[redacted]

From: [redacted]
Sent: Monday, February 26, 2007 4:47 PM
To: [redacted]
Subject: FW: NETCOM Email (UNCLASSIFIED)"FOIA" (UNCLASSIFIED)
Signed By: [redacted]

Attachments: RE: Army Web Risk Assessment Cell (AWRAC) (UNCLASSIFIED)

RE: Army Web Risk Assessment C...

Classification: UNCLASSIFIED
Caveats: NONE

-----Original Message-----
[redacted]
Sent: Monday, July 24, 2006 8:35 AM
[redacted]
Subject: RE: NETCOM Email (UNCLASSIFIED)

Classification: UNCLASSIFIED

Caveats: NONE

[redacted] we will stay with the 31st as a planned visit. I've attached an email from [redacted] on a mission creep for AWRAC. We will need to discuss how we will monitor, alert and report when we come out..

J

[redacted]
CIO/G6 NETC ESTA, OIA&C
[redacted]
"Our Army at War -- Relevant and Ready"

From: [redacted]
Sent: Sunday, July 23, 2006 11:05 AM
[redacted]
Subject: RE: NETCOM Email (UNCLASSIFIED)

Classification: UNCLASSIFIED

Caveats: NONE

Sir,

Not a problem. Good news for [redacted] The 31st is probably the best for a visit. We are finishing up the training and the room organization next week. [redacted]

[redacted]
Sent: Friday, July 21, 2006 6:38 PM
[redacted]
Subject: RE: NETCOM Email (UNCLASSIFIED)

Classification: UNCLASSIFIED

Caveats: NONE

Steve,

good news and bad news...

Good news you on board and have email

Bad news - [redacted] will be leaving sometime at the end of Aug which means you will be the principal lead for the AWRAC.

That means you will have day to day oversight of the three contractor's here and the 9 soldiers at the [redacted]. [redacted] and I will try to get out next week but believe we are scheduled for the 31st if that does not happen. Don't expect that your work flow will change much but will require you to come into office occasionally. We will cover your local travel cost when that happens.

Let you know more when we get together..

J

[redacted]
CIO/G6 NETC ESTA, OIA&C
[redacted]
"Our Army at War -- Relevant and Ready"

[redacted]
Sent: Thursday, July 20, 2006 3:54 PM
[redacted]
Subject: NETCOM Email (UNCLASSIFIED)

Classification: UNCLASSIFIED

Caveats: NONE

[redacted]

I'm up on NETCOM Email and will use it as my primary Email for the next year. [redacted]

Classification: UNCLASSIFIED

Caveats: NONE

Classification: UNCLASSIFIED

Caveats: NONE

Classification: UNCLASSIFIED

Caveats: NONE

Classification: UNCLASSIFIED

Caveats: NONE

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

From: [redacted]
Sent: Tuesday, February 27, 2007 [redacted] M
To: [redacted]
Subject: FW: NOTIFICATION LETTERS (UNCLASSIFIED)
Signed By: [redacted]

Attachments: spouse notification letter (3).doc; HajjiiNet Ltr.doc


spouse notification letter (3)...


HajjiiNet Ltr.doc

Classification: UNCLASSIFIED
Caveats: NONE

-----Original Message-----
[redacted]
Sent: Tuesday, August 01, 2006 8:14 AM
[redacted]
Subject: NOTIFICATION LETTERS (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

Below is a example of notification letters.

V/R

[redacted]

Classification: UNCLASSIFIED
Caveats: NONE
Classification: UNCLASSIFIED
Caveats: NONE

Dear Sir/Ma'am

1. The Army Web Risk Assessment Cell (AWRAC) is currently monitoring U.S. Army affiliated Blog (Web Log). One of the Army foremost concerns is the safety and wellbeing of our troops. AWRAC assists in this endeavor by ensuring information on websites does not inadvertently provide information that may endanger our troops or their families. Computers recovered in Afghanistan and Iraq validate that enemies of the United States do monitor websites and Blogs looking for the type of information displayed on your Blog's site as described below. We have determined that this information constitutes a threat. Please contact the AWRAC for more information and guidance. This material should be removed as soon as possible.

(CUT AND PASTE AREA OF CONCERN)

AWRAC contact information

Hello [redacted]

I work for the Army Web Risk Assessment Cell (AWRAC). We are currently tasked with monitoring U.S. Army affiliated Blogs (Web Logs). One of the Army's foremost concerns is the safety and well-being of our troops. The AWRAC assists in this endeavor by ensuring information on websites does not inadvertently provide information that may endanger our troops or their families.

Computers recovered in Afghanistan and Iraq validate that enemies of the United States do monitor websites and Blogs. I am writing today to ask you if the Hajji net has any policies in place to ensure OPSEC information is not inadvertently provided to our adversaries.

[redacted]

From: [redacted]
Sent: Tuesday, February 27, 2007 7:37 AM
To: [redacted]
Subject: FW: [redacted] LETTER (UNCLASSIFIED)
Signed By: [redacted]

Attachments: [redacted]

Classification: UNCLASSIFIED
Caveats: NONE

-----Original Message-----
From: [redacted]
Sent: Wednesday, August 30, 2006 10:40 AM
To: [redacted]
Subject: HICKS LETTER (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]
LMIT Professional Services

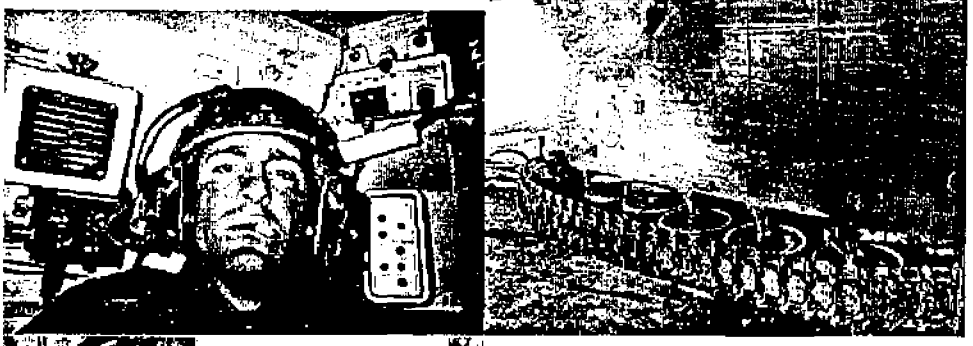
Information Assurance Directorate NETC-EST-A

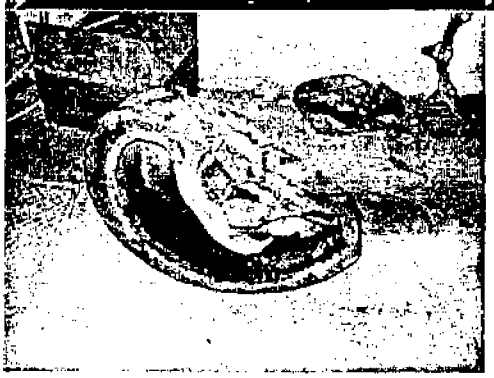
Army Web Risk Assessment Cell
[redacted]

Classification: UNCLASSIFIED
Caveats: NONE
Classification: UNCLASSIFIED
Caveats: NONE

Hello [redacted]

My name is [redacted], I work for the Army Web Risk Assessment Cell (AWRAC). We monitor U.S. Army affiliated Blog (Web Log). One of the Army foremost concerns is the safety and wellbeing of our troops. AWRAC assists in this endeavor by ensuring information on websites does not inadvertently provide information that may endanger our troops or their families. Computers recovered in Afghanistan and Iraq validate that enemies of the United States do monitor websites and Blogs. My concerns about your sight is the photos showing IED damage to our equipment. Please review and remove or block photos.

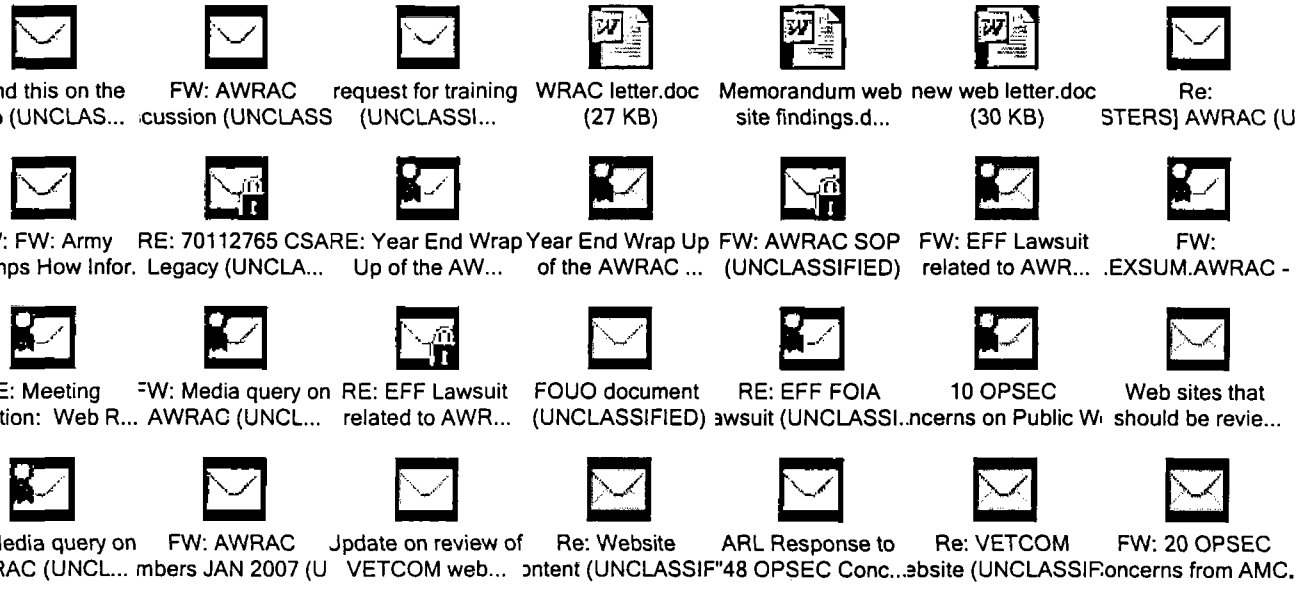


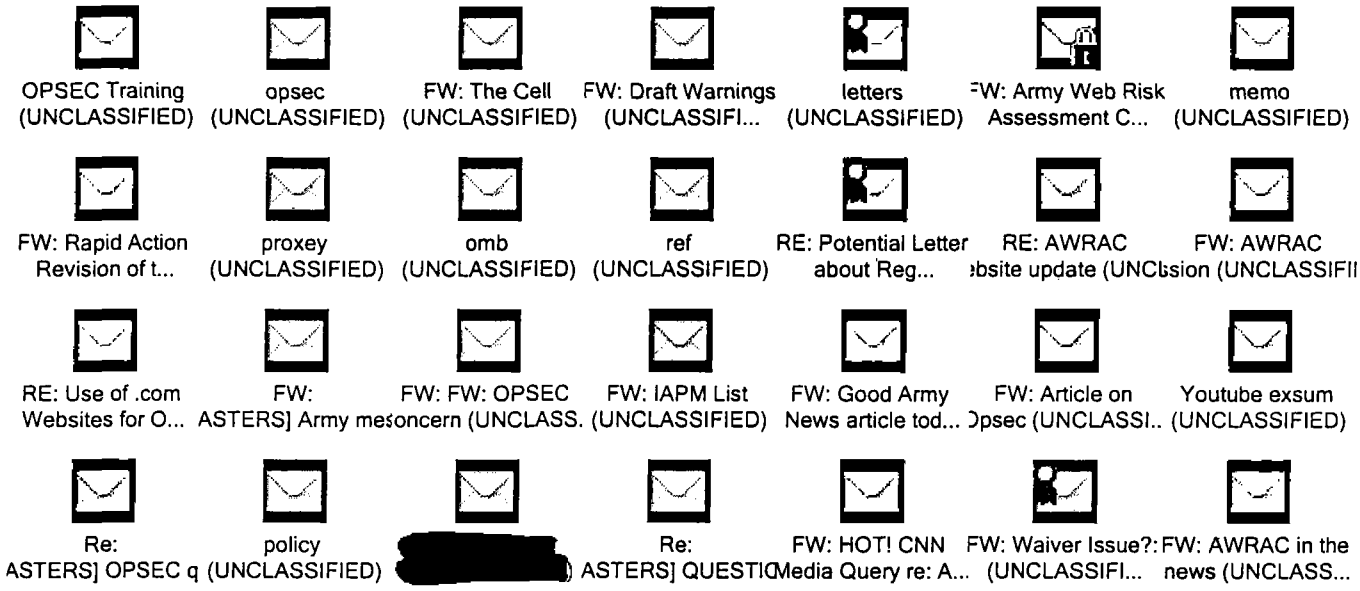


[redacted]

From: [redacted]
Sent: Monday, February 26, 2007 4:05 PM
To: [redacted]G6
Subject: Emails (UNCLASSIFIED)

