

For Official Use Only

NETC-EST-I

16 MAR 06

DECISION PAPER THRU ESTA Director

FOR COMMANDING GENERAL

SUBJECT: Request for Mobilization of Reserve Component Information Operations Teams

1. FOR: Signature.
2. PURPOSE: To obtain the Commanding General's signature on a request for the 365-day mobilization of two five-person Reserve Component Information Operations teams in support of the Chief of Staff of the Army's directive on OPSEC and the World Wide Web.
3. RECOMMENDATION: The CG signs the policy memo.
4. ASSUMPTIONS: None.
5. FACTS:
  - a. Background. The Army Web Risk Assessment Cell (AWRAC) is responsible for reviewing the content of the Army's publicly-accessible web sites. AWRAC conducts ongoing operational security and threat assessments of Army websites. AWRAC is made up of Army Reserve and National Guard soldiers, and uses weekend drills and annual training to support its mission.
  - b. Facts. CSA message (DTG: 200001Z Aug 05) has expanded the AWRAC mission to include review of Army-related web-logs (blogs), video logs, photo-sharing sites and unofficial websites posted by service members for OPSEC concerns.
6. RATIONALE FOR RECOMMENDATION: To protect Army units, servicemembers, and DA civilians from harm due to an OPSEC compromise.
7. IMPACT FOR OF SUCCESS OR FAILURE: If this mobilization request is not approved, it will significantly impact the ability of the G-6 to continue executing this directive. This measure is essential to ensure the safety of both classified information and U.S. servicemembers.
8. APPROVED \_\_\_\_\_ NEED MORE INFORMATION \_\_\_\_\_ SEE ME \_\_\_\_\_

PREPARED BY: CPT [REDACTED] /AWRAC Government Lead/(703) 602-7482  
RELEASED BY: COL Stephen J. Jurinko/ Director of the Information Assurance and Compliance Directorate for the Department of the Army/(703) 602-7403

For Official Use Only

DTG: 200001Z Aug 05

From: DOD, ARMY, ORGANIZATIONS, ARMY OPERATIONS CENTER, AOC CAT  
OPSWATCH G3 DAMO AOC(MC)  
Subj: (U) CHIEF OF STAFF OF THE ARMY OPSEC GUIDANCE (U//FOUO)

UNCLASSIFIED//FOR OFFICIAL USE ONLY.

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

UNCLASSIFIED//FOR OFFICIAL USE ONLY

EXECUTIVE SUMMARY

18 October 2006

(U) ARMY WEB RISK ASSESSMENT CELL. (NETC-EST-I)

(U//FOUO) The Army Web Risk Assessment Cell (AWRAC) made up of 10 mobilized Virginia National Guard soldiers, 3 traditional (part time) National Guard Teams from Maryland, Washington, Texas, and an Army Reserve Team from Virginia continues to successfully review official and unofficial web sites and blogs for Operational Security (OPSEC) violations IAW the CSA's 20 AUG 2005 message. The team also has three full-time contractors to provide continuity. The Cell conducts a wide range of tasks that have increased the amount of web sites and blogs being reviewed, constant refinement of tracking procedures, and streamlining of the notification process. The Cell typically reviews several hundred thousand web pages and makes dozens of notifications every month. Over the past nine months, the Cell has reviewed over 715 web sites and blogs comprised of more than 4,213,000 pages. The Cell's search has uncovered more than 1630 OPSEC violations and ensured their correction. In addition, the Cell has expanded their monthly review of the popular blog from approximately 30 blogs comprised of 5500 pages each month to 75 blogs comprised of 210,000 pages. Soldiers continue to post articles and blogs that contain information about the Army mission that are clear OPSEC violations. The AWRAC is on the front line to identify these risks which save lives and Army resources through the painstaking review of all official and thousands of unofficial sites. The Virginia National Guard is training two more teams to augment the mission and to serve as possible replacements for the soldiers who are currently mobilized.

PREPARE MEMO\_\_\_\_\_.

LTC STEPHEN WARNOCK/NETC-EST-I/703-571-3528

APPROVED BY

UNCLASSIFIED//FOR OFFICIAL USE ONLY



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: 20 July 2002

8 July 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 2 July 2002, the Headquarters, Department of the Army, Chief Information Officer (CIO)/G-6 Web Risk Assessment Cell was notified of the following web site for evaluation [https:// http:// http://www.21tsc.army.mil/](https://http://http://www.21tsc.army.mil/). The following security concerns were noted and rated by category (see below).

