 8 (a)(6) available at http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf; see also, The Paperwork Reduction Act available at http://www.archives.gov/federal_register/public_laws/paperwork_reduction_act/3501.html

5 Id. at section 8 (a)(5).

C. By December 31, 2005, this search function should, to the extent practicable and necessary to achieve intended purposes, permit searching of all files intended for public use on the website, display search results in order of relevancy to search criteria, and provide response times appropriately equivalent to industry best practices.

D. By December 31, 2005, agency public websites should to the extent practicable and necessary to achieve intended purposes, provide all data in an open, industry standard format permitting users to aggregate, disaggregate, or otherwise manipulate and analyze the data to meet their needs.
E. Agencies should note the Interagency Committee on Government Information has provided to OMB recommendations for organizing, categorizing, and searching for government information. By December 17, 2005, OMB will issue any necessary additional policies in this area.

6. Use Approved Domains.
6-4n(11) All Army private (nonpublicly accessible) Web sites must be located on a ".mil" domain.

Need to change to all web sites and get waver from the secretary of Defense.

A. Your agency must use only .gov, .mil, or Fed.us domains unless the agency head explicitly determines another domain is necessary for the proper performance of an agency function.
B. This requirement recognizes the proper performance of agency functions includes an obligation for clear and unambiguous public notification of the agency's involvement in or sponsorship of its information dissemination products including public websites. It also recognizes in certain limited circumstances other domains may be necessary for the proper performance of an agency function.

7. Implement Security Controls.
A. Your agency is already required to implement security policies in OMB Circular A-130, Appendix III; OMB memorandum M-04-25, "Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting;" National Institute of Standards and Technology (NIST) Special Publication 800-44, "Guidelines on Securing Public Web Servers;" and other associated guidance from NIST. For additional information see:
http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html,
http://csrc.nist.gov/policies/FISMA-final.pdf,
http://www.whitehouse.gov/omb/memoranda/fy04/m04-25.pdf,
http://csrc.nist.gov/publications/nistpubs/800-44/sp800-44.pdf
B. Your agency is already required to provide adequate security controls to ensure information is resistant to tampering to preserve accuracy, remains confidential as necessary, and the information or service is available as intended by the agency and expected by users. Agencies must also implement management controls to prevent the inappropriate disclosure of sensitive information.

8. Protect Privacy. AR25-2 and 25-1 6-4 and 5-1
A. Your agency is already expected to protect the privacy of information about members of the public by continuing to implement OMB Circular A-130 Appendix I and OMB memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002." For additional information see:
http://www.whitehouse.gov/omb/memoranda/m03-22.html

9. Maintain Accessibility. AR25-16-4n(13)

A. Your agency is already required to ensure accessibility for individuals with disabilities by implementing Section 508 of the Rehabilitation Act (29 U.S.C. 794d). Federal agency public websites must be designed to make information and services fully available to individuals with disabilities. For additional information see: http://www.access-board.gov/index.htm

B. Your agency is already required to provide appropriate access for people with limited English proficiency by implementing Department of Justice guidance for Executive Order 13166, "Improving Access to Services for People with Limited English Proficiency." Agencies must determine whether any individual document on their Federal agency public website(s) requires translation. For additional information see: http://www.usdoj.gov/crt/cor/Pubs/lepqa.htm

10. Manage Records. Ar25-1 2-28 d and 6-2c

AR25-1 **Chapter 8**

Records Management Policy

A. You are already required to meet records management requirements by implementing OMB Circular A-130 and guidance from the National Archives and Records Administration. See 36 Code of Federal Regulations (CFR), Parts 1220-1238). For additional information see: http://www.archives.gov/records_management/index.html

[redacted]

From: [redacted]
Sent: Monday, October 23, 2006 12:25 PM
To: [redacted]

Subject: [redacted] Article (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

Look who picked up [redacted] Article.

http://www.sofmag.com/news/permalink/2006/10/13/0944533637595.html

[redacted]
Web Risk Assessment/Information Assurance Analyst
[redacted]

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

From: [redacted]
Sent: Monday, October 23, 2006 9:50 AM
To: [redacted]
Subject: policy (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

I am checking on the other letter, but these two should help.

http://www.defenselink.mil/webmasters/policy/dod_web_policy_12071998_with_amendments_and_corrections.html
Part I para 5.4 to 5.8

http://www.dtic.mil/whs/directives/corres/pdf/i523029_080699/i523029p.pdf

[redacted]
Web Risk Assessment/Information Assurance Analyst
[redacted]

Classification: UNCLASSIFIED
Caveats: NONE

-----Original Message-----
From: [redacted]
Sent: Thursday, August 23, 2001 11:08 AM
To: DISC4 Army CIO Executive Board; DISC4 MACOM IAPMs
Cc: [redacted]

Subject: Reverse Proxy Server Policy
Importance: Low

Reference SecArmy/Chief of Staff Army (CSA) Memorandum dated 8 August 2001, Subject: Army Knowledge Management (AKM) Guidance Memorandum Number 1.

1. Attacks on our computer networks are becoming increasingly more sophisticated. The recent Code Red worm is no exception. The automated attack features of the Code Red worm both confirm and warn us that we can expect more sophisticated and malicious payloads in the future. For Code Red, the Defense Information Systems Agency (DISA) was forced to shut down most access to DoD web pages (Inbound Port 80 traffic) from outside the NIPRNET in order to prevent an overload of our unclassified networks. As a result, many important functions, such as E-business, that requires INTERNET access were disrupted. While INTERNET access to Army web pages is now partially restored, in the future we can expect more disruptions unless protective measures are implemented.

2. To immediately increase our protective posture, this message directs that all mission essential, publicly accessible, Army web sites (e.g., sites that must be accessed from the INTERNET that can be affected by another Port 80 shut down) will be protected behind a currently operational, Army Computer Emergency Response Team (ACERT) certified Army "reverse web proxy server." The following instructions will be supplemented by more detailed implementing instructions issued by the ACERT/Army Network Operations and Security Center (ANOSC).

A. By 28 August 2001 MACOM and PEO/PM IAPMs will provide the ACERT with a prioritized list of all mission-essential web servers that must be accessed from the INTERNET. The list will identify which web sites are not protected as well as those already protected behind a "reverse web proxy server." Any web server that for technical reasons cannot be put behind a proxy server will be evaluated by the ACERT and ANOSC. The ACERT will recommend to the web site owner alternative security procedures necessary to protect the web server that must be implemented before INTERNET access to the web server will be allowed.

B. After 7 September 2001 the ANOSC/ACERT will begin shutting down INTERNET (Inbound Port 80 traffic) access at all Army security routers. As a result, Army web sites not behind proxy servers or otherwise protected with an approved alternative security solution, will not be available to personnel outside

the NIPRNET (the ".mil" domain).