Attachments: found this on the web (UNCLASSIFIED); FW: AWRAC discussion (UNCLASSIFIED); request for training (UNCLASSIFIED); WRAC letter.doc; Memorandum web site findings.doc; new web letter.doc; Re: [WEBMASTERS] AWRAC (UNCLASSIFIED); FW: FW: Army Revamps How Information Is Deemed Classified (UNCLASSIFIED); RE: 70112765 CSA Legacy (UNCLASSIFIED); RE: Year End Wrap Up of the AWRAC You Requested (UNCLASSIFIED); Year End Wrap Up of the AWRAC You Requested (UNCLASSIFIED); FW: AWRAC SOP (UNCLASSIFIED); FW: EFF Lawsuit related to AWRAC (UNCLASSIFIED); FW: 070130.EXSUM.AWRAC - Analysis of Army A-Z Websites.doc (UNCLASSIFIED); RE: Meeting Invitation: Web Risk Assessment Cell (UNCLASSIFIED); FW: Media query on AWRAC (UNCLASSIFIED); RE: EFF Lawsuit related to AWRAC (UNCLASSIFIED); FOUO document (UNCLASSIFIED); RE: EFF FOIA lawsuit (UNCLASSIFIED); 10 OPSEC Concerns on Public Website (UNCLASSIFIED); Web sites that should be reviewed. (UNCLASSIFIED); RE: Media query on AWRAC (UNCLASSIFIED); FW: AWRAC Numbers JAN 2007 (UNCLASSIFIED); Update on review of VETCOM website; Re: Website Content (UNCLASSIFIED); ARL Response to "48 OPSEC Concerns on Public Website" (UNCLASSIFIED); Re: VETCOM Website (UNCLASSIFIED); FW: 20 OPSEC Concerns from AMC Website (UNCLASSIFIED); OPSEC Training (UNCLASSIFIED); opsec (UNCLASSIFIED); FW: The Cell (UNCLASSIFIED); FW: Draft Warnings (UNCLASSIFIED); letters (UNCLASSIFIED); FW: Army Web Risk Assessment Cell (AWRAC) (UNCLASSIFIED); memo (UNCLASSIFIED); FW: Rapid Action Revision of the text changes to DA Pam 25-1-1, Information Technology Support and Services S:31 Aug (UNCLASSIFIED); proxey (UNCLASSIFIED); omb (UNCLASSIFIED); ref (UNCLASSIFIED); RE: Potential Letter about Registering in DTIC (UNCLASSIFIED); RE: AWRAC website update (UNCLASSIFIED); FW: AWRAC Mission (UNCLASSIFIED); RE: Use of .com Websites for Official Business (UNCLASSIFIED); FW: [WEBMASTERS] Army message (UNCLASSIFIED); FW: FW: OPSEC Concern (UNCLASSIFIED); FW: IAPM List (UNCLASSIFIED); FW: Good Army News article today (UNCLASSIFIED); FW: Article on Opsec (UNCLASSIFIED); Youtube exsum (UNCLASSIFIED); Re: [WEBMASTERS] OPSEC question (UNCLASSIFIED); policy (UNCLASSIFIED); [redacted] (UNCLASSIFIED); Re: [WEBMASTERS] QUESTION: .com Site?? (UNCLASSIFIED); FW: HOT! CNN Media Query re: Army blog policy (Desire response by 4 p.m. today) (UNCLASSIFIED); FW: Waiver Issue?: (UNCLASSIFIED); FW: AWRAC in the news (UNCLASSIFIED)





Classification: UNCLASSIFIED
Caveats: NONE

[redacted]
Lockheed Martin Mission Services

Information Assurance Directorate NETC-EST-A

Army Web Risk Assessment Cell
703-602-7481 (DSN 332)
703-602-3751 (Fax)
[redacted].army.mil
AKO IM User

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

From: [redacted]
Sent: Tuesday, October 31, 2006 10:21 AM
To: [redacted]

Subject: found this on the web (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

http://www.wired.com/news/politics/0,72026-0.html?tw=rss.index

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

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

From: [redacted]
Sent: Friday, November 03, 2006 12:52 PM
To: [redacted]
Subject: FW: AWRAC discussion (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

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

---

some of the comments from the Military.com discussion board on the AWRAC story.

[redacted]

Check These Out: <http://www.military.com/Military/Locator/New/Splash> Buddy Finder |
<http://shock.military.com/Shock/home.do> Videos |
<http://photocenter.military.com/smugmug/home.do> PhotoCenter |
<http://www.spousebuzz.com/> SpouseBUZZ |
<http://myfriends.military.com/friendnetwork/myFriends.do> My Friend Network |
<http://www.military.com/News/Home/0,,,00.html> News |
<http://tech.military.com/equipment/home.do> Military Equipment

<http://forums.military.com/eve>

Military.com <http://www.military.com/>
<http://forums.military.com/groupee_common/platform_images/blank.gif> Military.com
Forums <http://forums.military.com/eve/forums> <javascript:void(0);> Hop To Forum
Categories Hot Topics <http://forums.military.com/eve/forums/a/cfrm/f/81519858> &
Current Events <javascript:void(0);> Hop To Forums In the News
<http://forums.military.com/eve/forums/a/frm/f/672198221>
<http://forums.military.com/groupee_common/platform_images/blank.gif> Army Monitors
Soldiers' Blogs

Page 1 2 <http://forums.military.com/eve/forums/a/tpc/f/672198221/m/1880072590001/p/2> 3
<http://forums.military.com/eve/forums/a/tpc/f/672198221/m/1880072590001/p/3>

Moderators: BloodThirstyWench <javascript:void(0)> , dmuhler <javascript:void(0)> ,
DrillVietnamVet <javascript:void(0)> , OldAFcop <javascript:void(0)> , snake021
<javascript:void(0)>

Go <http://forums.military.com/groupee_common/platform_images/blank.gif>

New <http://forums.military.com/groupee_common/platform_images/blank.gif>

Find <http://forums.military.com/groupee_common/platform_images/blank.gif>

Notify <http://forums.military.com/groupee_common/platform_images/blank.gif>

Tools <http://forums.military.com/groupee_common/platform_images/blank.gif>

Reply <http://forums.military.com/groupee_common/platform_images/blank.gif>

<http://forums.military.com/groupee_common/platform_images/blank.gif>

Admin <http://forums.military.com/groupee_common/platform_images/blank.gif>

New PM! <http://forums.military.com/groupee_common/platform_images/blank.gif>

Personal <http://forums.military.com/eve/personal> Zone

?

Military.com <http://forums.military.com/eve/forums> Forums

?

Profile <http://forums.military.com/eve/personal?x_myspace_page=profile>

Buddies <http://forums.military.com/eve/personal?x_myspace_page=buddies>

Ignore <http://forums.military.com/eve/personal?x_myspace_page=ignore_list> List

Groups <http://forums.military.com/eve/personal?x_myspace_page=groups>

Permissions <http://forums.military.com/eve/personal?x_myspace_page=permissions>

Private <http://forums.military.com/eve?a=ugtpc> Messaging

Notifications <http://forums.military.com/eve/personal?x_myspace_page=subscriptions>

Karma <http://forums.military.com/eve/personal?x_myspace_page=karma>

Preferences <http://forums.military.com/eve/personal?x_myspace_page=uprefs>

Favorites <http://forums.military.com/eve/personal?
x_myspace_page=ufav&x_myspace_module=forums>

More... <http://forums.military.com/eve/personal?x_myspace_page=profile>

Discussion <javascript:void(0);>

Poll <javascript:void(0);>

Private Message <javascript:void(0);>

Keyword Search

Search current forum only

Advanced Search <http://forums.military.com/eve/forums?a=srchf>

New Since your Last Visit <http://forums.military.com/eve/forums?a=nslv>

Today's <http://forums.military.com/eve/forums?a=tat&c=81519858> Active Topics in this Category

Add to My Favorites <javascript:void(0);>

Printer
<http://forums.military.com/eve/forums/a/tpc/f/672198221/m/1880072590001/p/1/xsl/print_topic> Friendly Format

Email a Friend <javascript:void(0);>

Help <javascript:void(0);>

Manage Topic <javascript:void(0);>

Manage Content in This Topic <http://forums.military.com/eve?a=cp&x_show_template_page=afrmcntmgmt&x_show_searchby=topic_posts&x_show_template_module_oid=600106&x_show_topic_oid=1880072590001&x_show_forum=672198221>

Manage Members <http://forums.military.com/eve/cp?x_show_template_page=ammgmt&x_show_template_module_oid=500106>

Online Now <http://forums.military.com/eve/cp?x_show_template_page=aolnow&x_show_template_module_oid=500106>

Control Panel <http://forums.military.com/eve/cp>

Login/Join <http://forums.military.com/eve/login> Welcome, [Logout <http://forums.military.com/eve/logout>]

TeamAmerica <javascript:void(0)>

Member
Picture of TeamAmerica <http://www.themoviespot.net/images/image91.jpg>

<http://forums.military.com/eve/forums/a/tpc/f/672198221/m/1880072590001?r=1880072590001#1880072590001>

Posted Mon 30 October 2006 11:52

Mon 30 October 2006 11:52

RE: http://www.military.com/NewsContent/0,13319,117978,00.html

Posts: <http://forums.military.com/eve/forums?a=userposts&sortType=1&u=7210097830001>
1377 | Registered: Sat 17 December 2005

<javascript:void(0);> Reply With Quote <javascript:void(0);> Edit or Delete Message <http://forums.military.com/eve/forums?a=ma&m=1880072590001&t=1880072590001&f=672198221> Report This Post

scooter_mech <javascript:void(0)>

Member
Picture of scooter_mech <http://i12.photobucket.com/albums/a241/skywise8/images.jpg>

<http://forums.military.com/eve/forums/a/tpc/f/672198221/m/1880072590001?r=6850082590001#6850082590001>

Posted Mon 30 October 2006 12:19

Mon 30 October 2006 12:19

<javascript:void(0);> Hide Post

"In one incident, a blogger was describing his duties as a guard, providing pictures of his post and discussing how to exploit its vulnerabilities. Other Soldiers posted photos of an Army weapons system that was damaged by enemy attack, and another showed personal information that could have endangered his family."

This is not the kind of info that should NOT fall into enemy hands. What do you think, TeamAmerica since this is your thread....

Posts: <http://forums.military.com/eve/forums?a=userposts&sortType=1&u=3470063020001>
1651 | Registered: Fri 09 September 2005

<javascript:void(0);> Reply With Quote <javascript:void(0);> Edit or Delete Message <http://forums.military.com/eve/forums?a=ma&m=6850082590001&t=1880072590001&f=672198221> Report This Post

Ignored post by scooter_mech <javascript:void(0)> posted Mon 30 October 2006 12:19

Mon 30 October 2006 12:19

Show Post <javascript:void(0);>

[redacted] <javascript:void(0)>

Basic Training
Picture of Dutch_Shaulis
<http://forums.military.com/groupee_files/avatars/5/6/1/5610023290001/avatar.jpg>

<http://forums.military.com/eve/forums/a/tpc/f/672198221/m/1880072590001?r=6020092590001#6020092590001>

Posted Mon 30 October 2006 12:26

Mon 30 October 2006 12:26

<javascript:void(0);> Hide Post

Got to agree with Scooter on this one. Let's not give our enemies anymore information especially unit routes. Where's the common sense here? Remember the "Loose Lips Sink Ships", think they need to start reinforcing that again!!

"Retired Navy and Damn Proud of it!!!"

Posts: <http://forums.military.com/eve/forums?a=userposts&sortType=1&u=5610023290001> 19 | Registered: Thu 12 October 2006

<javascript:void(0);> Reply With Quote <javascript:void(0);> Edit or Delete Message <http://forums.military.com/eve/forums?a=ma&m=6020092590001&t=1880072590001&f=672198221> Report This Post

Ignored post by Dutch_Shaulis <javascript:void(0)> posted Mon 30 October 2006 12:26

Mon 30 October 2006 12:26

Show Post <javascript:void(0);>

cinlurker <javascript:void(0)>

Member

<http://forums.military.com/eve/forums/a/tpc/f/672198221/m/1880072590001?r=7920092590001#7920092590001>

Posted Mon 30 October 2006 12:36

Mon 30 October 2006 12:36

<javascript:void(0);> Hide Post

quote:

Originally posted by scooter_mech:
"In one incident, a blogger was describing his duties as a guard, providing pictures of his post and discussing how to exploit its vulnerabilities. Other Soldiers posted photos of an Army weapons system that was damaged by enemy attack, and another showed personal information that could have endangered his family."

This is not the kind of info that should NOT fall into enemy hands. What do you think, TeamAmerica since this is your thread....

THERE MIGHT BE A FEW INSTANCES WHERE A SERVICE PERSON DOES SOMETHING STUPID BUT THEN SOME COLONEL OR GENERAL DECIDED TO LET THE CHINESE LOOK AT SOME OF OUR MILITARY BASES...

IF THAT DOESN'T TAKE THE CAKE FOR "DUMB" NOTHING DOES.

Posts: <http://forums.military.com/eve/forums?a=userposts&sortType=1&u=6310095620001> 408 | Registered: Wed 12 October 2005

<javascript:void(0);> Reply With Quote <javascript:void(0);> Edit or Delete Message <http://forums.military.com/eve/forums?a=ma&m=7920092590001&t=1880072590001&f=672198221> Report This Post

Ignored post by cinlurker <javascript:void(0)> posted Mon 30 October 2006 12:36

Mon 30 October 2006 12:36

Show Post <javascript:void(0);>

outlaws93 <javascript:void(0)>

Experienced Member
Picture of outlaws93
<http://forums.military.com/groupee_files/avatars/8/3/7/8370097510001/avatar.jpg>

<http://forums.military.com/eve/forums/a/tpc/f/672198221/m/1880072590001?r=6640092590001#6640092590001>

Posted Mon 30 October 2006 12:51

Mon 30 October 2006 12:51

<javascript:void(0);> Hide Post

quote:

Originally posted by cinlurker:

quote:

Originally posted by scooter_mech:
"In one incident, a blogger was describing his duties as a guard, providing pictures of his post and discussing how to exploit its vulnerabilities. Other Soldiers posted photos of an Army weapons system that was damaged by enemy attack, and another showed personal information that could have endangered his family."

This is not the kind of info that should NOT fall into enemy hands. What do you think, TeamAmerica since this is your thread....

THERE MIGHT BE A FEW INSTANCES WHERE A SERVICE PERSON DOES SOMETHING STUPID BUT THEN SOME COLONEL OR GENERAL DECIDED TO LET THE CHINESE LOOK AT SOME OF OUR MILITARY BASES...

IF THAT DOESN'T TAKE THE CAKE FOR "DUMB" NOTHING DOES.

sure and it was monatered... they didnt see everything and anything they didnt need to see \know about....

<http://i45.photobucket.com/albums/f53/outlaws93/15.gif>

Posts: <http://forums.military.com/eve/forums?a=userposts&sortType=1&u=8370097510001>
9870 | Registered: Thu 18 August 2005

<javascript:void(0);> Reply With Quote <javascript:void(0);> Edit or Delete Message
<http://forums.military.com/eve/forums?a=ma&m=6640092590001&t=1880072590001&f=672198221>
Report This Post

Ignored post by outlaws93 <javascript:void(0)> posted Mon 30 October 2006 12:51

Mon 30 October 2006 12:51

Show Post <javascript:void(0);>

TheGoodOne <javascript:void(0)>

Member

<http://forums.military.com/eve/forums/a/tpc/f/672198221/m/1880072590001?r=5150092590001#5150092590001>

Posted Mon 30 October 2006 12:56

Mon 30 October 2006 12:56

<javascript:void(0);> Hide Post

Roll Eyes <http://forums.military.com/groupee_common/emoticons/icon_rolleyes.gif> When they are done here, they need to focus on those responsible for letting our enemies inside our own country.