CATEGORY	Document	FINDING	REFERENCE
Major	See attached	Unsecured web page Document marked FOUO, Bio's with family information, external links with out disclaimer and commercial sponsorship and logos	Web Site Admin Policies & procedures w/amendments 11 JAN 2002 and AR25-1

SAIS-IOA

Subject: Web Risk Assessment Findings

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g., questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to

acknowledge receipt via email to the AWRAC

[REDACTED]@s.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 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.)

SAIS-IOA

Subject: Web Risk Assessment Findings

6. POC: Mr. [REDACTED] Army Web Risk Assessment

Analyst, COM: 717-865-1785

Email: [REDACTED]@ARMY.MIL



THADDEUS A. DMUCHOWSKI

COL, GS

Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

### **WEB SITE CONTENT GUIDANCE**

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

Army Regulation (AR) 25-1, 31 May 2002, Army Information Management

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

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



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: 12 September 2003

2 September 2003

MEMORANDUM FOR WEB SITE ACTIVITY COMMANDER/SUPERVISOR

SUBJECT: Web Risk Assessment Findings (71ST CSB)

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 1 August 2003, the Headquarters, Department of the Army, Chief Information Officer (CIO)/G-6 Web Risk Assessment Cell conducted an assessment of your web site

(<http://www.7thcsg.vcorps.army.mil/71ST/csmbrinson.htm>

[http://www.7thcsg.vcorps.army.mil/71ST/Cusimano Biography.doc](http://www.7thcsg.vcorps.army.mil/71ST/Cusimano%20Biography.doc)

). The following registration and security concerns were noted and rated by category (see below).

CATEGORY	Document	FINDING	REFERENCE	
Personnel	Leaderships	Unsecured web page	Web Site	
Major	BIO	Documents: Bio for Commander and CSM contains full DOB Family member information.	Admin Policies & procedures w/amendments 11 JAN 2002 Para. 3.5.3.4	
			AR25-1	

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

SAIS-IOA

Subject: Web Risk Assessment Findings

security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to acknowledge receipt via email to the AWRAC

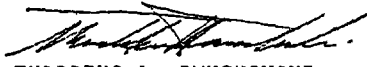
[REDACTED]@us.army.mil) and forward the memorandum to the commander/ supervisor, or his/her designated representative, responsible for the website. Suspense dates for corrective actions/resolution of security concerns are provided in the memorandum. Copies of this memorandum will be furnished to the appropriate MACOM, PEO, PM 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 their families.

5. Definitions:

- a. CRITICAL: Information that is either classified or, when combined with other sensitive information, may have significant operational impact. It is information that could put either personnel or facilities at risk.
- b. MAJOR: Information in itself or in aggregation that is FOR OFFICIAL USE ONLY (FOUO).
- c. MINOR: All other violations that do not fall in either of the above two categories. Information, which may not be posted, on official web sites open to public access. Also, information that is contrary to the web policy guidance. (Note: Commanders may elect to assume this level of risk.)

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

  
THADDEUS A. DMUCHOWSKI  
COL, GS  
Director, Information Assurance



SAIS-IOA

Subject: Web Risk Assessment Findings

CF: Appropriate MACOM/PEO/PM

## **WEB SITE CONTENT GUIDANCE**

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

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

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

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



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

Office, Chief Information Officer / G6

NETC-ESTA-A

S: 11 December 2002

9 December 2002

MEMORANDUM FOR WEB SITE ACTIVITY COMMANDER/SUPERVISOR  
(Battle Projection Group(BPG) 1<sup>st</sup> Brigade 75<sup>th</sup> Division)

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. During 1<sup>th</sup> quarter FY03, Headquarters, Department of the Army, Chief Information Officer Web Risk Assessment Cell was notified of security concerns on the following web sites.

CATEGORY	Document	FINDING	REFERENCE
Major	<a href="http://www.75div.army.mil/bpg/Commandbulletin.htm">http://www.75div.army.mil/bpg/Commandbulletin.htm</a>	Documents SSN	Web Site Admin Policies & procedures w/amendments 11 JAN 2002 and AR25-1
	<a href="http://www.75div.army.mil/bpg/index.htm">http://www.75div.army.mil/bpg/index.htm</a>	Training schedule	

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g., questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to

NETC-ESTA-A

Subject: Web Risk Assessment Findings

acknowledge receipt via email to the AWRAC


[REDACTED]my.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 IAPMS

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

5. Definitions:

- a. CRITICAL: Information that is either classified or, when combined with other sensitive information, may have significant operational impact. It is information that could put either personnel or facilities at risk.
- b. MAJOR: Information in itself or in aggregation that is FOR OFFICIAL USE ONLY (FOUO).
- c. MINOR: All other violations that do not fall in either of the above two categories. Information, which may not be posted, on official web sites open to public access. Also, information that is contrary to the web policy guidance. (Note: Commanders may elect to assume this level of risk.)