C. Before a web server is put behind a proxy server or is allowed to be accessed from the INTERNET utilizing an alternative security solution, the following actions must be accomplished:

(1) MACOMs and PEOs/PMs must install all (not just Code Red) IAVA fixes for their server(s) before submitting them to the ACERT for connection behind a "reverse web proxy server." The ACERT will scan the system(s) to verify that all fixes are in place. Systems that are not IAVA compliant for all IAVAs will not be put behind the proxy server and INTERNET access will not be allowed until compliance is verified.

(2) The web site must be registered in accordance with Army and DoD web policy on the Government Information Locator Service (GILS) web page, <http://sites.defenselink.mil>. MACOM and PEO/PM IA Program Managers must state that that GILS registration (registration takes 5-10 days to complete) has been initiated when the web site is submitted to the ACERT.

(3) Joint Task Force Computer Network Operations (JTF-CNO) requires all technical points of contact (system administrators) for all web sites be identified to the ACERT. To accomplish this, web site system administrators must register to the IAVA Compliance Reporting Database before a web site is put behind a proxy server or otherwise protected (see paragraph 4 and <https://information>assurance.us.army.mil for further information).

3. Beyond the immediate fixes outlined above, this message directs development, not later than 30 August 2001, of an Army enterprise-wide, centrally managed, reverse web proxy server acquisition and consolidation plan to protect all Army publicly accessible web sites. The plan will be developed in accordance with (IAW) and to support goals 1,3, and 4 of reference above. The HQDA, ODISC4, IA Office will contact selected MACOMs and PEOs/PMs to assist in developing and funding the centrally managed, web proxy server enterprise consolidation strategy. The POCs for this action are LTC John Quigg, phone (703) 604-8377 (DSN 664), email: <mailto:john.quigg@hqda.army.mil> and Roy Lundgren, phone (703) 604-7579 (DSN 664), email: mailto:leroy.lundgren@hqda.army.mil.

4. Finally, we must fix what we know is broken and that is compliance with ACERT issued Information Assurance Vulnerability Alert (IAVA) messages. IAVA requires the personal involvement of commanders at all levels in taking charge of how well their commands implement the Army's IAVA process. The Army currently has the highest rate of Code Red infections. Much of this is a "self-inflicted wound." On 21 June 2001 the ACERT identified the vulnerability that Code Red exploits and published an IAVA message that mandated the fix that all MACOM and PEO/PM system administrators were required to complete.

This did not happen and now we are attempting to recover from damage and disruption caused by organizations that failed to comply with the IAVA process. I ask commanders at all levels direct their IA Program Managers/Officers to brief them on their command's IAVA compliance status. By 14 September 2001, I will send an Army CIO message directing the use of a consolidated, enterprise-wide IAVA compliance and critical infostructure reporting database. This database will not only assist commanders in achieving greater accountability in reporting IAVA compliance, but will provide the Army, its MACOMs, and PEOs/PMs with a more accurate assessment of critical infostructure assets and training, e.g., types of servers and the training status of our information technology (IT) professionals. The Army POCs for the IAVA/critical infostructure asset reporting database are Ron Sturmer, phone (703) 604-6870 (DSN 664), email: <mailto:ronald.sturmer@hqda.army.mil> and Ralph Lowenthal, phone 607-5886 (DSN 327), email: <mailto:ralph.lowenthal@hqda.army.mil>.

5. Some commands "may" have obtained unauthorized commercial INTERNET access as "field expedient" workarounds. These unprotected "backdoors" into the NIPRNET violate DoD policy, compromise the overall security of the Army's and DoD's networks and systems, and will be identified and terminated. If your command has an unauthorized connection(s), take action to immediately terminate that access capability. The Army POC for alternative connections resolution is Mr. Bill Buzinski, phone (703) 607-5888 (DSN 327), email: mailto:william.buzinski@hqda.army.mil.

6. The VCSA, in his 160453Z January 2001 message, again stated the Chief of Staff, Army's position that keeping Army systems and networks secure and operational is "a force protection issue and compliance with the IAVA process is mandatory." Your system administrators and network managers are fighting a cyber war daily. In the cyber battle space it truly takes only a very few who do not do their jobs to put us all at risk. Take for action.

[redacted]

From: [redacted]
Sent: Monday, August 21, 2006 11:25 AM
To: [redacted]

Subject: proxey (UNCLASSIFIED)

Attachments: reverse proxey server.doc

reverse proxey server.doc

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

Web Risk Assessment/Information Assurance Analyst

[redacted]

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

From: [redacted]
Sent: Tuesday, November 21, 2006 12:04 PM
To: DODWEBMASTERS-L@DTIC.MIL
Subject: Re: [WEBMASTERS] AWRAC (UNCLASSIFIED)

Both are registered by defenseweb.com.

myarmylifetoo.com
==========

Contact: ***@defenseweb.com

Domain name: MYARMYLIFETOO.COM

Registrant Contact:
DefenseWeb Technolodgies Inc.
DefenseWeb Technologies ****@defenseweb.com)
858-272-8505
Fax: 858-272-8565
4150 Mission Blvd., Suite 220
San Diego, CA 92109
US

Administrative Contact:
DefenseWeb Technologies Inc.
DefenseWeb Technologies ****@defenseweb.com)
+1.8582728505
Fax: 858-272-8565
4150 Mission Blvd., Suite 220
San Diego, CA 92109
US

Technical Contact:
DefenseWeb Technologies Inc.
DefenseWeb Technologies ****@defenseweb.com)
+1.8582728505
Fax: 858-272-8565
4150 Mission Blvd., Suite 220
San Diego, CA 92109
US

Status: Locked

Name Servers:
ns.defenseweb.net
ns2.defenseweb.net

Creation date: 10 Jun 2003 09:13:41
Expiration date: 10 Jun 2007 00:00:00

armyfrg.org
==========

Domain ID: D104655904-LROR
Domain Name: ARMYFRG.ORG
Created On: 21-Jul-2004 01:33:00 UTC
Last Updated On: 12-Nov-2006 06:59:54 UTC Expiration Date: 21-Jul-2007 01:33:00 UTC
Sponsoring Registrar: eNom401, Incorporated (R21-LROR)
Status: CLIENT DELETE PROHIBITED
Status: CLIENT TRANSFER PROHIBITED
Registrant ID: JC1165-BR
Registrant Name: DefenseWeb Technologies Registrant Organization: DefenseWeb Technologies Inc.
Registrant Street1: 4150 Mission Blvd., Suite 220 Registrant Street2: Registrant Street3: Registrant City: San Diego Registrant State/Province: CA Registrant Postal Code: 92109 Registrant Country: US Registrant Phone: +1.8582728505 Registrant Phone Ext.: Registrant FAX: +1.8582728565 Registrant FAX Ext.: Registrant Email: dns@defenseweb.com Admin ID: JC1165-BR Admin Name: DefenseWeb Technologies Admin Organization: DefenseWeb Technologies Inc.
Admin Street1: 4150 Mission Blvd., Suite 220 Admin Street2: Admin Street3: Admin City: San Diego Admin State/Province: CA Admin Postal Code: 92109 Admin Country: US Admin Phone: +1.8582728505 Admin Phone Ext.: Admin FAX: +1.8582728565 Admin FAX Ext.: Admin Email: dns@defenseweb.com Tech ID: JC1165-BR Tech Name: DefenseWeb Technologies Tech Organization: DefenseWeb Technologies Inc.
Tech Street1: 4150 Mission Blvd., Suite 220 Tech Street2: Tech Street3: Tech City: San Diego Tech State/Province: CA Tech Postal Code: 92109 Tech Country: US Tech Phone: +1.8582728505 Tech Phone Ext.: Tech FAX: +1.8582728565 Tech FAX Ext.: Tech Email: dns@defenseweb.com Name Server: NS.DEFENSEWEB.NET Name Server: NS2.DEFENSEWEB.NET