Posts: <http://forums.military.com/eve/forums?a=userposts&sortType=1&u=3331938856> 371 |
Registered: Thu 19 June 2003

<javascript:void(0);> Reply With Quote <javascript:void(0);> Edit or Delete Message
<http://forums.military.com/eve/forums?a=ma&m=5150092590001&t=1880072590001&f=672198221>
Report This Post

Ignored post by TheGoodOne <javascript:void(0)> posted Mon 30 October 2006 12:56

Mon 30 October 2006 12:56

Show Post <javascript:void(0);>

cafedad <javascript:void(0)>

Basic Training
Picture of cafedad
<http://forums.military.com/groupee_files/avatars/3/1/6/3161999416/avatar.bmp>

<http://forums.military.com/eve/forums/a/tpc/f/672198221/m/1880072590001?r=9960092590001#9960092590001>

Posted Mon 30 October 2006 13:18

Mon 30 October 2006 13:18

<javascript:void(0);> Hide Post

quote:

Let's not give our enemies anymore information especially unit routes. Where's the common sense here? Remember the "Loose Lips Sink Ships", think they need to start reinforcing that again!!

"Retired Navy and Damn Proud of it!!!"

Your right Dutch, Loose lips... what happend to OPSEC?? Just because we have a younger Army doesn't mean the "old school" ways are not still in use. THINK SOLDIERS, THINK!!!!

Posts: <http://forums.military.com/eve/forums?a=userposts&sortType=1&u=3161999416> 24 |
Registered: Tue 28 January 2003

<javascript:void(0);> Reply With Quote <javascript:void(0);> Edit or Delete Message
<http://forums.military.com/eve/forums?a=ma&m=9960092590001&t=1880072590001&f=672198221>
Report This Post

Ignored post by cafedad <javascript:void(0)> posted Mon 30 October 2006 13:18

Mon 30 October 2006 13:18

Show Post <javascript:void(0);>

GroovyLady <javascript:void(0)>

Member
Picture of GroovyLady
<http://forums.military.com/groupee_common/platform_images/avatars/set1/59.jpg>

<http://forums.military.com/eve/forums/a/tpc/f/672198221/m/1880072590001?r=1720003590001#1720003590001>

Posted Mon 30 October 2006 13:48

Mon 30 October 2006 13:48

<javascript:void(0);> Hide Post

yeah, and, we get tours of Russia's nuclear facilities and weapons manufacturers.

quote:

Originally posted by cinlurker:
THERE MIGHT BE A FEW INSTANCES WHERE A SERVICE PERSON DOES SOMETHING STUPID BUT THEN SOME COLONEL OR GENERAL DECIDED TO LET THE CHINESE LOOK AT SOME OF OUR MILITARY BASES...

IF THAT DOESN'T TAKE THE CAKE FOR "DUMB" NOTHING DOES.

Posts: <http://forums.military.com/eve/forums?a=userposts&sortType=1&u=9510032630001>
2018 | Registered: Mon 05 December 2005

<javascript:void(0);> Reply With Quote <javascript:void(0);> Edit or Delete Message
<http://forums.military.com/eve/forums?a=ma&m=1720003590001&t=1880072590001&f=672198221>
Report This Post

Ignored post by GroovyLady <javascript:void(0)> posted Mon 30 October 2006 13:48

Mon 30 October 2006 13:48

Show Post <javascript:void(0);>

rd350 <javascript:void(0)>

Member

Picture of rd350
<http://forums.military.com/groupee_files/avatars/2/8/4/284106245/avatar.jpg>

<http://forums.military.com/eve/forums/a/tpc/f/672198221/m/1880072590001?r=1990092590001#1990092590001>

Posted Mon 30 October 2006 13:56

Mon 30 October 2006 13:56

<javascript:void(0);> Hide Post

quote:

yeah, and, we get tours of Russia's nuclear facilities and weapons manufacturers.

Not that far off the mark.

http://travel2.nytimes.com/2006/10/15/travel/15transiran.html

"An Invitation From Iran: Inspect It for Yourself If you have ever wanted to see the inside of a pressurized nuclear reactor plant, Iran could be the next adventure vacation for you."

personally myself? BTDT

Posts: <http://forums.military.com/eve/forums?a=userposts&sortType=1&u=284106245> 241 | Registered: Thu 27 January 2005

<javascript:void(0);> Reply With Quote <javascript:void(0);> Edit or Delete Message <http://forums.military.com/eve/forums?a=ma&m=1990092590001&t=1880072590001&f=672198221> Report This Post

Ignored post by rd350 <javascript:void(0)> posted Mon 30 October 2006 13:56

Mon 30 October 2006 13:56

Show Post <javascript:void(0);>

8718368 <javascript:void(0)>

Member
Picture of 8718368
<http://forums.military.com/groupee_files/avatars/1/2/0/1200019240001/avatar.JPG>

<http://forums.military.com/eve/forums/a/tpc/f/672198221/m/1880072590001?r=4930003590001#4930003590001>

Posted Mon 30 October 2006 14:05

Mon 30 October 2006 14:05

<javascript:void(0);> Hide Post

Well, I see no problem in enforcing OPSEC. The only problem some soldiers seem to have is just ambigous rules. Clear those up and everyone will be happy, especially those serving in FOBs and active combat zones.

In God we Trust,
Scott

Posts: <http://forums.military.com/eve/forums?a=userposts&sortType=1&u=1200019240001> 52 | Registered: Fri 06 January 2006

<javascript:void(0);> Reply With Quote <javascript:void(0);> Edit or Delete Message <http://forums.military.com/eve/forums?a=ma&m=4930003590001&t=1880072590001&f=672198221> Report This Post

Ignored post by 8718368 <javascript:void(0)> posted Mon 30 October 2006 14:05

Mon 30 October 2006 14:05

Show Post <javascript:void(0);>

GroovyLady <javascript:void(0)>

Member
Picture of GroovyLady
<http://forums.military.com/groupee_common/platform_images/avatars/set1/59.jpg>

<http://forums.military.com/eve/forums/a/tpc/f/672198221/m/1880072590001?r=2240003590001#2240003590001>

Posted Mon 30 October 2006 14:09

Mon 30 October 2006 14:09

<javascript:void(0);> Hide Post

the American public's plan might call for a quick withdrawal and a series of appeasement measures to get our troops out of Iraq.

However, that's not the Jihadist's plan. We leave Iraq; they will continue to hunt our troops here and abroad. 1989 and then from 1993 - 2000 they've demonstrated they're quite capable of attacking our troops while our troops are not under a wartime command.

Obviously, jihadists realize they can't take us down quickly. They will have to simulataneously attack our economy, attack our foreign policies/diplomatic efforts, attack the popular will of the people in our country (i.e. using enemy propaganda as valid news sources, etc.) and get busy weakening our defense systems. the largest component of our defense system are our troops.

At the time of Alexander the Great's crusade to conquor Persia; the Perisan military's strongest core of fighters were Greek mercenaries whom the Persians paid quite well. Regardless that Alexander unified Greece and became the leader of the Greek states; many Greeks still got bought and fought on the side of their countrymen's enemy, the Persians.

it wouldn't surprise me in the least to see our enemy employ that tactic again. hence, the necessity of blog monitoring/security to minimize risk of exposing our troops and their families to the threat of our enemy. would kind of suck for a troop's spouse, child or parent (or even close friends) to get kidnapped with the ransom being the soldier's submission to fight the jihad against us Americans.

Posts: <http://forums.military.com/eve/forums?a=userposts&sortType=1&u=9510032630001>
2018 | Registered: Mon 05 December 2005

<javascript:void(0);> Reply With Quote <javascript:void(0);> Edit or Delete Message
<http://forums.military.com/eve/forums?a=ma&m=2240003590001&t=1880072590001&f=672198221>
Report This Post

Ignored post by GroovyLady <javascript:void(0)> posted Mon 30 October 2006 14:09

Mon 30 October 2006 14:09

Show Post <javascript:void(0);>

rd350 <javascript:void(0)>

Member
Picture of rd350
<http://forums.military.com/groupee_files/avatars/2/8/4/284106245/avatar.jpg>

<http://forums.military.com/eve/forums/a/tpc/f/672198221/m/1880072590001?r=2010013590001#2010013590001>

Posted Mon 30 October 2006 14:16

Mon 30 October 2006 14:16

<javascript:void(0);> Hide Post

This is an interesting topic (the topic is bloggin soldiers, isn't it?) ? being out for so long, I am amazed that blogging and email are so commonplace, bu considering the emotional cost of being separated from family, if this technology can help, it has to make the troops more effective.

On the other hand, I have seeen all too many disturbing videos that anyone could use to characterize our men as cowboys, and I?m sure there are less than positive rantings on the blogs. We?ve opened the www.pandorasbox <http://www.pandorasbox/> now and pulling back the reigns would be hard.

We had deployments where we didn?t even see (snail) mail or phone calls or anything for more than a month. I also remember the excitement of spending nearly $30 US in 1975 dollars to be able to call home as soon as we hit port.. In that relative light, being allowed ot email once a day seems (in retrospect) to be a luxury.

Posts: <http://forums.military.com/eve/forums?a=userposts&sortType=1&u=284106245> 241 |

Registered: Thu 27 January 2005

<javascript:void(0);> Reply With Quote <javascript:void(0);> Edit or Delete Message <http://forums.military.com/eve/forums?a=ma&m=2010013590001&t=1880072590001&f=672198221> Report This Post

Ignored post by rd350 <javascript:void(0)> posted Mon 30 October 2006 14:16

Mon 30 October 2006 14:16

Show Post <javascript:void(0);>

Troll116 <javascript:void(0)>

Basic Training

<http://forums.military.com/eve/forums/a/tpc/f/672198221/m/1880072590001?r=3560003590001#3560003590001>

Posted Mon 30 October 2006 14:46

Mon 30 October 2006 14:46

<javascript:void(0);> Hide Post

It sure seems to me that the potential here should not be over looked. What a fantastic opportunity to invite some of our friends to an ambush.

Posts: <http://forums.military.com/eve/forums?a=userposts&sortType=1&u=3320011070001> 17 | Registered: Mon 29 May 2006

<javascript:void(0);> Reply With Quote <javascript:void(0);> Edit or Delete Message <http://forums.military.com/eve/forums?a=ma&m=3560003590001&t=1880072590001&f=672198221> Report This Post

Ignored post by Troll116 <javascript:void(0)> posted Mon 30 October 2006 14:46

Mon 30 October 2006 14:46

Show Post <javascript:void(0);>

juice68 <javascript:void(0)>

Member

<http://forums.military.com/eve/forums/a/tpc/f/672198221/m/1880072590001?r=5760013590001#5760013590001>

Posted Mon 30 October 2006 15:44

Mon 30 October 2006 15:44

<javascript:void(0);> Hide Post

quote:

In one incident, a blogger was describing his duties as a guard, providing pictures of his post and discussing how to exploit its vulnerabilities. Other Soldiers posted photos of an Army weapons system that was damaged by enemy attack, and another showed personal information that could have endangered his family."

seems like its commonsence not to do that kind of thing. what was he thinking!!! duh!!

Posts: <http://forums.military.com/eve/forums?a=userposts&sortType=1&u=4570008460001>
2024 | Registered: Mon 24 April 2006

<javascript:void(0);> Reply With Quote <javascript:void(0);> Edit or Delete Message
<http://forums.military.com/eve/forums?a=ma&m=5760013590001&t=1880072590001&f=672198221>
Report This Post

Ignored post by juice68 <javascript:void(0)> posted Mon 30 October 2006 15:44

Mon 30 October 2006 15:44

Show Post <javascript:void(0);>

rd350 <javascript:void(0)>

Member
Picture of rd350
<http://forums.military.com/groupee_files/avatars/2/8/4/284106245/avatar.jpg>

<http://forums.military.com/eve/forums/a/tpc/f/672198221/m/1880072590001?r=2530023590001#
2530023590001>

Posted Mon 30 October 2006 16:41

Mon 30 October 2006 16:41

<javascript:void(0);> Hide Post

both my grandfather (WWI horse cavalry) and my Dad (WWII, Seabee) had their mail censored and heavily edited.

the technology is there to flag word strings and graphics. What I'm seeing as the most counterproductive are the digital videos being floated around.

Posts: <http://forums.military.com/eve/forums?a=userposts&sortType=1&u=284106245> 241 | Registered: Thu 27 January 2005

<javascript:void(0);> Reply With Quote <javascript:void(0);> Edit or Delete Message <http://forums.military.com/eve/forums?a=ma&m=2530023590001&t=1880072590001&f=672198221> Report This Post

Ignored post by rd350 <javascript:void(0)> posted Mon 30 October 2006 16:41

Mon 30 October 2006 16:41

Show Post <javascript:void(0);>

[redacted] <javascript:void(0)>

Member

<http://forums.military.com/eve/forums/a/tpc/f/672198221/m/1880072590001?r=3730023590001#3730023590001>

Posted Mon 30 October 2006 16:44

Mon 30 October 2006 16:44

<javascript:void(0);> Hide Post

quote:

Originally posted by scooter_mech:
"In one incident, a blogger was describing his duties as a guard, providing pictures of his post and discussing how to exploit its vulnerabilities. Other Soldiers posted photos of an Army weapons system that was damaged by enemy attack, and another showed personal information that could have endangered his family."

This is not the kind of info that should NOT fall into enemy hands. What do you think, TeamAmerica since this is your thread....

I don't think it's OPSEC the DoD is worried about. We've been blogging since the beginning of the invasion and occupation.