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

  
THADDEUS A. DMUCHOWSKI  
COL, GS  
Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

NETC-ESTA-A

Subject: Web Risk Assessment Findings

### **WEB SITE CONTENT GUIDANCE**

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

Army Regulation (AR) 25-1, 31 May 2002, Army Information Management

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

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



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

Office, Chief Information Officer / G6

NETC-ESTA-A

S: 5 January 2003

30 December 2002

MEMORANDUM FOR WEB SITE ACTIVITY COMMANDER/SUPERVISOR  
(Battle Projection Group(BPG) 1<sup>st</sup> Brigade 75<sup>th</sup> Division)  
(2<sup>ND</sup> NOTIFICATION)  
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 November 2002, the Headquarters, Department of the Army, Chief Information Officer NETC-ESTA-A Web Risk Assessment Cell conducted an assessment of your web site.  
<http://www.75div.army.mil/bpg/CommandBulletin.htm> The following security concerns were noted and rated by category (see below and attached).  
During 1<sup>th</sup> quarter FY03, Headquarters, Department of the Army, Chief Information Officer Web Risk Assessment Cell notified your office of same security concerns no action was taken to remove this information from the web sites.

CATEGORY	Document	FINDING	REFERENCE
Major	<a href="http://www.75div.army.mil/bpg/CommandBulletin.htm">http://www.75div.army.mil/bpg/CommandBulletin.htm</a>	Documents SSN	Web Site Admin Policies & procedures w/amendments 11 JAN 2002 and AR25-1
	<a href="http://www.75div.army.mil/bpg/index.htm">http://www.75div.army.mil/bpg/index.htm</a>	Training schedule	
see attached			

NETC-ESTA-A

Subject: Web Risk Assessment Findings

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g., questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to

acknowledge receipt via email to the AWRAC

[REDACTED]@us.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 IAPMs

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


5. Definitions:

- a. CRITICAL: Information that is either classified or, when combined with other sensitive information, may have significant operational impact. It is information that could put either personnel or facilities at risk.
- b. MAJOR: Information in itself or in aggregation that is FOR OFFICIAL USE ONLY (FOUO).
- c. MINOR: All other violations that do not fall in either of the above two categories. Information, which may not be posted, on official web sites open to public access. Also, information that is contrary to the web policy guidance. (Note: Commanders may elect to assume this level of risk.)

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

NETC-ESTA-A

Subject: Web Risk Assessment Findings



THADDEUS A. DMUCHOWSKI

COL, GS

Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

### **WEB SITE CONTENT GUIDANCE**

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

Army Regulation (AR) 25-1, 31 May 2002, Army Information Management

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

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



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: 15 July 2002

June 26, 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 14 June 2002, the Headquarters, Department of the Army, Chief Information Officer (CIO)/G-6 Web Risk Assessment Cell conducted a routine assessment of your website (See attached).

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g., questionable material removed, risk accepted by commander (06 or above), request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to acknowledge receipt via email to the AWRAC ([redacted]@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 IAPMs



SAIS-IOA

Subject: Web Risk Assessment Findings

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 their families.

5. Definitions:

- a. CRITICAL: Information that is either classified or, when combined with other sensitive information, may have significant operational impact. It is information that could put either personnel or facilities at risk.
- b. MAJOR: Information in itself or in aggregation that is FOR OFFICIAL USE ONLY (FOUO).
- c. MINOR: All other violations that do not fall in either of the above two categories. Information, which may not be posted, on official web sites open to public access. Also, information that is contrary to the web policy guidance. (Note: Commanders may elect to assume this level of risk.)

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



THADDEUS A. DMUCHOWSKI  
COL, GS  
Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

SAIS-IOA

Subject: Web Risk Assessment Findings

## **WEB SITE CONTENT GUIDANCE**

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

Army Regulation (AR) 25-1, 31 May 2002, Army Information Management

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

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



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

April 24, 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 19 March 2002, the Headquarters, Department of the Army, Chief Information Officer (CIO)/G-6 Web Risk Assessment Cell was notified by the Office of SECDEF that persistent cookies may be located on the following AMEDD websites and being used for data collection. ( www.dewitt.wramc.amedd.army.mil , www.narmc.amedd.army.mil, www.wramc.amedd.army.mil). The following registration and security concerns were noted and rated by category (see below).