-----Original Message-----
[redacted]
Sent: Tuesday, November 21, 2006 09:03
To: DODWEBMASTERS-L@DTIC.MIL
Subject: [WEBMASTERS] AWRAC (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

Can anyone tell me the owner of these website?

http://www.myarmylifetoo.com/skins/malt/home.aspx?AllowSSL=true
<http://www.myarmylifetoo.com/skins/malt/home.aspx?AllowSSL=true>

https://www.armyfrg.org/skins/FRGPat/display.aspx
<https://www.armyfrg.org/skins/FRGPat/display.aspx>

[redacted]
Web Risk Assessment/Information Assurance Analyst
[redacted]

Classification: UNCLASSIFIED
Caveats: NONE

****
FAQ & Subscription info: http://www.dod.mil/webmasters/faq/

****
FAQ & Subscription info: http://www.dod.mil/webmasters/faq/

[redacted]

From: [redacted]
Sent: Thursday, October 19, 2006 1:07 PM
To: DODWEBMASTERS-L@DTIC.MIL
Subject: Re: [WEBMASTERS] OPSEC question (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

The PAO should be explaining to you why you should not link to some of the articles. The PAO and G2 are responsible for reviewing contain on Army web site for OPSEC and Army policy. See AR 25-1 ch 6 and DA Pan 25-1-1 ch 8 or DoD web policy on defense link.

[redacted]
Web Risk Assessment/Information Assurance Analyst
[redacted]

-----Original Message-----
[redacted]
Sent: Thursday, October 19, 2006 12:18 PM
To: DODWEBMASTERS-L@DTIC.MIL
Subject: Re: [WEBMASTERS] OPSEC question

"I'd appreciate any insight into whether or not I should be linking to these articles. I'm more and more apprehensive each time I'm asked to link to an article that contains names and/or photos. But I also need a little advice on how to explain to PAO that I can't link to the articles on someone else's site that contain what would amount to OPSEC violations if they were on our own public site."

Our base newspaper does the same thing. What I do each week is: They have given me an 'admin' login to the news site. Every week I go in and edit out any names/photos that are OPSEC. Any stories which would be OPSEC, I just remove entirely from the online site. So if they won't give you direct access to editing the info, here's some more ideas.

1. Explain to the PAO that while a local newspaper has 'base only'
distribution most of the time, once you put it on the web, it gets worldwide exposure - therefore any base newspaper that is posted online by the base, and linked to by their official website, needs to be OPSEC'd just like the website.

2. Give a basic OPSEC list to the online publisher, and ask them to remove items listed on that page before posting it, or:
Tell them you will contact them when the paper is published each week and tell them what can't go online.

3. Make sure in the next contract done with whoever publishes the paper, that removing material that is an OPSEC violation is one of the clauses, whether they remove as instructed, or whether they allow you or the PAO to remove it once posted (or before posted). :)

[redacted]
Public Affairs Specialist/Webmaster
jill.savin@us.army.mil
[redacted]
4550 Parade Field Lane Rm. 102
Fort Meade, MD 20755

****

FAQ & Subscription info: http://www.dod.mil/webmasters/faq/
Classification: UNCLASSIFIED
Caveats: NONE

****

FAQ & Subscription info: http://www.dod.mil/webmasters/faq/

[redacted]

From: [redacted]
Sent: Monday, October 23, 2006 10:33 AM
To: DODWEBMASTERS-L@DTIC.MIL
Subject: Re: [WEBMASTERS] QUESTION: .com Site?? (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

You need to fine this ref.
M-05-04
MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES
[redacted]
Deputy Director for Management
SUBJECT: Policies for Federal Agency Public Websites

[redacted]
Web Risk Assessment/Information Assurance Analyst
[redacted]

-----Original Message-----
[redacted]
Sent: Monday, October 23, 2006 8:49 AM
To: DODWEBMASTERS-L@DTIC.MIL
Subject: Re: [WEBMASTERS] QUESTION: .com Site??

[redacted]

For Army private sites this guidance is very clear at 6-4-n-11 of AR25-1. Army policy is not what you need, but it might help you to point to 1.a. at http://www.cio.gov/documents/ICGI/ICGI-June9report.pdf - Federal public websites must use government domains. Scroll down to page 9 of 54 on this page. This document is very helpful because it describes the exceptions and the rationale along with the guidance.

[redacted]
Fort Leavenworth, KS

-----Original Message-----
[redacted]
Sent: Monday, October 23, 2006 6:29 AM
To: DODWEBMASTERS-L@DTIC.MIL
Subject: [WEBMASTERS] QUESTION: .com Site??

All -

I know this has been discussed but I didn't save any of the emails since I never thought I'd have to know this. I have a client who wants a .com or .org site for their organization. I can't remember where

to look for this and they are prepared to take whatever steps necessary to get a site like that. If someone could point me in the right direction, I'd appreciate it.

Thank you!

[redacted]
SAF/AQ Webmaster
https://www.safaq.hq.af.mil

****
FAQ & Subscription info: http://www.dod.mil/webmasters/faq/

****
FAQ & Subscription info: http://www.dod.mil/webmasters/faq/
Classification: UNCLASSIFIED
Caveats: NONE

****
FAQ & Subscription info: http://www.dod.mil/webmasters/faq/

[redacted]

From: [redacted]
Sent: Monday, September 25, 2006 10:28 AM
To: [redacted]
Subject: RE: AWRAC website update (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

David

We need to put in the links to our ako site and the direct link to the DoD wet policy.

We need to ad a statement about the bloggs from the CoS message. And the OMB message.

Also add the IA training site link for Web training.

[redacted]
Web Risk Assessment/Information Assurance Analyst
202-492-7797
[redacted]

[redacted]
Sent: Monday, September 25, 2006 10:12 AM
[redacted]
Subject: FW: AWRAC website update (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

Good Morning Pete,
Got this in my email this morning. Any thoughts on this?
-David

[redacted]
LMIT Professional Services

Information Assurance Directorate NETC-EST-A

Army Web Risk Assessment Cell
A&VTR Analyst
[redacted]
AKO IM User

[redacted]
Sent: Monday, September 25, 2006 10:05 AM
[redacted]
Subject: FW: AWRAC website update (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

AWRAC Team,

Lets discuss/review this by 27 Sep 06 in order to meet the suspense of 28 Sep 06.