Posts: <http://forums.military.com/eve/forums?a=userposts&sortType=1&u=2800025140001> 845 | Registered: Sat 31 December 2005

<javascript:void(0);> Reply With Quote <javascript:void(0);> Edit or Delete Message <http://forums.military.com/eve/forums?a=ma&m=3730023590001&t=1880072590001&f=672198221> Report This Post

Ignored post by mcgreer <javascript:void(0)> posted Mon 30 October 2006 16:44

Mon 30 October 2006 16:44

Show Post <javascript:void(0);>

Copper71 <javascript:void(0)>

Member
Picture of Copper71
<http://forums.military.com/groupee_files/avatars/9/8/0/9800001090001/avatar.png>

<http://forums.military.com/eve/forums/a/tpc/f/672198221/m/1880072590001?r=6630053590001#6630053590001>

Posted Mon 30 October 2006 19:31

Mon 30 October 2006 19:31

<javascript:void(0);> Hide Post

Remember that old WW2 saying, "Loose lips sink ships." Those words are as true today as they were then. If anyone thinks the enemy isn't logging in to the blogs, they had better shake their heads. Sometimes the bloggers go overboard with the information they post. The reason they get generous with info. can be anything from trying to impress a woman/man, dazzle mom & dad or just plain DUMB. There is something to be said for some censorship.

Posts: <http://forums.military.com/eve/forums?a=userposts&sortType=1&u=9800001090001> 102 | Registered: Sun 01 October 2006

<javascript:void(0);> Reply With Quote <javascript:void(0);> Edit or Delete Message <http://forums.military.com/eve/forums?a=ma&m=6630053590001&t=1880072590001&f=672198221> Report This Post

Ignored post by Copper71 <javascript:void(0)> posted Mon 30 October 2006 19:31

Mon 30 October 2006 19:31

Show Post <javascript:void(0);>

Schistosome <javascript:void(0)>

Member
Picture of Schistosome
<http://forums.military.com/groupee_files/avatars/9/9/0/9900030290001/avatar.jpg>

<http://forums.military.com/eve/forums/a/tpc/f/672198221/m/1880072590001?r=8950043590001#8950043590001>

Posted Mon 30 October 2006 20:05

Mon 30 October 2006 20:05

<javascript:void(0);> Hide Post

with all the training we receive... what made his dumb *** blog such critical stuff??? what next... yes monitor it and stop this nonsense. we can blog on the safe stuff.

Posts: <http://forums.military.com/eve/forums?a=userposts&sortType=1&u=9900030290001> 73 | Registered: Wed 11 October 2006

<javascript:void(0);> Reply With Quote <javascript:void(0);> Edit or Delete Message <http://forums.military.com/eve/forums?a=ma&m=8950043590001&t=1880072590001&f=672198221> Report This Post

Ignored post by Schistosome <javascript:void(0)> posted Mon 30 October 2006 20:05

Mon 30 October 2006 20:05

Show Post <javascript:void(0);>

mcgreer <javascript:void(0)>

Member

<http://forums.military.com/eve/forums/a/tpc/f/672198221/m/1880072590001?r=5060043590001#5060043590001>

Posted Mon 30 October 2006 20:06

Mon 30 October 2006 20:06

<javascript:void(0);> Hide Post

Again, it probably isn't OPSEC the DoD's worried about.

A majority of these guys are smart enough to not post things that will get them and their buddies killed. And we know that. Consider that there's a lot of negative sentiment about the occupation right now. That we're in an election cycle. And that guys and gals who have been sent back into the breach for the fourth time, experiencing family problems as a result, questioning their own presence there, might have a little to say in these blogs.

Now, we understand perfectly that a majority of our troops serve faithfully and will not do anything that will bring discredit upon themselves, their units, their service, or their country. But this is turning into a long, hard slog. People are going to start pouring out their feelings on these things. Putting your business in the street via blogs and other public web sites is normal with many of our young people these days.

Do you remember the amateur porn site that offered GIs free membership if they would post photos from the field? I went there once, out of curiosity. The pictures some of our troopers were posting were not pretty; in fact, many of them made the Abu Ghraib photos look like a Sunday school outing. They were incredibly graphic and horribly gruesome.

There is a sense that our experience in Iraq is not going well, and there will be efforts to try to stop the flow of negative information as much as possible.

OPSEC? Probably not. PR? Probably more accurate.

Posts: <http://forums.military.com/eve/forums?a=userposts&sortType=1&u=2800025140001> 845 | Registered: Sat 31 December 2005

<javascript:void(0);> Reply With Quote <javascript:void(0);> Edit or Delete Message <http://forums.military.com/eve/forums?a=ma&m=5060043590001&t=1880072590001&f=672198221> Report This Post

Ignored post by [redacted] <javascript:void(0)> posted Mon 30 October 2006 20:06

Mon 30 October 2006 20:06

Show Post <javascript:void(0);>

reconhottie <javascript:void(0)>

Member
Picture of reconhottie
<http://forums.military.com/groupee_files/avatars/2/3/3/2330047140001/avatar.jpg>

<http://forums.military.com/eve/forums/a/tpc/f/672198221/m/1880072590001?r=9400073590001#9400073590001>

Posted Mon 30 October 2006 22:10

Mon 30 October 2006 22:10

<javascript:void(0);> Hide Post

What is next? Listing names, location, units and the like on a blog? Maybe invite the bad guys to look at it and take notes? Why the hell not straight invite them on bases to save them the effort of looking up sensitive info online, info posted by soldiers who think it is interesting to do.
OPSEC is not so hard to understand and remember. If they are doing this just to have a way to vent, they need to think twice about it. About what is ok to post and what not.

Classification: UNCLASSIFIED
Caveats: NONE

[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

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.

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 (XXXXXXXXXXXXXXXXXXXXX) 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

[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
202-492-7797
[redacted]

Classification: UNCLASSIFIED
Caveats: NONE

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

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

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.

[redacted]

From: [redacted]
Sent: Tuesday, November 21, 2006 2:17 PM
To: [redacted]

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: Friday, February 09, 2007 5:22 PM
To: [redacted]
Cc:
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 COL 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...

[redacted]

-----Original Message-----
[redacted]
Sent: Thursday, February 08, 2007 6:45 PM
[redacted]
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

[redacted]

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

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.

[redacted] 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

[redacted]

From: [redacted]
Sent: Thursday, February 08, 2007 11:20 AM
To: [redacted]
Cc: [redacted]

Subject: FW: AWRAC SOP (UNCLASSIFIED)
Signed By: [redacted]@us.army.mil

Classification: UNCLASSIFIED
Caveats: NONE

FYI - Info [redacted] sent to NETCOM C of S.

[redacted]

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

-----Original Message-----
[redacted]
Sent: Thursday, February 08, 2007 8:47 AM
[redacted]
Subject: FW: AWRAC SOP (UNCLASSIFIED)

[redacted]

Here it is.

[redacted]

-----Original Message-----
[redacted]
Sent: Tuesday, February 06, 2007 2:21 PM
[redacted]
Subject: FW: AWRAC SOP (UNCLASSIFIED)

[redacted]

[redacted] is in training this afternoon.

I called the U.S. District Court and requested the pleadings. They wanted a faxed request which I sent out. I have also tried to call the attorney for the Electronic Freedom Foundation named in the article without success. I will keep trying.

Below is an e-mail from [redacted] to his folks about the lawsuit. Apparently, all FOIA requests and the lawsuit were directed to and against DOD.

Based on [redacted] information, this is a FOIA lawsuit against DOD asking for information. I will try to find out who is handling it at DOD. The worst case scenario from such a lawsuit is we have to give information and possible attorneys' fees.

Obviously, the FOIA request is the first salvo in exploring the legality of what it is the AWRAC is doing. I helped develop the SOP and if it is

being followed, we should be on safe ground. Basically, our people are not intelligence assets and not subject to AR 381-10 intelligence oversight. They only review either AKO or publicly available blogs and websites on the internet. They are only looking for OPSEC violations, not free speech issues. If they can identify the source of the information, they send a gentle e-mail asking the person to desist. Most responses they get are positive. If they cannot determine the source of the information, they do not investigate. They have the ability to turn over to law enforcement or counterintelligence investigators, but I am told they haven't had much luck in doing so. If they can identify the source of the information and the source won't desist, they will notify the chain of command.

Since I approved the SOP, obviously I don't think any legal challenge will be sustained, provided we are following the SOP. As with any lawsuit, the ultimate decision is with the court. Also, decisions on litigation strategies and settlement must factor in the Department of Justice viewpoints. At this time, I think we are on solid ground.

With regard to the NETCOM statements, I had reviewed them last week and have no objection. This is not a covert mission, and I think we would do more harm than good by not fielding inquiries. We have had and answered media inquiries before.

My recommendation would be to continue to field questions about the AWRAC mission unless and until we are advised to stop by DA, DOD, or DOJ. Any questions about the lawsuit itself should be referred to DOD/DOJ.

[redacted]

-----Original Message-----
[redacted]
Sent: Tuesday, February 06, 2007 1:01 PM
[redacted]
Subject: FW: AWRAC SOP (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

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

-----Original Message-----
[redacted]
Sent: Monday, February 05, 2007 9:46 AM
[redacted]
Subject: AWRAC SOP (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

ALCON,

I know that I sound like a broken record -- but -- you are probably aware that a Privacy Group is suing DoD for release of FIOA information concerning the AWRAC. The privacy group wants this to be an expedited FOIA release

rather than a normal FOIA release -- that is what the suite is about. I have no idea what the outcome will be or when it will be resolved.

Bottom line - eventually a FIOA will be honored.

I am sure you have followed our SOP and we are sticking to our review of potential OPSEC and Privacy content violations contained in publicly accessible information. This may be the time to do a make sure all "Ts" are crossed and "Is" are dotted.

I understand that we also receive information from WASH state NGB - I assume they are well aware of the conditions for this mission -- and that will be reinforced during the upcoming training event.

This is also a great time to be thankful that we are not associated with any intelligence gathering. Other wise this would be very difficult. I think you can now see why we were so adamant that we cannot be associated with intelligence gathering.

Now is the time to make sure that all your information is properly marked FOUO when required per existing SOP. Since what we review is publicly accessible - may not be a lot marked FOUO.

One legal item to be aware of -- now that you know a FOIA is coming -- you cannot decide that all information that we have will be marked FOUO which precludes release under FIOA. You can look and see if there is any information that according to your SOP should have been FOUO but was over looked (meaning --- that in general -- due to an item in the SOP -- if you had all along been marking something FOUO and you forgot one or two items that was part of a large group of items -- no problem -- but you cannot decide to make something FOUO simply for the intent of avoiding a FOIA release -- some what like back dating your stock options -- that is illegal. To decide today that everything done to this date must be FOUO to preclude release under FIOA is illegal. Do not go there.

Based on our legal review and training we will be O.K. . Please do not make any disparaging remarks about the group asking for the FOIA release and executing the law suite. They are executing their mission as a watch dog for privacy concerns and FOIA request are legally codified. Basically they are doing their job.

Please make sure that everyone supporting this mission is aware of what is in this email:

-- There is a FOIA request
-- Privacy Advocate Group is suing DoD for an expedited release of FOIA information
-- Make sure all elements are following our SOP
-- Make sure everyone understands that we will not start marking everything FOUO to preclude release under FOIA
-- No disparaging remarks concerning the privacy advocacy group -- they are doing their job, and using legally codified processes to obtain information.

-- As long as we review Army publicly accessible information for OPSEC and Privacy content violations -- we are O.K..

Remember -- your best intentions can only be used as a mitigating factor at the sentencing phase of your trial !! We are O.K. -- we will just be asked to release information for a FOIA - do not know when we will be asked to support the FOIA action.

[redacted]

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

[redacted]

Classification: UNCLASSIFIED
Caveats: NONE

Classification: UNCLASSIFIED
Caveats: NONE

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

From: [redacted]
Sent: Monday, February 05, 2007 3:54 PM
To: [redacted]
Cc:
Subject: FW: 070130.EXSUM.AWRAC - Analysis of Army A-Z Websites.doc (UNCLASSIFIED)
Signed By: [redacted]

Attachments: 070130.EXSUM.AWRAC - Analysis of Army A-Z Websites.doc

070130.EXSUM.A
WRAC - Analysis ...

Classification: UNCLASSIFIED
Caveats: NONE

What is the A-Z list ? Where is the site and what is the authority that directs web site owners to register at this site ?

[redacted]

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

-----Original Message-----
[redacted]
Sent: Tuesday, January 30, 2007 2:58 PM
[redacted]
Subject: 070130.EXSUM.AWRAC - Analysis of Army A-Z Websites.doc (UNCLASSIFIED)

Classification: UNCLASSIFIED

Caveats: NONE

For your review from LTC Warnock

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: [redacted]us.army.mil

Classification: UNCLASSIFIED
Caveats: NONE

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

[redacted]

[redacted]P
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]
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]

Classification: UNCLASSIFIED
Caveats: NONE

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

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

Subject: [redacted]
Signed By:

Importance: High

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

This is what we suggest as a response to [redacted]o (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]PA
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: Wednesday, February 15, 2006 3:25 PM
To: [redacted]
Cc:
Subject: FOUO document (UNCLASSIFIED)

Attachments: AMC.doc; Findings list.doc

AMC.doc (27 KB) Findings list.doc (46 KB)

Classification: UNCLASSIFIED
Caveats: NONE

https://iassure.usareur.army.mil/policy/iava/iavaitem.aspx?iavaID=118

IAPM -- 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 is publically accessible, and is marked FOUO. Please review the attached document for further guidance, and report resolution of this issue NLT 22 FEB 06.
Please contact me if you have questions.

[redacted]
Asset and Vulnerability Tracking Resource (A&VTR) PM Liaison AWRAC Analyst NETCOM (CIO/G6)
2530 Crystal Drive Arlington, VA 22202
[redacted]

"Press any key....hmmm, where's the any key?"

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

From: [redacted]
Sent: Thursday, December 14, 2006 12:08 PM
To: [redacted]
Subject: 10 OPSEC Concerns on Public Website (UNCLASSIFIED)
Signed By: [redacted]

Importance: High

Attachments: hood.xls; AMC.doc; Findings list.doc


hood.xls


AMC.doc


Findings list.doc

Classification: UNCLASSIFIED

Caveats: NONE

PAO-- The Army Web Risk Assessment Cell (AWRAC) is currently reviewing U.S. Army Web sites for OPSEC and security compliance. Ten OPSEC concerns were found on your organization's website and have been classified as major findings. The attached spreadsheet contains URLs that are publicly accessible, and are marked FOUO and contain personal information. Please review the attached documents for further guidance, and report resolution of these issue NLT 21 DEC 06.