CATEGORY	Document	FINDING	REFERENCE	
Personnel	URL	Persistent Cookies		

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g., questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to

SAIS-IOA

Subject: Web Risk Assessment Findings

acknowledge receipt via email to the AWRAC

[REDACTED] my.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 IAPMs

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

5. Definitions:

- a. CRITICAL: Information that is either classified or, when combined with other sensitive information, may have significant operational impact. It is information that could put either personnel or facilities at risk.
- b. MAJOR: Information in itself or in aggregation that is FOR OFFICIAL USE ONLY (FOUO).
- c. MINOR: All other violations that do not fall in either of the above two categories. Information, which may not be posted, on official web sites open to public access. Also, information that is contrary to the web policy guidance. (Note: Commanders may elect to assume this level of risk.)

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

  
THADDEUS A. DMUCHOWSKI  
COL, GS  
Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

SAIS-IOA

Subject: Web Risk Assessment Findings

## **WEB SITE CONTENT GUIDANCE**

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

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

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

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



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

April 24, 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 19 March 2002, the Headquarters, Department of the Army, Chief Information Officer (CIO)/G-6 Web Risk Assessment Cell was notified by the SECDEF that persistent cookies may be located on the following website and being used for data collection. ([www.amsc.army.mil/rmo/memo](http://www.amsc.army.mil/rmo/memo)). The following registration and security concerns were noted and rated by category (see below).

CATEGORY	Document	FINDING	REFERENCE	
Personnel	URL	Persistent Cookies		

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g., questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to acknowledge receipt via email to the AWRAC ([\[REDACTED\].army.mil](mailto:[REDACTED].army.mil)) and forward the memorandum to the

SAIS-IOA

Subject: Web Risk Assessment Findings


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: 717-865-1785  
Email: [REDACTED]@ARMY.MIL

  
THADDEUS A. DHUCHOWSKI  
COL, GS  
Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

SAIS-IOA

Subject: Web Risk Assessment Findings

## **WEB SITE CONTENT GUIDANCE**

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

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

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

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





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

April 24, 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 19 March 2002, the Headquarters, Department of the Army, Chief Information Officer (CIO)/G-6 Web Risk Assessment Cell was notified by the SECDEF that persistent cookies may be located on the following website and being used for data collection. ([www.atrrs.army.mil](http://www.atrrs.army.mil)). The following registration and security concerns were noted and rated by category (see below).

CATEGORY	Document	FINDING	REFERENCE
Personnel	URL	Persistent Cookies	

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g., questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to acknowledge receipt via email to the AWRAC ([AWRAC@army.mil](mailto:AWRAC@army.mil)) and forward the memorandum to the

SAIS-IOA

Subject: Web Risk Assessment Findings


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] Z, Army Web Risk Assessment  
Analyst, COM: 717-865-1785  
Email: [REDACTED] ARMY.MIL

  
THADDEUS A. DMUCHOWSKI  
COL, GS  
Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

SAIS-IOA

Subject: Web Risk Assessment Findings

## **WEB SITE CONTENT GUIDANCE**

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

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

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

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



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: April 26, 2002

April 24, 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 22 April 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.bragg.army.mil/1-321far/chainofcommand.htm](http://www.bragg.army.mil/1-321far/chainofcommand.htm). This assessment was at the request of the Office of the Secretary of Defense. 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		Document	FINDING	REFERENCE
Force Protection	Major	Chain of Command	Unsecured web page contains names, photos, telephone number, and e-mail links, Information on Military operations	Web Site Admin Policies & procedures w/amendments 11 JAN 2002
Admin			privacy and security notice	same

SAIS-IOA

Subject: Web Risk Assessment Findings

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g., questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to acknowledge receipt via email to the AWRAC

[REDACTED]@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 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.)

SAIS-IOA

Subject: Web Risk Assessment Findings

6. POC: Mr. [REDACTED] Army Web Risk Assessment

Analyst, COM: 717-945-1785

Email: [REDACTED]@MIL

THADDEUS A. DMUCHOWSKI

COL, GS

Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

### WEB SITE CONTENT GUIDANCE

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

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

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

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

[REDACTED] this is to inform you that your Bio currently posted on the 1<sup>st</sup> Brigade website at, <http://www.lewis.army.mil/1bde/index2.html> is in violation of DoD and Army policy. It contains personal information about your family including you wife and son's name. (He is married to the former [REDACTED] They have one son, Connor)



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: 17 October 2002

7 October 2002

MEMORANDUM FOR WEB SITE ACTIVITY COMMANDER/SUPERVISOR  
(DCSLOG)  
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. During 4<sup>th</sup> quarter FY02, Headquarters, Department of the Army, Chief Information Officer (CIO)/G-6 Web Risk Assessment Cell was notified of security concerns on the following web sites. See Attached excel document.