Thanks,

[redacted]
USA, MSG
[redacted]
2530 Crystal Drive
Arlington, VA 2202

[redacted]
Sent: Wednesday, September 20, 2006 12:28 PM
To: [redacted] NETCOM
Subject: AWRAC website update (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

This is on website under Website OPSEC, it is an older message. If there is a newer message we need to post or a validated AWRAC mission statement that describes what they do that we can post, please work with the AWRAC support people put it together. Then we can put that up on the website.

Suspense: 28 September.

-----Original Message-----
[redacted]
Sent: Friday, September 28, 2001 10:22 AM
To: DISC4 MACOM IAPMs; DISC4 IAM
Subject: Force Protection and Web Site Content Security
Importance: High
IA Professionals,
We all know that America is in a state of emergency. We have heard what the President said and we know that part of securing America is protecting our information and protecting ourselves against cyber attack. We all are on the front lines of this emergency.
All Army IAPMs need to provide guidance to their subordinate elements to get involved with the

Force Protection personnel/unit/organizations in their commands and make sure that they realize that protection against cyber attack is a force protection issue. This position is nothing new and was articulated by the VCSA in two messages: DTG 151830Z MAR 00/Information Assurance Vulnerability Alert (IAVA) Compliance////DTG 160453Z JAN 01/VCSA SENDS: Defense of Army Information Systems. We are in the process of putting both messages in the "hot topics" of the Army Web Site to include a link to the URL mentioned later in this email.
We must make sure that building bigger fences and providing additional lights are not the only Force Protection indicatives that are reviewed and implemented. Are critical cyber nodes such as switches, server farms and routers adequately protected ? Are critical communication nodes on UPS ? Is the power to these nodes protected ? Is there redundant communications and appropriate back up stored away from the main site? Etc. Etc.
The IAPMs need to immediately provide guidance to their subordinates directing a scrub of all publicly accessible web sites. We need to make sure names, SSNs, addresses, home addresses etc are not on these sites.
The layout of a site, the location and contents of buildings may have been appropriate on 10 September but they are probably not appropriate today. Make sure we are not giving away sensitive critical infrastructure information. If there is any doubt about information take it off while it is being reviewed.
TO HELP YOU DEVELOP GUIDANCE recommend that you go to http://www.defenselink.mil. Once there scroll to the very bottom and click on the small print that states web policy. Once there find Web Site Administration Policies and Procedures (11/25/98) including amendments (04/26/2001). Review Part II -Procedures sections 3.51 - 3.5.6 and Part V Examples and Best Practices, Part 1 Information Vulnerabilities, the WEB and OPSEC.
Also I wish to remind you that when the IAVA Compliance Verification Team visits your organizations the main reason for IAVAs not being applied is that a new system/old backup data was introduced and the IAVAs were not applied. Please remind everyone that using an old backup and the introduction of a new system are the main reasons for IAVA non compliance.
In conclusion we need to ensure we are an active part of the Force Protection community, we need to move fast on reviewing the content of our web servers and we need to make sure that IAVAs are applied to all systems.

thanks

[redacted]
Information Assurance Specialist
NETCOM, NETC-EST-IC
[redacted]

Classification: UNCLASSIFIED
Caveats: NONE

Classification: UNCLASSIFIED
Caveats: NONE

Classification: UNCLASSIFIED
Caveats: NONE

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

From: [redacted]
Sent: Thursday, February 01, 2007 4:37 PM
To: [redacted]
Cc: [redacted]
NETCOM; Van Vleet, Gordon M MR NETCOM
Subject: RE: Media query on AWRAC (UNCLASSIFIED)
Signed By: [redacted]

Classification: UNCLASSIFIED
Caveats: NONE

[redacted] Based on the AWRAC mission, yes, Soldier blogs on the public web could be reviewed by AWRAC. Per AWRAC:

The Army Web Risk Assessment Cell's (AWRAC) goal is to review all Army information that is publicly available for violations of Operational Security (OPSEC) which may put Army assets, operations, or people at risk and the posting of privacy information that may lead to identity theft and/or endanger Army personnel or their families.

Regards,
[redacted]
Strategic Communications Officer
Army Chief Information Office/G-6
[redacted]
http://www.army.mil/ciog6/

-----Original Message-----
[redacted]
Sent: Thursday, February 01, 2007 3:15 PM
[redacted]

This is what we suggest as a response to [redacted] reference a media query she received. Do you see any issues with this response.

PROPOSED RESPONSE: The Army Web Risk Assessment Cell's (AWRAC) goal is to review all Army information that is publicly available for violations of Operational Security (OPSEC) which may put Army assets, operations, or people at risk and the posting of privacy information that may lead to identity theft and/or endanger Army personnel or their families.

Do you want to deal with her or do you want us to contact her. Thanks.

[redacted]

-----Original Message-----
[redacted]
Sent: Wednesday, January 31, 2007 5:46 PM
To: NETCOM Army Web Risk Assessment Cell
Subject: Media query on AWRAC (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

I received a query asking about the AWRAC and if it screens opinion or editorial essay-type material of Soldier blogs. I would think yes, but I wanted to check to make sure. Do you have any guidance on this?

[redacted]

[redacted]
Army Public Affairs
1500 Pentagon, RM 1E475
(703) 697-7487
ARMY STRONG

Classification: UNCLASSIFIED
Caveats: NONE

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

From: [redacted]
Sent: Monday, February 05, 2007 8:44 AM
To: [redacted]
Subject: RE: Meeting Invitation: Web Risk Assessment Cell (UNCLASSIFIED)
Signed By: leroy.lundgren@us.army.mil

Classification: UNCLASSIFIED
Caveats: NONE

Yes - I assume that [redacted] is also attending ? What about [redacted] ?

[redacted]

[redacted]
Deputy Director Army Office of Information Assurance and Compliance
[redacted]

-----Original Message-----
[redacted]
Sent: Sunday, February 04, 2007 12:02 PM
[redacted]
Subject: FW: Meeting Invitation: Web Risk Assessment Cell (U) (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]
May I attend?

[redacted]
Web Risk Assessment/Information Assurance Analyst
[redacted]

-----Original Message-----
[redacted]
Sent: Thursday, February 01, 2007 3:19 PM
[redacted]

[redacted]

Subject: Meeting Invitation: Web Risk Assessment Cell (U)

UNCLASSIFIED

You are invited to attend a DoD Web Risk Assessment meeting on Friday, February 23, 2007, sponsored by OUSD(I), and hosted by the Interagency OPSEC Support Staff at their facility located at 6411 Ivy Lane, Suite 400, Greenbelt, MD 20770. (www.ioss.gov <file://www.ioss.gov>)

The purpose of the meeting is to re-establish Joint / Service relationships, find out the current status of the WRACs, successes and challenges, and explore (and possibly identify) a way-ahead to optimize the efficiency and effectiveness of the Joint and Service WRAC missions.