Please contact me if you have questions.
<<...>> <<...>> <<...>>

R/,

[redacted]
Lockheed Martin Information Technology

Information Assurance Directorate NETC-EST-A

Army Web Risk Assessment Cell
703-602-7481 (DSN 332)
703-602-3751 (Fax)
[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
Fort Sam Houston, TX 78234

[redacted]
Fax: 6066

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

[redacted]

From: [redacted]
Sent: Thursday, February 01, 2007 3:40 PM
To: [redacted]
Subject: FW: AWRAC Numbers JAN 2007 (UNCLASSIFIED)

Attachments: AWRAC Numbers JAN 2007.ppt

AWRAC Numbers JAN 2007.ppt (85...

David,

Not sure if you remember me, we spoke on the phone briefly about the last AWRAC numbers. I'm curious if your team's done any decomposition of why the numbers went up so much in Web site violations and blogs?
Are you catching more due to better scanning / more staff, or are more occurring? What are your thoughts?

[redacted]
Army Enterprise Systems
The MITRE Corporation
[redacted]

-----Original Message-----
[redacted]
[mailto:[redacted]us.army.mil]
Sent: Thursday, February 01, 2007 9:24 AM
[redacted]
Subject: FW: AWRAC Numbers JAN 2007 (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: FOUO

[redacted]
Office of Information Assurance and Compliance
Army CIO/G-6, NETCOM
[redacted]

-----Original Message-----
[redacted]
Sent: Wednesday, January 31, 2007 11:34 AM
[redacted]
Subject: AWRAC Numbers JAN 2007 (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

Good Afternoon Sir,
I have attached the AWRAC Numbers for January 2007 to this email. As
always, please contact me if you have any questions.

<<...>>

[redacted]
Lockheed Martin Mission Services

Information Assurance Directorate NETC-EST-A

Army Web Risk Assessment Cell
[redacted]
AKO IM User

Classification: UNCLASSIFIED
Caveats: NONE

Classification: UNCLASSIFIED
Caveats: FOUO

[redacted]

From: [redacted]
Sent: Tuesday, January 30, 2007 11:11 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: <mailto:AWRAC@hqda.army.mil> AWRAC@hqda.army.mil

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

From: [redacted]
Sent: Tuesday, January 23, 2007 1:02 PM
To: [redacted]
Cc: [redacted]
ARL/CISD)
Subject: ARL Response to "48 OPSEC Concerns on Public Website" (UNCLASSIFIED)

Follow Up Flag: Follow up
Flag Status: Completed

Attachments: ARL-MEMO-25-70.pdf

ARL-MEMO-25-70.pdf (131 KB)

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

As per our conversation of January 9th, below is the response to your December email, "48 OPSEC Concerns on Public Website."

ARL is fully cognizant of the need to follow proper OPSEC procedures, as well as the DA and DoD guidance. In September of 2005, ARL used the established guidances in crafting its own regulations on how material would be published on the external internet site. This policy also <<ARL-MEMO-25-70.pdf>> took into account the need for flexibility to pursue ARL's stated mission as the Army's corporate laboratory, and reflected our dedication as an organization to proper OPSEC procedures.

We recognize that names and contact information are posted on the external server. However, the posted information pertains to recognized POCs for internal lab programs. Quoting the ARL memo, these POCs help ARL "act as the bridge between the science and technology community and the warfighter." The relevant section of the policy is below for your convenience. Additionally, I have attached the full policy in PDF form to this file.

With this in mind, ARL believes the content on its internet server is in conformity with the existing guidance. Should you have any immediate questions, you may reach me at [redacted] ARL's Associate for Corporate Programs, [redacted]y, oversees the website and may be reached at [redacted]

[redacted]
ARL Public Affairs Office
[redacted]

ARL MEMO 25-70
5. POLICY AND PROCEDURES
(2) Content.
(b) Information NOT Appropriate or Releaseable
(vi) Information of a personal nature which could be used to identify an individual or their location is prohibited with the exception of 1) and 2) below. The consent of an individual does not negate this requirement. All Internet references shall be anonymous with reference to an organization, a generic office symbol, central organization phone number or function-based email address.

* 1) The posting of names and contact information for the ARL Director and the ARL Public Affairs Officer is permitted.
** 2) ARL is not an insular organization. Its success hinges on its ability to act as the bridge between the science and technology community and the warfighter. ARL has identified

technical topics that are essential to its mission accomplishment and has assigned responsibility to select individuals for communicating with the public in these topical areas. It is in these areas that ARL must effectively collaborate with the public sector.

For those individuals designated as technical topic leaders, their duty descriptions and performance objectives designate them as organizational spokespersons and recognized leaders in their specialty fields and they require a high-level of unrestricted national visibility to carry-out their duties. Their duties include: being readily identified and contacted as the Army's lead for discussions of potential new extramural programs in their area of expertise; being sought out to serve on special task forces and committees; being sought as a consultant by other specialists; and receiving invitations and address national professional organizations.

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

From: [redacted]
Sent: Wednesday, December 20, 2006 3:55 PM
To: [redacted]@us.army.mil'
Cc: [redacted] HQAMC CIO/G6/IMD
Subject: FW: 20 OPSEC Concerns from AMC Website (UNCLASSIFIED)

Importance: High

Follow Up Flag: Follow up
Flag Status: Red

Attachments: AMC.xls; AMC.doc; Findings list.doc


AMC.xls (21 KB)

AMC.doc (33 KB)

Findings list.doc (46 KB)

Classification: UNCLASSIFIED

Caveats: NONE

[redacted]

We have completed the corrections to our public website outlined the AMC.xls file.

Thank you,

[redacted]
Webmaster, HQ AMC
Ft. Belvoir, VA

[redacted]

Sent: Thursday, December 14, 2006 11:51 AM
To: Public Communications
Subject: 20 OPSEC Concerns from AMC Website (UNCLASSIFIED)
Importance: High

Classification: UNCLASSIFIED
Caveats: NONE

Webmaster and PAO -- The Army Web Risk Assessment Cell (AWRAC) is currently reviewing U.S. Army Web sites for OPSEC and security compliance. Twenty OPSEC concerns were found on your organization's website and have been classified as a major and minor findings. The attached spreadsheet contains URLs that are publicly accessible. Please review the attached document for further guidance, and report resolution of these issues NLT 21 DEC 06.

Please contact me if you have questions.
<<AMC.xls>> <<AMC.doc>> <<Findings list.doc>> R/, [redacted]
Lockheed Martin Information Technology

Information Assurance Directorate NETC-EST-A

Army Web Risk Assessment Cell
703-602-7481 (DSN 332)
703-602-3751 (Fax)
[redacted]
AKO IM User

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

From: [redacted]
Sent: Tuesday, August 01, 2006 9:04 AM
To: [redacted]
Cc: [redacted]

Subject: FW: Army Web Risk Assessment Cell (AWRAC) (UNCLASSIFIED)
Signed By: [redacted]

Classification: UNCLASSIFIED

Caveats: NONE

FYI

[redacted]

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

[redacted]
Sent: Tuesday, August 01, 2006 8:40 AM
[redacted]
Subject: RE: Army Web Risk Assessment Cell (AWRAC) (UNCLASSIFIED)

Classification: UNCLASSIFIED

Caveats: NONE

Sir,

We had a discussion with the AWRAC team yesterday and are looking into how we will identify those Websites that are .mil's that are not resident behind our reverse proxy server. Additionally we are also going to screen for sites that are contractor operated on the .com domain that contain sensitive Army information that should be on the .mil domain.

We will work with the AGNOSC and appropriate commands to get them in compliance.

[redacted]

[redacted]
CIO/G6 NETC ESTA, OIA&C
[redacted]
"Our Army at War -- Relevant and Ready"

[redacted]
Sent: Sunday, July 23, 2006 12:30 PM

[redacted]

Subject: RE: Army [redacted] Assessment Cell (AWRAC) (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: FOUO

[redacted]

How can we use this team to also compile a list of severs that may be out there to locate on the APCs. Maybe and additional tasking. Please look into it.

******"Do what's right,....and risk the consequences!"******

[redacted]
LTG, USA
HQDA CIO-G6
Pentagon - [redacted]

****
Digitally signed with a DoD certificate.
To download the DoD Root and Medium assurance certificate
authorities visit https://dod411.chamb.disa.mil <https://dod411.chamb.disa.mil/>

[redacted]
Sent: Friday, July 21, 2006 7:11 PM
[redacted]

Subject: Army Web Risk Assessment Cell (AWRAC) (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

Classification: Caveats: *NOTICE:
Classification: UNCLASSIFIED
Caveats: NONE

Sir,

Latest information of mobilization of Army Guard personnel to support our Web and BLOG OPSEC operations. 10 personnel have been mobilized to support our expanded mission per the CSA.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

EXECUTIVE SUMMARY 21 July 2006

(U) MOBILIZATION OF ARMY WEB RISK ASSESSMENT CELL TEAM (NETC-EST-I)
(U//FOUO)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 will support 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 Belvoir, and is assigned to NETCOM, with duty at the unit's headquarters at Manassas Armory. Team members have received 90 percent of their initial required training, and will receive additional outside training during the next month. The group has received NETCOM computers, badges and e-mail accounts, and has been task organized under NETCOM EST-A. The armory was provided with two phone lines with DSN capabilities in support of the mission, and the unit voluntarily added a T-1 line. The team has been assigned a range of tasks

which will increase web monitoring, refine tracking procedures and streamline notification processes.

PREPARE MEMO_____.

[redacted]

MAJ [redacted]

APPROVED BY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

[redacted]
COL, GS
Director, Office of Information Assurance & Compliance
IA & C Directorate, Taylor Bldg
[redacted]

"Our Army at War -- Relevant and Ready"

Classification: UNCLASSIFIED
Caveats: NONE

Classification: Caveats:

Classification: UNCLASSIFIED
Caveats: NONE

Classification: UNCLASSIFIED
Caveats: FOUO

Classification: UNCLASSIFIED

Caveats: NONE

Classification: UNCLASSIFIED

Caveats: NONE

[redacted]

From: [redacted]
Sent: Tuesday, August 01, 2006 11:12 AM
To: [redacted]
Subject: memo (UNCLASSIFIED)

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

Army Chief of Staff Urges Incr...

Classification: UNCLASSIFIED
Caveats: NONE

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

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
202-492-7797
[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.
David

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

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

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
[redacted]

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

Classification: UNCLASSIFIED
Caveats: NONE

Good Morning [redacted]
Got this in my email this morning. Any thoughts on this?
[redacted]

[redacted]
[redacted]r
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]
[redacted]
[redacted]
2530 Crystal Drive
[redacted]rlington, VA 2202

[redacted]
Sent: Wednesday, September 20, 2006 12:28 PM
[redacted]
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]C4
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
Taylor Building - DSN 332 7408 Comm 703 602 7408
[redacted].army.mil

Classification: UNCLASSIFIED
Caveats: NONE

Classification: UNCLASSIFIED
Caveats: NONE

Classification: UNCLASSIFIED
Caveats: NONE

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

From: [redacted]
Sent: Tuesday, September 26, 2006 7:57 AM
To: [redacted]
Subject: FW: AWRAC Mission (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

Below is the list of personnel we would be meeting with, if the funds are available to travel to [redacted]

The location is [redacted] just outside [redacted]

The topic is there new TDA, manning, training and the AWRAC mission.

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

[redacted]
Sent: Monday, September 25, 2006 7:01 PM
[redacted]
Subject: RE: AWRAC Mission (UNCLASSIFIED)

[redacted]

Our schedules are still wide open in October. Our preference is to meet prior to 14 October, so we can develop a plan and brief the team on 14/15 October. So, anytime between the 2nd and 13th of October should work for us.

Attendees will likely include [redacted] (Group XO), [redacted] (Bn Cdr), [redacted] XO), [redacted] (Bn S3), and either [redacted] Web OPSEC Team Leader) or CPT Miguel (Web OPSEC Deputy).

V/R,

[redacted]

[redacted]
Operations Officer
56th IO Group
[redacted]

COMM: 253-512-7814

[redacted]
Sent: Monday, September 25, 2006 5:52 AM
[redacted]
Subject: RE: AWRAC Mission (UNCLASSIFIED)

Classification: UNCLASSIFIED

Caveats: NONE

[redacted]

The weekend of 14/15 will not work for us. What other dates could we do the visit. I need the name and the position of the all the personnel who may be at the meeting, so I can justify the travel funds for the new FY.

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

[redacted]
Sent: Monday, September 18, 2006 7:14 PM
[redacted]
Subject: FW: AWRAC Mission (UNCLASSIFIED)

[redacted]

I am the [redacted] Please give me a call at your earliest convenience. I'd like to take you up on your offer to visit [redacted] We are currently planning training for calendar year 2007, and would like to discuss your organization, mission, training opportunities, etc.

V/R,

[redacted]

[redacted]
Operations Officer
56th IO Group
[redacted]

From: [redacted]
Sent: Monday, September 18, 2006 1:13 PM
[redacted]
Subject: FW: AWRAC Mission (UNCLASSIFIED)

FYI

[redacted]
Sent: Wednesday, August 23, 2006 7:06 AM
To: [redacted]
Subject: AWRAC Mission (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

Sir

[redacted] has just been appointed as government lead for the AWRAC mission. We need an update of your unit's personnel status to include the name and email of new BN command. Both of us would like to visit you to work out any training or mission tasking issues you may have. Please give us possible visit dates between now and JAN 07.

[redacted]

Web Risk Assessment/Information Assurance Analyst

[redacted]

[redacted]

Classification: UNCLASSIFIED
Caveats: NONE

Classification: UNCLASSIFIED

Caveats: NONE

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] <CTR>
[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

[redacted]

From: [redacted]@us.army.mil [mailto:[redacted]@us.army.mil]
Sent: Sunday, October 08, 2006 2:59 PM
To: [redacted]<CTR>
Subject: Fwd: FW: OPSEC Concern (UNCLASSIFIED)

Forward to IQ.

MAJ [redacted]
NCRIOC

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] the Link has been corrected.

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

[redacted]
Sent: Thursday, October 12, 2006 4:07 PM
[redacted]
Cc: [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], or [redacted]) at [redacted] 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 -----

[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: Saturday, October 14, 2006 8:55 PM
To: [redacted]

Subject: FW: Article on Opsec (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

Our first response for the news article.

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

-----Original Message-----
[redacted]
Sent: Saturday, October 14, 2006 5:13 PM
To: NETCOM Army Web Risk Assessment Cell
Subject: Article on Opsec

I read your article a few days ago and after doing so felt some concerns about the unit that you have monitoring non department of defense personal communications of uniformed personnel. First, I think it would have been appropriate for you to mention in your article that you have procedures to safeguard the constitutional rights of uniformed personnel to freely express their views in a non military context.

The second problem is about the two soldiers you featured in your article who say they take their mission to ferret out violators of OPSEC seriously because its personal with them. If its personal than they should not be doing that job. It's positive to be motivated to do a good job and even a little zeal is a good thing. Being a fanatic is not a good thing.

You might want to share with those two soldiers in your anti OPSEC unit the news's story about the young Marine who is being nominated for the Congressional Medal of Honor. In that story he was killed a month later doing the same heroic acts that lead to his nomination. The news story related that when his parents were notified about his death, they and other family were shocked that he had done those things.

Here's a what if scenario. Lets say uniformed personnel feel don't free to communicate with family members about what they or their unit is doing because someone is monitoring their personal communications. So a soldier or marine who might communicate with a father or uncle that they are bravely leading their squad whenever they confront a terriorist threat might raise a level of concern with the family. The family could follow through by contacting the commander of their son's unit through the chain of command and request more information. That sort of thing might motivate the unit commander to consider this family's concerns resulting in their son not being awarded the Medal of Honor, but being alive and well for the rest of his life. So do you keep soldiers alive by shutting down the flow of communications to a family or in fact kill them faster?

One last thing. I think that the enemy can gather all the intelligence they need on the ground and don't have to worry about surfing the net to get that information. If you are really concerned about OPSEC than send your personnel to the Middle East and have them agressivly hunt down enemy personnel, interrogate suspicious civilians, etc instead of wasting their time in front of a computer surfing the net and harrassing brave young Americans with threatening e-mails.

[redacted]
Classification: UNCLASSIFIED
Caveats: NONE

[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
[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 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

[redacted]

From: [redacted]
Sent: Monday, October 23, 2006 12:25 PM
To: [redacted]
NETCOM
Subject: Pam's Article (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

Look who picked up Pan's 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 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
[redacted] 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]

-----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: Thursday, October 26, 2006 1:37 PM
To: [redacted]
NETCOM/LMIT
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]1

[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 the 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 AND 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
[redacted]
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

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

DEPUTY DIRECTOR
FOR MANAGEMENT

December 17, 2004

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.

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 [redacted] (202) 395-3787 [redacted]@omb.eop.gov, or [redacted] (202) 395-7857 [redacted]@omb.eop.gov, Policy Analysts, Information Policy and Technology Branch, Office of Management and Budget.

Attachment

Attachment

Policies for Federal Agency Public Websites

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 manner[1] and to maintain inventories of information dissemination products.

   B. Section 207 of the E-Government Act[2] 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

   A. Your agency is already required under the Information Quality Act and associated guidelines[3] 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

   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-130[4] 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.
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.
   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.
   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.

   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.

    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

INFORMATION PAPER

NETC-EST-I
12 JAN 2007

SUBJECT: Army Web Risk Assessment Cell (AWRAC)

1. Purpose. To provide an end of year synopsis to the Senior Leadership regarding the accomplishments of the Army Web Risk Assessment Cell (AWRAC) for 2006.

2. Facts: The AWRAC mission is to search Army Websites and unofficial sites posted by Army personnel for information that could pose a risk to national security on unsecured web sites. In addition, the AWRAC evaluates website content to ensure compliance with departmental policies, federal regulations and procedures, and industry best practices. The AWRAC's core mission consists of website patrolling, bulk analysis, and operational security analysis.

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. The mobilized soldiers are also developing two applications. One will replace the Joint Web Discrepancy Tracking System (JWTDS). The other application will collect information from the disparate reporting tools and present a consolidated view of the web sphere for analyst and members of the Army leadership.

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) and Freedom of Information Act (FOIA) 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. Ongoing reviews keep the AWRAC mission on track and up-to-date.

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.

[redacted] 202-492-7797 [redacted] /703-602-7481

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

[redacted]

From: [redacted]
Sent: Tuesday, February 27, 2007 6:52 AM
To: [redacted]
Subject: FW: AWRAC Mission Tracking (UNCLASSIFIED)
Signed By: [redacted]

Classification: UNCLASSIFIED
Caveats: NONE

-----Original Message-----
[redacted]
Sent: Wednesday, September 06, 2006 11:06 AM
[redacted]
Subject: AWRAC Mission Tracking (UNCLASSIFIED)

Classification: UNCLASSIFIED

Caveats: NONE

Gentlemen,

We've been talking about improving a lot of different things since we've started this mission, and now I want to execute some improvements. Starting with tracking. First I need to know what we are scanning, second who is analyzing what area within in a RCIO. I don't necessarily need to know specific links, that would be crazy. Third, I want to track all "concerns" opened. Finally, I want to track technical issues with our tools, i.e. watchfire. Some of this information may be exportable from Watchfire

Until we get a DB together, a simple spreadsheet will suffice. Keep it on the share so everybody has access to it and can update it as needed.

The reason for this is multifaceted to include giving us a way to track and evaluate our work, provide bullets for evaluation reports, and most importantly to provide fodder for writing awards for our soldiers.

I'm easy, you all can give me options, or I can set up a template for you, either way we're going to start next week.

I'm hearing that are "numbers" aren't so good, and the perception among some of the full-timers is that we are not doing much in terms of unit either. My priority is to get the mission squared away first.

Thanks

[redacted]

Classification: UNCLASSIFIED

Caveats: NONE

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

From: [redacted]
Sent: Tuesday, February 27, 2007 6:51 AM
To: [redacted]
Subject: FW: INDIVIDUAL BLOG SITES (UNCLASSIFIED)
Signed By: [redacted]

Classification: UNCLASSIFIED
Caveats: NONE

-----Original Message-----
[redacted]
Sent: Tuesday, August 29, 2006 10:54 AM
[redacted]
Subject: Re: INDIVIDUAL BLOG SITES (UNCLASSIFIED)

Yes. No problem.

Sent from my BlackBerry Wireless Handheld

----- Original Message -----
[redacted]
COM
Sent: Tue Aug 29 07:13:49 2006
Subject: INDIVIDUAL BLOG SITES (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

Good Morning, my name is [redacted] I worked for AWARC monitoring Army affiliated individual Blog sites. I'm finding a lot of IED damage photos online. I can tell the individual is in the Army by the photo of himself. However, he does not give enough information to locate him through the AKO directory. Can we officially notify him via his blog's contact link? Please give guidance on this issue.

[redacted]

LMIT Professional Services

Information Assurance Directorate NETC-EST-A

Army Web Risk Assessment Cell

[redacted]

Classification: UNCLASSIFIED
Caveats: NONE
Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

From: [redacted]
Sent: Tuesday, February 27, 2007 6:51 AM
To: [redacted]
Subject: FW: INDIVIDUAL BLOG SITES (UNCLASSIFIED)
Signed By: [redacted]

Classification: UNCLASSIFIED
Caveats: NONE

-----Original Message-----
[redacted]
Sent: Tuesday, August 29, 2006 10:14 AM
[redacted]
Subject: INDIVIDUAL BLOG SITES (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

Good Morning, my name is [redacted] I worked for AWARC monitoring Army affiliated individual Blog sites. I'm finding a lot of IED damage photos online. I can tell the individual is in the Army by the photo of himself. However, he does not give enough information to locate him through the AKO directory. Can we officially notify him via his blog's contact link? Please give guidance on this issue.

[redacted]
LMIT Professional Services

Information Assurance Directorate NETC-EST-A

Army Web Risk Assessment Cell
[redacted]

Classification: UNCLASSIFIED
Caveats: NONE
Classification: UNCLASSIFIED
Caveats: NONE

[redacted]

From: [redacted]
Sent: Tuesday, February 27, 2007 6:49 AM
To: [redacted]
Subject: FW: Modifying Search Criteria in Watchfire... (UNCLASSIFIED)
Signed By: [redacted]

Attachments: How to modify a rule.doc

How to modify a rule.doc

Classification: UNCLASSIFIED
Caveats: NONE

-----Original Message-----
[redacted]
Sent: Wednesday, August 02, 2006 10:46 AM
[redacted]
Subject: Modifying Search Criteria in Watchfire... (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

Hi guys,
I remembered, this morning, that I never sent this "How-to" guide on changing page rules to you. I haven't played around with this at all, but thought you might want to give it a go. Let me know how it works out. We can probable eliminate a lot of our false positives this way.

[redacted]

<<...>>

[redacted]
LMIT Professional Services

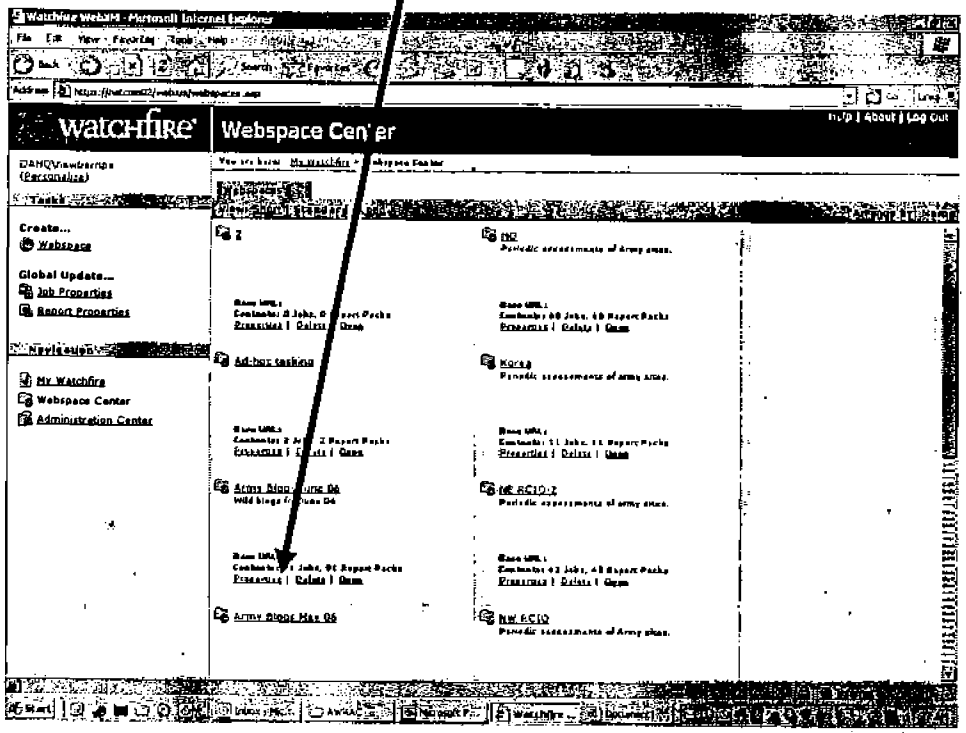
Information Assurance Directorate NETC-EST-A

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

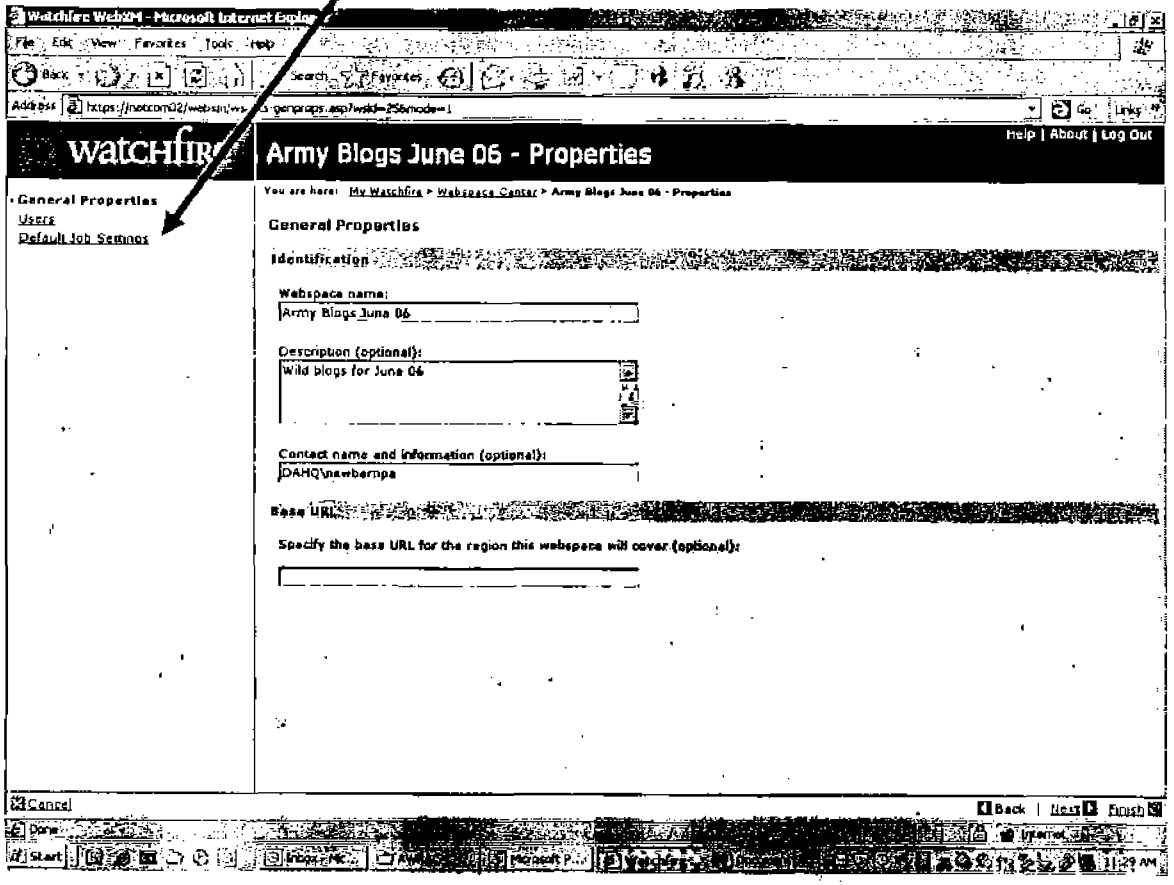
Classification: UNCLASSIFIED
Caveats: NONE