0900-0920:	Introductions & DOD Policy Review
0920-0950:	Army WRAC
0950-1020:	Navy WRAC
1020-1035:	Break
1035-1105:	Marine Corps WRAC
1105-1135:	Air Force WRAC
1135-1205:	JWRAC
1205-1315:	Lunch
1315-1430:	Way-ahead discussion
1430-1445:	Break
1445-1500:	Wrap-up

For your information, [redacted] DoD Director of Security, OUSD(I), will be attending for a portion of the day. He's interested in this topic & is looking to you for information that may assist in decision-making. With that in mind, request the briefers be prepared to provide information on the following:

What are the authorities that govern your WRAC?
How do personnel analyze identified information for concerns?
If a problem does surface, how do you notify, and then track it?
Do you go back and review sites for compliance?
Do you ever find systemic problems? If so, what do you do?
Do you think your efforts are making a difference?

Please let me know your availability by February 7 and provide me any briefing slides by February 20.

Respectfully,

[redacted]
OUSD(Intelligence)
Security Policy Directorate
[redacted]

[redacted]

Classification: UNCLASSIFIED
Caveats: NONE

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

From: [redacted]
Sent: Monday, September 25, 2006 8:35 AM
To: [redacted]
Subject: RE: Potential Letter about Registering in DTIC (UNCLASSIFIED)
Signed By: [redacted]

Classification: UNCLASSIFIED

Caveats: NONE

Add after DTIC the replacement for GILS IAW AR25-1

[redacted]
Web Risk Assessment/Information Assurance Analyst
[redacted]

[redacted]
Sent: Wednesday, September 20, 2006 6:56 PM
[redacted]
Subject: Potential Letter about Registering in DTIC (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

IAPM -- The Army Web Risk Assessment Cell (AWRAC) is currently reviewing U.S. Army Web sites to ensure they are registered in the Defense Technical Information Center (DTIC) Database. It has been noted that your organization's website is not registered with DTIC. Please review the URL below and enter it into the DTIC Database at www.DTIC.mil <file:///\\www.DTIC.mil> in order to comply with Army Webmaster Guidelines. We ask that you complete this task and report resolution of this issue NLT 22 FEB 06.

More information can be found at
http://www.army.mil/ciog6/references/webmaster/docs/DOD_GILS_File.doc
<http://www.army.mil/ciog6/references/webmaster/docs/DOD_GILS_File.doc>
Please contact me if you have questions.

[redacted] what do you think about the wording above? This is a rought draft obviously.

[redacted]

[redacted]
LMIT Professional Services

Information Assurance Directorate NETC-EST-A

Army Web Risk Assessment Cell
A&VTR Analyst
[redacted]

AKO IM User

Classification: UNCLASSIFIED
Caveats: NONE

Classification: UNCLASSIFIED

Caveats: NONE

[redacted]

From: [redacted]
Sent: Friday, October 06, 2006 11:52 AM
To: [redacted]
Cc:
Subject: [redacted]

Importance: High

Classification: UNCLASSIFIED
Caveats: NONE

No waivers have been issued for osmisweb.com

They are out of compliance on two counts:

1) use of .com instead of .mil
2) using log-on other than AKO SSO (without CIO/G-6 approval)

Any waiver request must have memo requesting from the org with 06/15 or higher signing the memo.
Explanation of why GIG resources with .mil cannot be used.
Explanation of why AKO/SSO cannot be used. (Description of customer base, system configuration issues, etc.)

Submit memo in pdf format to SAIS-GKP (either Mike Sandberg or myself).

If this system has privacy or OPSEC issues, it should be shut down immediately.

[redacted]
CIO Policy Division
Army Chief Information Officer/G-6
[redacted]

-----Original Message-----
[redacted]
Sent: Friday, October 06, 2006 9:38 AM
[redacted]
D)

Classification: UNCLASSIFIED
Caveats: NONE

Arlene
Can you tell me is this site has a wavier to use the .com domain

http://www.osmisweb.com/

David, please run a scan on this sit.

All we will contact the webmaster once we check the status of the scan and any wavers.

[redacted]
Web Risk Assessment/Information Assurance Analyst
[redacted]

-----Original Message-----
[redacted]
Sent: Friday, October 06, 2006 7:28 AM
[redacted]
Subject: FW: Use of .com Websites for Official Business (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

Pete,

Can you help here. This is an "official" site with no security.

Respectfully,
[redacted]MIT Professional Services) Office of Information Assurance and Compliance
NETC-EST-I GCIH//US Army CIO/G-6 Office [redacted]A good plan violently executed today is better than a perfect plan executed at some indefinite point in the future". Patton

-----Original Message-----
From: [redacted]ailto[redacted]@msl.army.mil]
Sent: Thursday, October 05, 2006 10:19 AM
[redacted]
Subject: RE: Use of .com Websites for Official Business

[redacted]

[redacted]

I look forward to hearing from you.

[redacted]
IA Program Manager
IM/IA Directorate
PEO Missiles and Space
[redacted]

-----Original Message-----
[redacted]
Sent: Thursday, October 05, 2006 6:47 AM

[redacted]
NETCOM/LMIT
Subject: Re: Use of .com Websites for Official Business

[redacted]ave worked these issues in the past. I have added them both. They should be able to help you out.

Sent from my BlackBerry Wireless Handheld

-----Original Message-----
[redacted]
Sent: Wed Oct 04 19:22:11 2006
Subject: Use of .com Websites for Official Business

Sally,

Are you the point of contact for issues concerning the use of .com websites for official business? PEO MS has concerns about the link below which has been cited for usage by [redacted]. The site SSL or CAC enabled, it is on a commercial site, and I am not if it has any IA security measures. Can you point me in the right direction for assistance?

http://www.osmisweb.com/.

[redacted]
IA Program Manager
IM/IA Directorate
PEO Missiles and Space
[redacted]

Classification: UNCLASSIFIED
Caveats: NONE

Classification: UNCLASSIFIED
Caveats: NONE

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

From: [redacted]
Sent: Wednesday, January 03, 2007 4:20 PM
To: [redacted]
Cc: [redacted]
Subject: Re: VETCOM Website (UNCLASSIFIED)

Attachments: AMC.doc; Findings list.doc

AMC.doc Findings list.doc

[redacted]

Thank you for your assessment of our website.

VETCOM is balancing the need for food security vs. food safety. If we "lock-down" the website, commercial vendors, who sell products to places like dining facilities, won't have ready access to the lists of potential food suppliers. Before the list was published on the worldwide web, access by vendors/contractors was limited. This created a situation where subsistence from "unapproved sources" found its way into our food chain because commercial vendors didn't have ready access to the hardcopy version of the list. This compromised DOD's food safety.