Classification: UNCLASSIFIED
Caveats: NONE

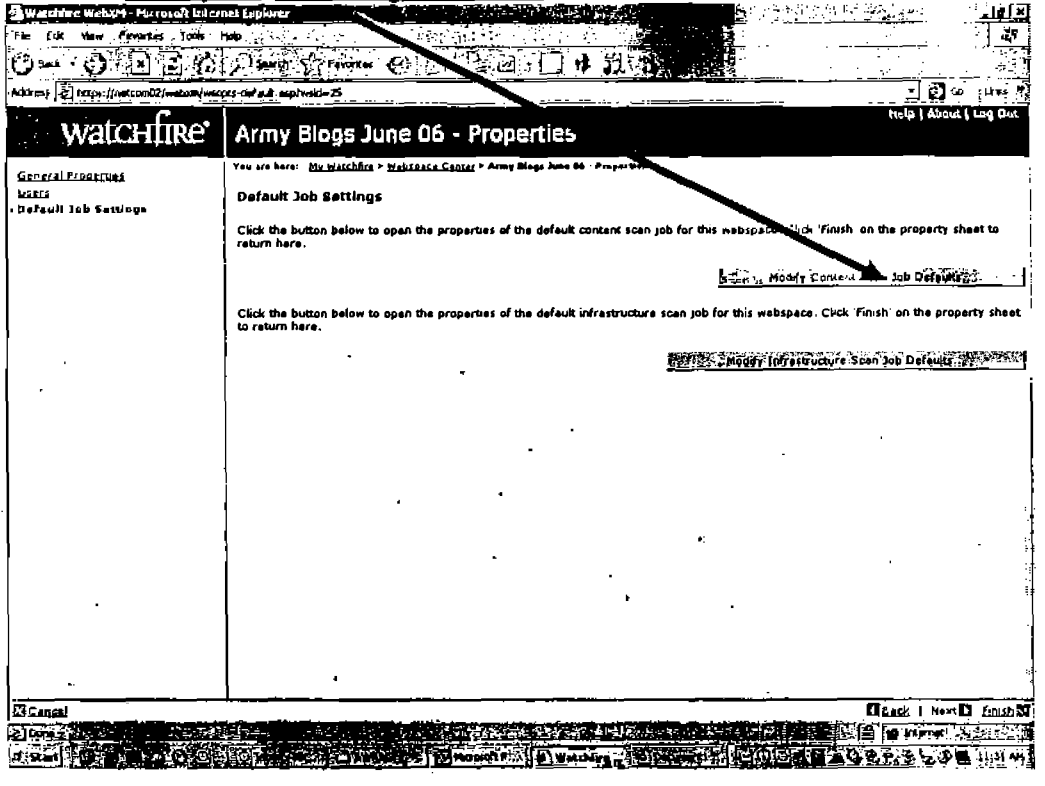
Begin by clicking on the properties of the webspace you wish to modify.



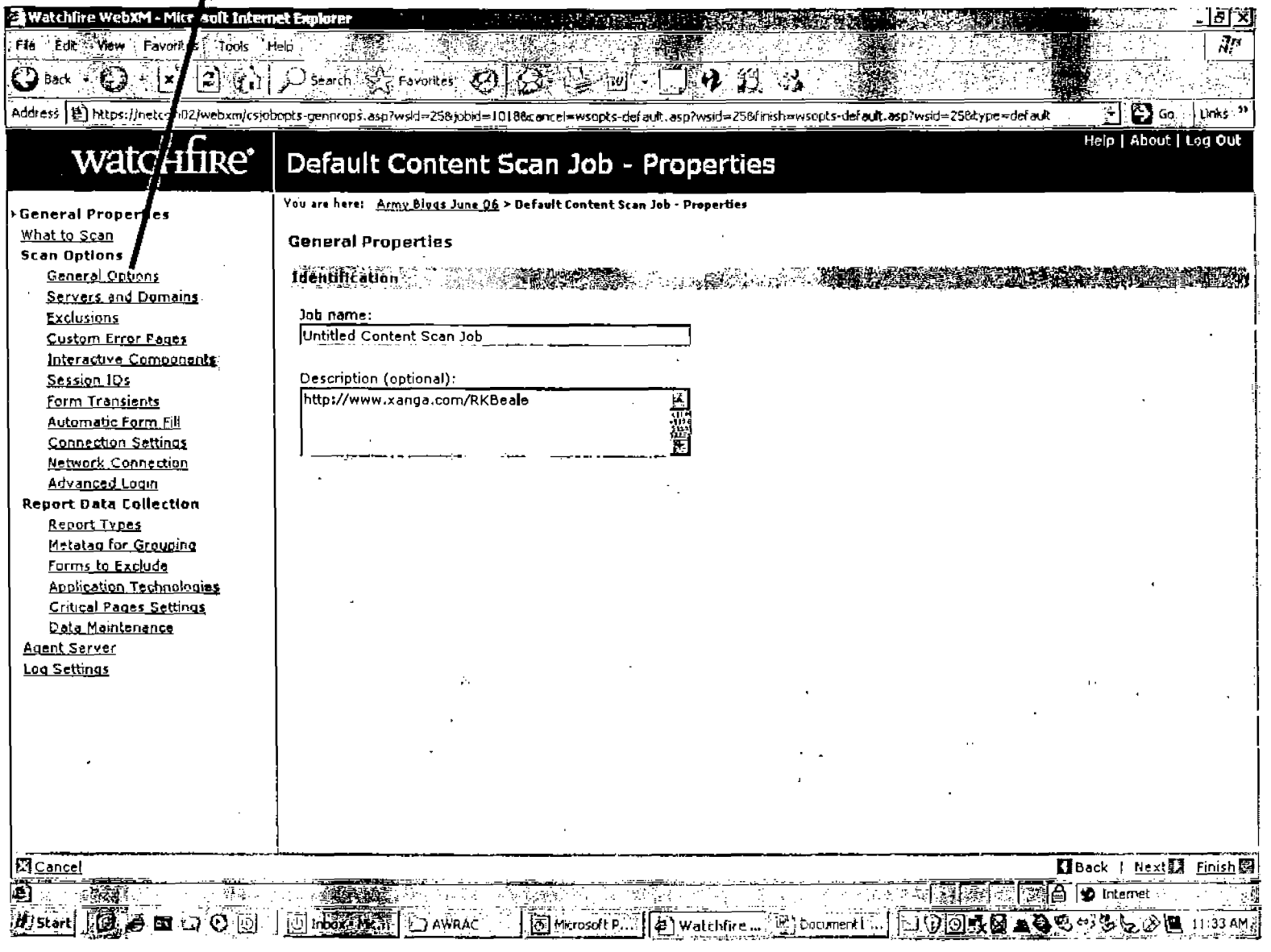
Click on "default job settings:



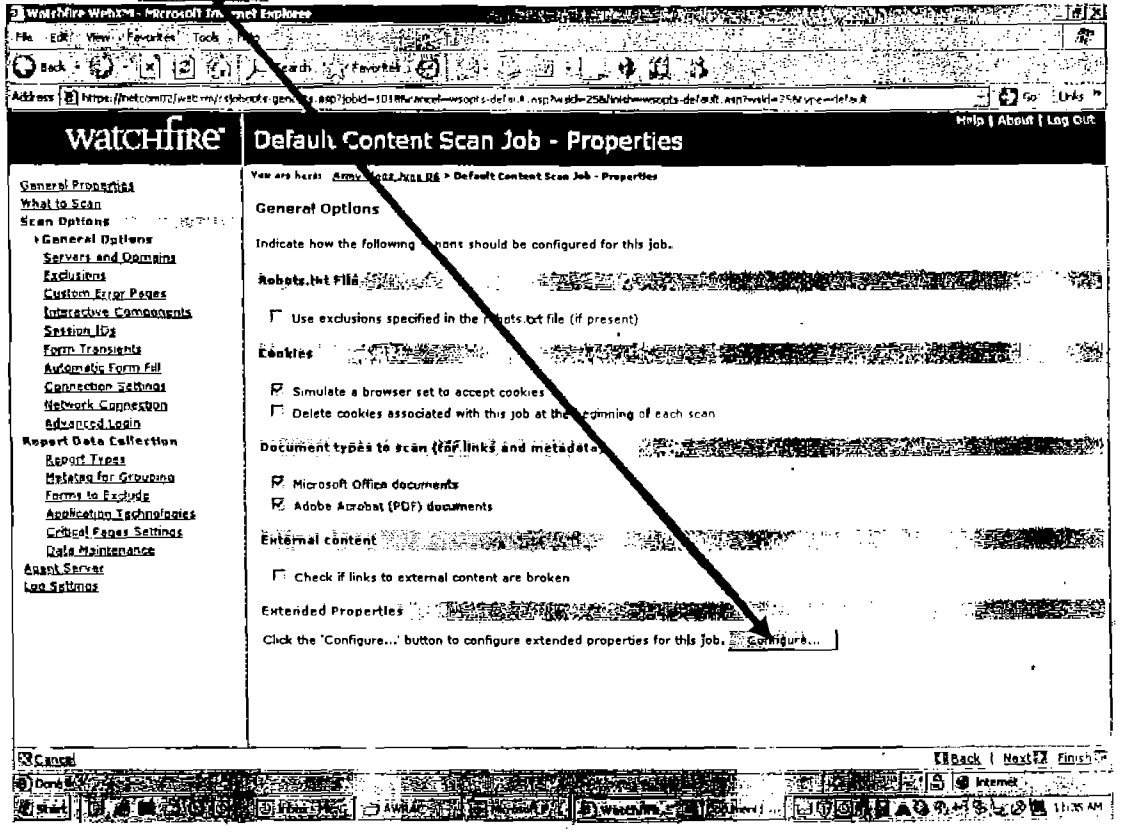
Click on modify content scan job defaults:



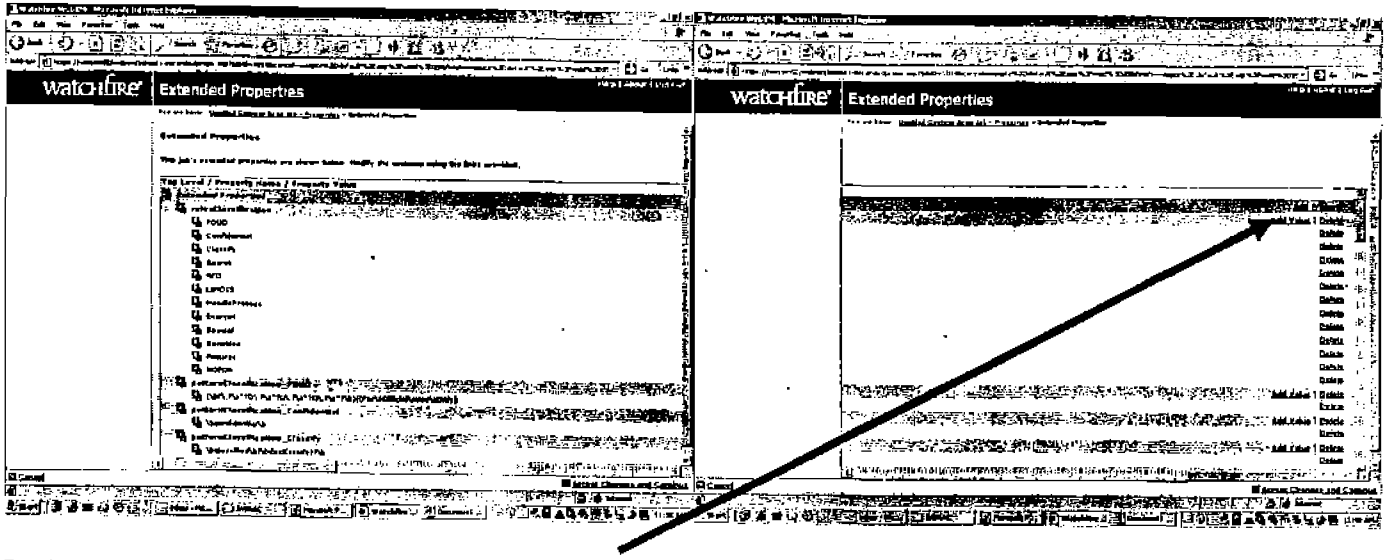
Click on "general options"


Watchfire WebXM - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://netc...02/webxm/csjobopts-genprops.asp?wsid=258&jobid=1018&cancel=wsopts-default.asp?wsid=258&finish=wsopts-default.asp?wsid=258&type=default
Go Links
Help | About | Log Out
watchfire
Default Content Scan Job - Properties
You are here: Army Blogs June 06 > Default Content Scan Job - Properties
General Properties
What to Scan
Scan Options
General Options
Servers and Domains
Exclusions
Custom Error Pages
Interactive Components
Session IDs
Form Transients
Automatic Form Fill
Connection Settings
Network Connection
Advanced Login
Report Data Collection
Report Types
Metatag for Grouping
Forms to Exclude
Application Technologies
Critical Pages Settings
Data Maintenance
Agent Server
Log Settings
General Properties
Identification
Job name:
Untitled Content Scan Job
Description (optional):
http://www.xanga.com/RKBeale
Cancel
Back | Next Finish
Internet
Start
Inbox - Mi...
AWRAC
Microsoft P...
Watchfire ...
Document1 ...
11:33 AM

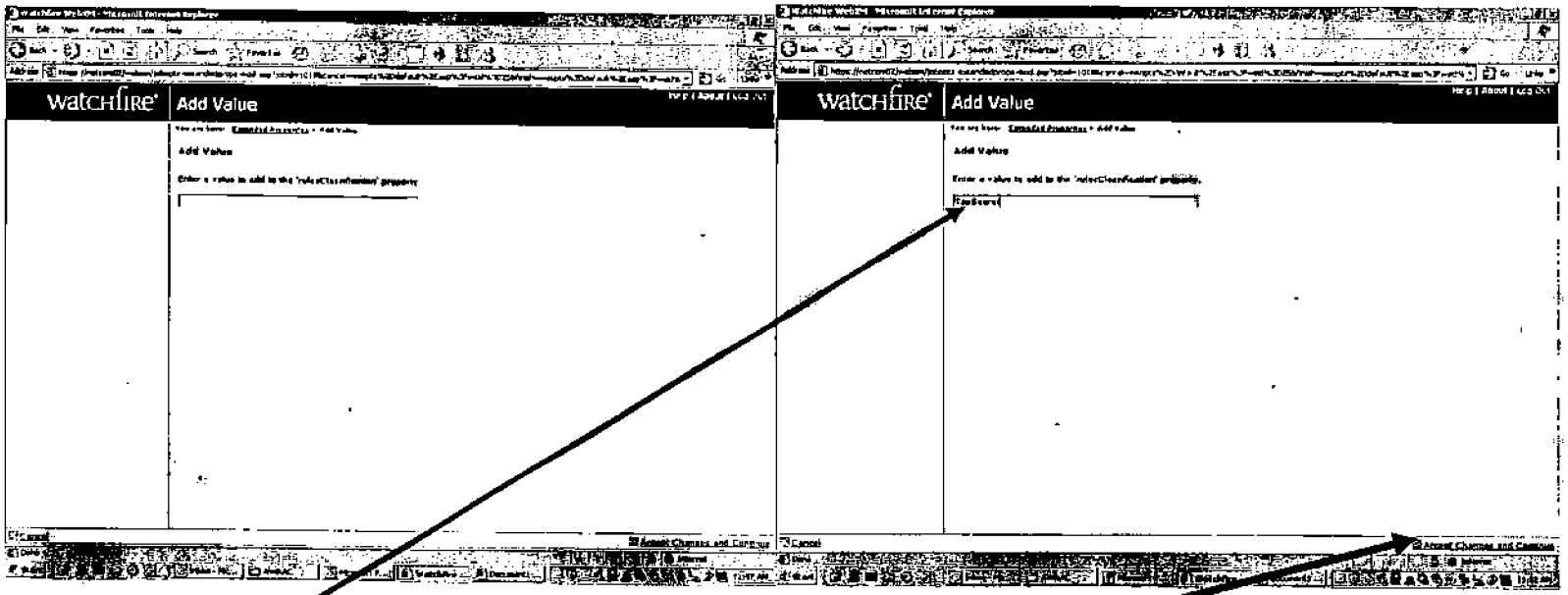
Click on "Configure"



This will take you to the "extended properties page. Select the rule that you want to modify (Operations, Classification, Personnel, etc.). For example, you decide that you want to scan for the word "Top Secret." This would go under the existing rule of "classification."

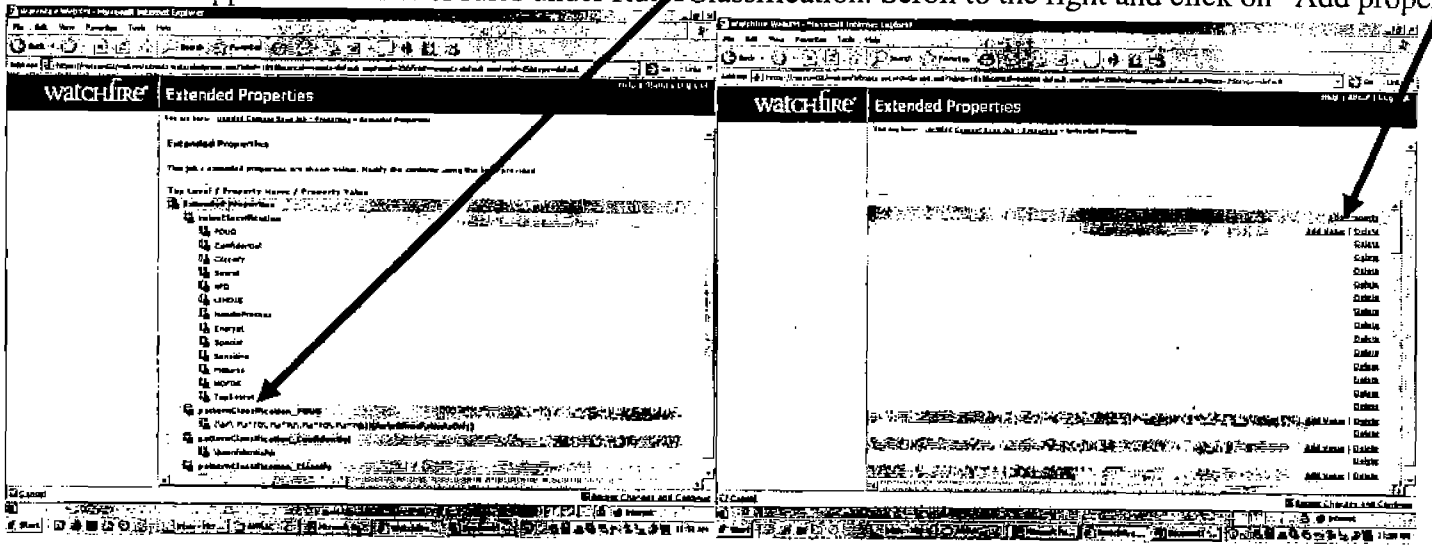


In the above example, we want to add a value to the existing rule "rulesClassification." To do so, first, scroll over to the far right of the page, using the bottom scroll bar. Click on the "add value" link of the rule you wish to modify. This will take you to the following screen:

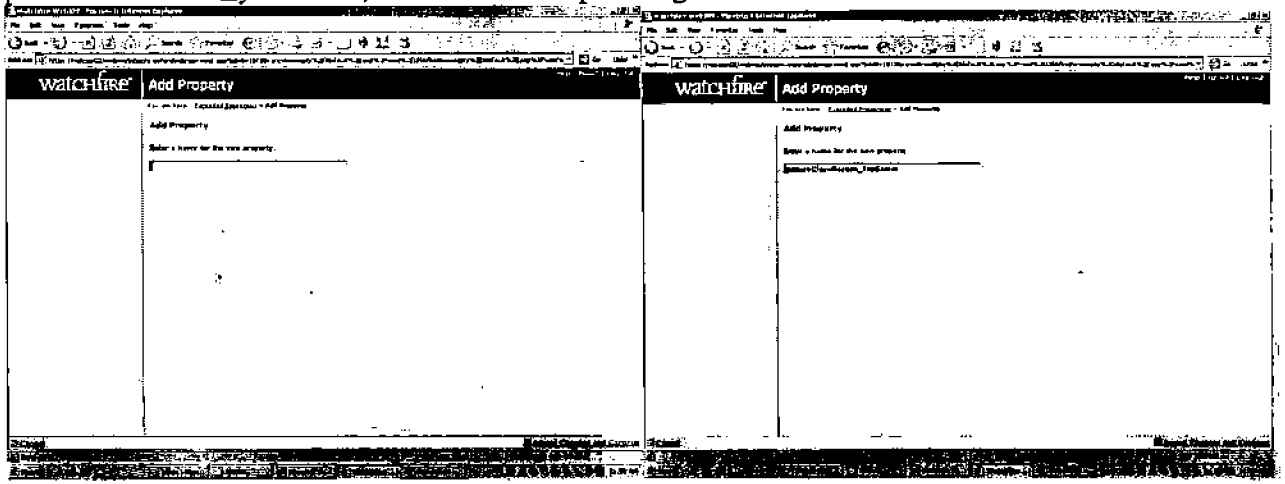


Enter the word that you wish to add to the scan. Click on "accept changes and continue."

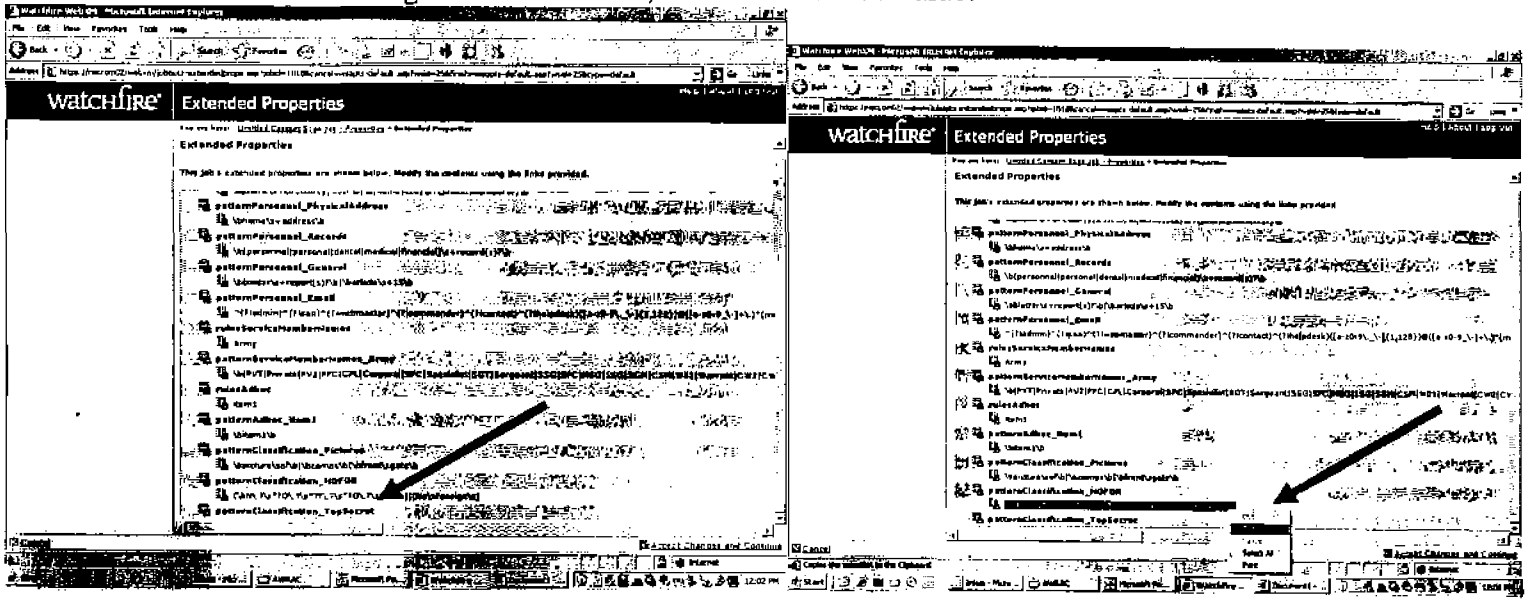
The word will appear on the list of rules under RulesClassification. Scroll to the right and click on "Add property."

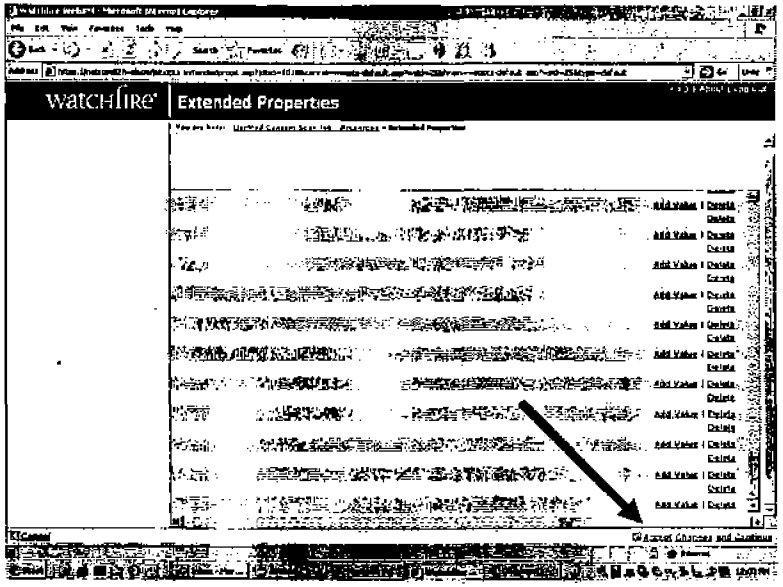


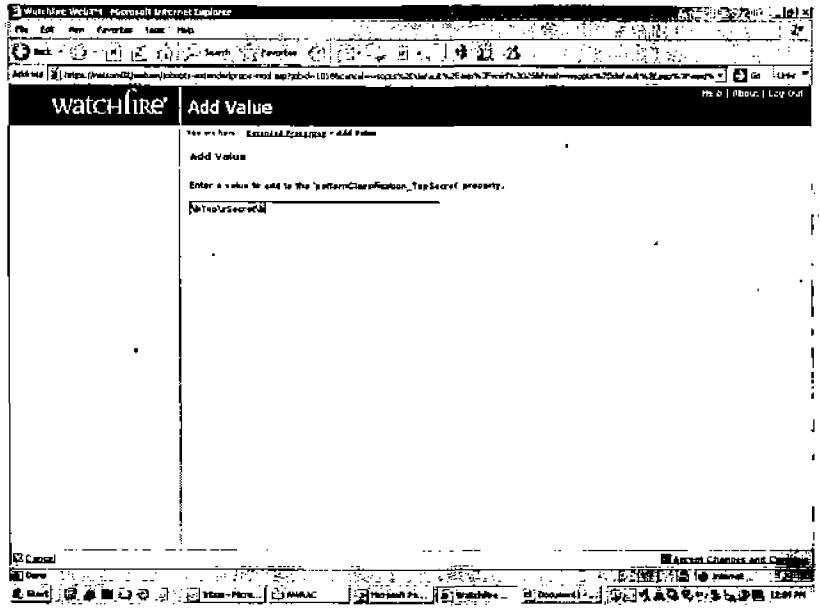
Add the word that you wish to scan, using the following format: patternClassification_TopSecret. (The format will change according to what rule you are modifying, and what the word is. For instance, if you are modifying the Personnel rule, the format would be: patternPersonnel_yourword). Click on "accept changes and continue."



The new word will appear at the very bottom of the extended properties rule. Highlight and copy the coding under one of the existing rules. Then scroll over to the right of the new rule, and click on "add value."




WATCHFIRE
Extended Properties



Paste the code into the "add value" box, and modify it to match your new word. For instance, "Top Secret" would be coded as: \bTop\sSecret\b. Some other codes are: patternForceProtection_Weapons: bweapon\s+system(s)?\b|\bweapon\s+spec(s|ification)?\b or patternPersonnel_General \bblotter\s+report(s)?\b|\barticle\s+15\b

Click on "accept changes and continue. The new word will now be at the bottom of the page, along with the coding. Click on "accept changes, finish, and finish. The next time you run the webspace, it will automatically scan for this word. Any scans you place in the webspace also will be searched for the word.