Our approved source lists includes lists published by the USDA, USDC and the FDA. By locking down our list, this doesn't preclude a potential terrorist from access to other lists of DOD food suppliers.

In addition, our list only includes "potential" suppliers. If a commercial vendor is on our list, this does not necessarily mean that the DOD procures food from the supplier. Many of our commercial vendors don't have an "active" contracts. These vendors want to sell to the military but don't necessarily "win" the contract, but they do wish to compete for future contracts, so they remain on our list.

Again, I believe there is no easy answer to this issue. Would it be possible to give you a call via conference phonecall so you could hear the concerns of all my staff members (more information than I can put in an email)? This will assist us in making the best possible decision regarding password protecting our Directory.

Respectfully,

[redacted]
LTC, VC, USA
Chief, Food Safety and Quality Assurance

[redacted]

To [redacted]

(UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

http://vets.amedd.army.mil/862567CA004D4461/Content/ApprovedSources
Good Morning [redacted],

The Army Web Risk Assessment Cell (AWRAC) is currently reviewing U.S. Army Web sites for OPSEC and security compliance. An OPSEC concern was found on your organization's website and has been classified as a minor finding. The attached URL are publicly accessible, and contains links to food distributors for mulitple regions and locations of our service members. AKO Authentication is used for one of the CENTCOM links, the other uses an "issued" login and password, while the rest have no login and password. Per AR 25-1, we strongly recommend placing each of these links behind an AKO username and password. Please review the attached document for further guidance, and report resolution of this issue NLT 10 JAN 07. Please contact me if you have questions.

<<...>> <<...>>

R/,

[redacted]

Lockheed Martin Information Technology
Information Assurance Directorate NETC-EST-A Army Web Risk Assessment Cell

[redacted]

AKO IM User

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

From: [redacted]
Sent: Tuesday, January 30, 2007 11:51 AM
To: [redacted]
Subject: Re: Website Content (UNCLASSIFIED)

Follow Up Flag: Follow up
Flag Status: Red

Hello,

Are you able to indicate anything specific photo/video-wise with sensitive information on the website? It isn't a military hosted site (it was a project by a few of the unit's members at the time), but we can adjust what you point out. The letter is very vague. While it mentions "DA PAM 25-1-1" it doesn't link to any example photo, or excerpt from the PAM or explain what is offensive.

Thanks,

[redacted]

[redacted]

Classification: UNCLASSIFIED
Caveats: NONE

January 30, 2007

Webmaster,

1. The Army Web Risk Assessment Cell (AWRAC) is currently monitoring U.S. Army affiliated Blogs (Web Logs). One of the Army's foremost concerns is the safety and well-being of our troops and their families. The AWRAC assists in this endeavor by ensuring information on publicly accessible websites does not inadvertently provide information that may harm our troops or their family members. Computers recovered in Afghanistan and Iraq validate that enemies of the United States do, in fact, monitor websites and blogs looking for the type of information displayed on your blog. Please review the information below and determine whether or not it poses a threat to the welfare of our soldiers. You are welcome to contact the AWRAC for more information and guidance. This material should be removed as soon as possible if it is determined to create a risk. Please notifiy the AWRAC of your actions NLT 6 February 2007.

-This site contains senstive information in some of the photos and videos, which must be removed or password protected, in accordance with DA PAM 25-1-1.

-This appears to be a military hosted site. If this is correct, this site is in violation of AR 25-1 and needs to migrate to a .mil domain or request a waiver from Army CIO/G-6.

Thank you,
Army Web Risk Assessment Cell
Email: AWRAC@hqda.army.mil <mailto:AWRAC@hqda.army.mil>

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

From: [redacted]
Sent: Friday, February 09, 2007 5:22 PM
To: [redacted]
Cc: [redacted]
Subject: RE: Year End Wrap Up of the AWRAC You Requested (UNCLASSIFIED)
Signed By: [redacted]

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

Please add info that the COL mentioned but talk about it in their holistic approach -- they are continuing to look at content but they also want to look at the web server to see if it is in AVTR - if the patches are up too date, see if it is registered and to see if it is behind a reverse proxy server. So they are approaching the server from many different directions and are not looking at just the content.

[redacted]

Arrange for [redacted] to brief the [redacted] and myself upon our return on this approach and to brief exactly where they are. Make sure his MSG briefs and continuous to tell the truth -- in other words if they are at square one tell us.

[redacted]

[redacted]
Deputy Director Army Office of Information Assurance and Compliance
[redacted]

-----Original Message-----
[redacted]
Sent: Friday, February 09, 2007 8:52 AM
[redacted]
Subject: RE: Year End Wrap Up of the AWRAC You Requested (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

I don't know if I missed it but can we talk about identification of Web Sites that are not registered nor behind Web Proxy server and how this improves overall Web page/server security...

-----Original Message-----
[redacted]
Sent: Thursday, February 08, 2007 6:45 PM
[redacted]
[redacted]
FLTC NETCOM
Subject: Year End Wrap Up of the AWRAC You Requested (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

<<...>>

[redacted] here is the AWRAC paper you asked for.

Phyllis and crew -- I changed a few items and added more yada yada of how the Guard guys are saving the world -- us this version. I also took out items such as we are developing -- not good words. Thank you for the effort -- BTW we review for OPSEC and privacy content violations.

[redacted]
[redacted]
Deputy Director Army Office of Information Assurance and Compliance
[redacted]

Classification: UNCLASSIFIED
Caveats: NONE

Classification: UNCLASSIFIED
Caveats: NONE

Classification: UNCLASSIFIED
Caveats: NONE

Dr. Hamre memorandum date 24 sep 1998 SUBJECT **Information Vulnerability and the World Wide Web**. http://www.defenselink.mil/other_info/depsecweb.pdf

> Personnel risk:
> Removal of : Plans and lessons Learned, Operations or Vulnerabilities.
> Any Reference to movement of or locations of units and personnel.
> Removal of all personal information: SSN, DOB, Name or location or family members.

Deputy SECDEF Memo, Subj: **Operations Security Throughout the Department of Defense** http://www.fas.org/sgp/bush/wolfowitz.html 18 Oct 2001.

> OPSEC in general,(Do not conduct *any* work-related conversations in common areas, public places, while commuting, or over unsecured electronic circuits)

OSD Memo Subj: **Withholding of Personally Identifying Information Under the Freedom of Information Act (FOIA):** http://www.defenselink.mil/pubs/foi/withhold.pdf 9 Nov 2001.

> Implementation of FOIA for personal information. Withholding of list of name and e-mail addresses under FOIA

OSD Memo Subj: **Removal of Personally Identifying Information from Unclassified Websites:** http://www.defenselink.mil/pubs/foi/names_removal.pdf 28 Dec 2001.

> Removal Of Lists and roster, Telephone directories, Organizational Charts.

DODD 5230.9 Clearance of DOD Information for Public Release April 9, 1996, ASD(PA) http://sites.defenselink.mil/dd5230_9.html#A

AR 530-1 is available at.. <http://www.fas.org/irp/doddir/army/ar530-1t.htm>

AR25-1 Army Information Management:
http://www.usapa.army.mil/pdffiles/r25_1.pdf - 30 JUN 2004

AR 25-1
http://www.usapa.army.mil/pdffiles/r25_2.pdf

DoD Web Policy

> Donald Rumsfeld's message to DOD (R 141553Z JAN 03)
> Web Site Administration Policies & Procedures (11/25/1998) including all updates (01/11/2002)
> Amendment and Corrections to Web Site Administration Policies & Procedures (01/11/2002)
> Accessibility of DoD Web Sites to People with Disabilities
> Clearance of DoD Information for Public Release DoD Directive 5230.9
> Security and Policy Review of DoD Information for Public Release DoD Instruction 5230.29

Clearing Electronic Information for the Public
Cookie / Privacy Policy
Domain Registration in the .mil Domain
Electronic Newspaper Policy DoD Instruction 5120.4
Freedom of Information Act - FOIA
DoD FOIA Guidance
Removal of Personally Identifying Information of DoD Personnel from
Unclassified Web Sites
Withholding of Personally Identifying Information under the FOIA
DoD Guidance on Attorney General FOIA Memorandum
GILS Policy; Deputy Secretary of Defense John White (09/02/1995)
Mobile Code Policy
Principles of Information
Records Management DoD Directive 5015.2

Posting NBC Information:
Some things can be publicly released and therefore posted, but the material must have been reviewed according to the most recent guidance and reviewed/released IAW existing policy. Guidance on what can be released is covered by the so-called "Card" memo (memo from White House signed by Andrew Card, 19 Mar 02, attached) and the associated DoD guidance/SECDEF msg (see <http://foia.navy.mil/020520policymemo-encl1.txt>), and in DoDI 5230.19 (see paras 6.1.7.4 and 6.2.7, in particular) which states the CBRN info is one of 7 areas of info that requires review at the DoD level. Thus, that info must be submitted to Army HQ for subsequent DoD determination (see para 6.2.3).

Basically from your point of view, I'd say that if something raises a question, the web site owner should be able to present the official public release clearance when requested to do so.

CBRN WH Memo 19 Mar 021.pdf

[redacted]

From: [redacted]
Sent: Tuesday, November 14, 2006 3:35 PM
To: [redacted]
NETCOM/LMIT
Subject: request for training (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

I spoke with [redacted] the government lead for the AWRAC, he wanted to know if you or the Bn commander would be at the National Guard Conference at Las Vegas in DEC? If so he would like to meet you about your training needs.
Also please let both of us know when the Memorandum for [redacted] is ready; we would like to make this work ASAP.

[redacted]
Web Risk Assessment/Information Assurance Analyst
[redacted]

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

From: [redacted]
Sent: Tuesday, January 30, 2007 1:33 PM
To: Lickwar, David M Mr NETCOM/LMIT
Cc: [redacted]

Subject: Update on review of VETCOM website

Attachments: AMC.doc; Findings list.doc


AMC.doc


Findings list.doc

[redacted]

I appreciate your organization taking the time to assist VETCOM in the review of our Approved Sources website. For the most part, our website looked OPSEC and security compliant. I just wanted to give you an update as to status of the password protection issue.

On 9 Jan 07, the Food Risk Evaluation Committee (FREC), the committee that provides expert guidance to the Army Surgeon General, reviewed this issue.
Here are the nuts and bolts of the presentation:

ISSUE: Password protection of VETCOM's Approved Source Directory

*PROS: Improved security of website

*CONS: Decreased usage of directory-->decrease food safety; US Department of Agriculture and Commerce don't password protect their website; password protection doesn't prevent open surveillance; VETCOM lists only includes potential supplier, not necessarily a list where DOD purchased food; Defense Supply Center Philadelphia and Defense Commissary Agency openly list suppliers of food sources and contract amounts.

I would like to direct you to the following links:

http://www.commissaries.com/business/contracting.cfm

http://www.dscp.dla.mil/subs/contract/index.asp

http://vm.cfsan.fda.gov/~ear/shellfis.html

The Defense Commissary link goes to their contracting website. Here you can access all their food procurement contracts with dollar amounts. The same can be said of the Defense Supply Philadelphia website. I have also included FDA's Shellfish Shippers list as an example of an open source of information on the web where DOD procures food.

BLUF: By password protecting VETCOM's Approve Sources website, security has not improved. The FREC voted not to recommend password protection at this time (CENTCOM Approved Sources list remains password protected).
However, VETCOM will continue to review its website for OPSEC violations on a continuing basis. If you have any questions, please give me a call at [redacted]

Respectfully,
[redacted]
LTC, VC, USA
Chief, Food Safety and Quality Assurance

[redacted]
01/03/2007 09:36 AM

[redacted]
(UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

http://vets.amedd.army.mil/862567CA004D4461/Content/ApprovedSources
Good Morning [redacted]
The Army Web Risk Assessment Cell (AWRAC) is currently reviewing U.S. Army Web sites for OPSEC and security compliance. An OPSEC concern was found on your organization's website and has been classified as a minor finding. The attached URL are publicly accessible, and contains links to food distributors for mulitple regions and locations of our service members. AKO Authentication is used for one of the CENTCOM links, the other uses an "issued" login and password, while the rest have no login and password. Per AR 25-1, we strongly recommend placing each of these links behind an AKO username and password. Please review the attached document for further guidance, and report resolution of this issue NLT 10 JAN 07. Please contact me if you have questions.
<<...>> <<...>>
R/
[redacted]
Lockheed Martin Information Technology
Information Assurance Directorate NETC-EST-A Army Web Risk Assessment Cell
[redacted]
AKO IM User

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

From: [redacted]
Sent: Tuesday, February 13, 2007 9:10 AM
To: [redacted]
Subject: Web sites that should be reviewed. (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: FOUO

Gentlemen,
Could you examine the following websites for an OPSEC concerns? These belong to the 1-34 BCT (National Guard Unit).

They both are on .com domains and seem to have a lot of official and possibly sensitive information in them.

Vr,

[redacted]
OPSEC Program Manager
United States Army Medical Command/
HQDA-Office of the Surgeon General
[redacted]

http://www.redbullweb.com/index.html <http://www.redbullweb.com/index.html>

http://www.hhc1-34bctfrg.com/index.html <http://www.hhc1-34bctfrg.com/index.html>

Classification: UNCLASSIFIED
Caveats: NONE

Classification: UNCLASSIFIED
Caveats: FOUO

DRAFT

1. On DATE, the Army Web Risk Assessment Cell conducted an assessment of your website for compliance with the following policy:

A. Web site posted on a .mil domain or exception wavier approved per AR 25-1 and DA Pam 25-1-1.

B. Site utilizing one of the Army reverse proxy services per AR 25-1 6-4n(7)(b).

C. Site registration. (The requirement to register all Army website with the Government Information Locator Service (GILS)is changing to the A-Z listing on the Army home page)per AR 25-1 and DA Pam 25-1-1.

2. It has been noted that your website (URL) is not in compliance with (A B C) above.

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of policy concerns and that appropriate remedial actions are taken.

4. The AWRAC will report security and policy concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to acknowledge receipt via email to the AWRAC (**AWRAC@hqda.army.mil**) and forward the memorandum to the commander/ supervisor, or his/her designated representative, responsible for the website. Suspense dates for corrective actions/resolution of security concerns are provided in the memorandum. Copies of this memorandum will be furnished to the appropriate MACOM, PEO, PM, or IAPM.

INFORMATION PAPER

NETC-EST-I
12 JAN 2007

SUBJECT: Army Web Risk Assessment Cell (AWRAC)

1. Purpose. To provide a synopsis to the Senior Leadership regarding the accomplishments of the Army Web Risk Assessment Cell (AWRAC) for 2006 and to highlight the essential role that the National Guard is executing in support of this CSA directed mission.

2. Facts: The AWRAC mission is to review publicly accessible Army Websites and unofficial sites posted by Army personnel for information that could pose a risk to operations security or the theft of privacy information. In addition, the AWRAC evaluates website content to ensure compliance with departmental policies, federal regulations and procedures, and industry best practices.

3. The Army Web Risk Assessment Cell (AWRAC) successfully mobilized 10 members of the Virginia National Guard Data Processing Unit on 10-21 July 2006 for one year. The team is leading AWRAC's mission to monitor official and unofficial web sites for OPSEC violations IAW the CSA's 20 AUG 2005 message. The team processed through Fort Belvior, and is assigned to NETCOM, with duty at the unit's headquarters at Manassas Armory. The Team also led the training of 20 additional traditional Guardsmen. During January 2007, the Cell conducted a eight day, 24X7 operation to review a multitude of web sites and blogs. The operation included mobilized soldiers, traditional Guardsmen, Reserve Soldiers, and contractors. This unit has been essential to the Army's ability to review Army web sites and web logs (BLOG) for potential operations security and privacy data content violations. Their continued mobilization status will be key to the Army being able to continue this important mission.

4. For the year ending DEC 2006 the AWRAC reviewed over 1200 official Army websites and over 500 blogs posted by Army personnel. These sites consisted of over four million pages and yielded over 1800 OPSEC concerns.
Following identification of potential risks, the AWRAC team worked with the sites' operators to remove information that could pose a security threat. Based on this review the team eliminated or secured over 1274 documented security violations. For example, the discovery and removal of a SECRET document that was posted on the AKO UNCLASSIFIED network. The AWRAC was instrumental in the removal of information on biological, chemical and missile weapon systems throughout the World Wide Web to ensure the safety of the American public and curtail leakage to unauthorized persons. In addition the AWRAC team removed or secured access to For Official Use Only (FOUO)) documents from publicly accessible web sites. This also included removing documents on Army web sites that protected personnel from identity theft of Social Security numbers, dates of birth, home addresses. This single action totally eliminated significant potential threats to national security and Army personnel.

5. The team reviews over 1700 websites for security concerns two to three times a year. It conducts announced and unannounced assessments of Army websites to determine compliance with regulations. A parallel and continuing AWRAC task is providing education and training to enable relevant audiences and Army personnel to become aware of and preventing/removing potential risks from the extensive and growing number of Army maintained web pages and personal blogs. The team has engaged in a number of outreach programs to increase awareness of the potential damage stemming from information on publicly accessible sites by publishing articles in military and technical publications, training over 2000 personnel on their OPSEC web site https://iatraining.us.army.mil since JAN 06, and by developing an Information Assurance Awareness Training Course posted on the IA training site. This training has been accessed by over 741 HQDA staff members since JUL 06 IAW the Army IG directive. The AWRAC also supports a website on Army Knowledge Online at https://www.us.army.mil/suite/portal.do?$p=254224 to provide information on AWRAC issues with over 540 members.

6. This mission is an ongoing endeavor that will require continuous fine-tuning and flexible, innovative tools and procedures to meet the existing and future needs of the Army's web community and public outreach programs.

7. The AWRAC currently employs three full-time analysts, a mobilized 10-member team from the VA National Guard's Data Processing Unit (DPU), and coordinates for support from 30 Army National Guard and Army Reserve soldiers to conduct analyses during their drill weekends and annual training. Currently a request is being processed to NETCOM for an additional year of mobilized manpower support from the VA DPU. Without the manpower being provided by the National Guard the review of web sites and BLOGs would be significantly curtailed and would lead to an increasing number of content and privacy content violations remaining undetected in the public domain.

[redacted]z/202-492-779[redacted]703-602-7481

[redacted]

From: [redacted]
Sent: Thursday, February 08, 2007 6:45 PM
To: [redacted]
Cc:

Subject: Year End Wrap Up of the AWRAC You Requested (UNCLASSIFIED)
Signed By: [redacted]

Attachments: 2006 AWRAC VER 2.doc

2006 AWRAC VER 2.doc

Classification: UNCLASSIFIED
Caveats: NONE

<<...>>

[redacted] here is the AWRAC paper you asked for.

Phyllis and crew -- I changed a few items and added more yada yada of how the Guard guys are saving the world -- us this version. I also took out items such as we are developing -- not good words. Thank you for the effort -- BTW we review for OPSEC and privacy content violations.

[redacted]

Deputy Director Army Office of Information Assurance and Compliance

[redacted]

Classification: UNCLASSIFIED
Caveats: NONE

UNCLASSIFIED

EXECUTIVE SUMMARY
17 October 2006

(U) Legal procedures for reviewing video log website (http://www.youtube.com/) A review of the Youtube website and coordination with the NETCOM council Tom King determined that Video log websites or video logs that are publicity accessible have no different legal status then the personal logs or photo logs. The AWRAC or other non-intelligence activity looking at content and reporting OPSEC violations on sites of confirmed Army personnel is consistent with the AWRAC mission.

UNCLASSIFIED

[redacted]ockheed Martin)

Information Assurance Directorate Army Web Risk Assessment Cell

202-492-7797 (NO DSN)

[redacted]s.army.mil

UNCLASSIFIED

EXECUTIVE SUMMARY
17 October 2006

(U) Legal procedures for reviewing video log website (http://www.youtube.com/) A review of the Youtube website and coordination with the NETCOM council Tom King determined that Video log websites or video logs that are publicity accessible have no different legal status then the personal logs or photo logs. The AWRAC or other non-intelligence activity looking at content and reporting OPSEC violations on sites of confirmed Army personnel is consistent with the AWRAC mission.

UNCLASSIFIED

[redacted] (Lockheed Martin)

Information Assurance Directorate Army Web Risk Assessment Cell

202-492-7797 (NO DSN)

[redacted]@us.army.mil