CATEGORY	Document	FINDING	REFERENCE
Major	See attached	limited distribution and FOUO documents	Web Site Admin Policies & procedures w/amendments 11 JAN 2002 and AR25-1

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g., questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to



SAIS-IOA

Subject: Web Risk Assessment Findings

acknowledge receipt via email to the AWRAC

[REDACTED]@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 IAPMs

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

5. Definitions:

- a. CRITICAL: Information that is either classified or, when combined with other sensitive information, may have significant operational impact. It is information that could put either personnel or facilities at risk.
- b. MAJOR: Information in itself or in aggregation that is FOR OFFICIAL USE ONLY (FOUO).
- c. MINOR: All other violations that do not fall in either of the above two categories. Information, which may not be posted, on official web sites open to public access. Also, information that is contrary to the web policy guidance. (Note: Commanders may elect to assume this level of risk.)

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



THADDEUS A. DMUCHOWSKI  
COL, GS  
Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

SAIS-IOA

Subject: Web Risk Assessment Findings

### **WEB SITE CONTENT GUIDANCE**

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

Army Regulation (AR) 25-1, 31 May 2002, Army Information Management

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

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



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

April 24, 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 19 April 2002, the Headquarters, Department of the Army, Chief Information Officer (CIO)/G-6 Web Risk Assessment Cell was notified by the Office of Joint Web Risk Assessment Cell that persistent cookies may be located on the following website and being used for data collection. ([www.doim.army.mil](http://www.doim.army.mil)). The following registration and security concerns were noted and rated by category (see below).

CATEGORY	Document	FINDING	REFERENCE	
Personnel	URL	Persistent Cookies		

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g., questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to acknowledge receipt via email to the AWRAC ([\[REDACTED\]@s.army.mil](mailto:[REDACTED]@s.army.mil)) and forward the memorandum to the

SAIS-IOA

Subject: Web Risk Assessment Findings

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: [REDACTED] Army Web Risk Assessment  
Analyst COM: 717-865-1785  
Email: [REDACTED]@ARMY.MIL



THADDEUS A. DMUCHOWSKI  
COL, GS  
Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

SAIS-IOA

Subject: Web Risk Assessment Findings

## **WEB SITE CONTENT GUIDANCE**

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

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

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

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



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

Office, Chief Information Officer / G6

SAIS-IOA

April 29, 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 19 March 2002, the Headquarters, Department of the Army, Chief Information Officer (CIO)/G-6 Web Risk Assessment Cell was notified by the JWRAC that persistent cookies may be located on the following website and being used for data collection. ([www.drum.army.mil](http://www.drum.army.mil)). The following registration and security concerns were noted and rated by category (see below).

CATEGORY	Document	FINDING
Personnel	URL <a href="http://www.drum.army.mil/garrison/director/1215th/events2.gif">www.drum.army.mil/garrison/director/1215th/events2.gif</a>	Persistent Cookies

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g., questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to acknowledge receipt via email to the AWRAC ([\[REDACTED\]@army.mil](mailto:[REDACTED]@army.mil)) and forward the memorandum to the

SAIS-IOA

Subject: Web Risk Assessment Findings

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: 717-865-1785  
Email: [REDACTED]@ARMY.MIL



THADDEUS A. DMUCHOWSKI  
COL, GS  
Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

SAIS-IOA

Subject: Web Risk Assessment Findings

## **WEB SITE CONTENT GUIDANCE**

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

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

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

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





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

April 24, 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 19 April 2002, the Headquarters, Department of the Army, Chief Information Officer (CIO)/G-6 Web Risk Assessment Cell was notified by the Joint Web Risk Assessment Cell that persistent cookies may be located on the following website and being used for data collection. ([www.dugway.army.mil](http://www.dugway.army.mil)). The following registration and security concerns were noted and rated by category (see below).

CATEGORY	Document	FINDING	REFERENCE	
Personnel	URL	Persistent Cookies		

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g., questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to acknowledge receipt via email to the AWRAC

**[REDACTED]** [army.mil](mailto:[REDACTED]@army.mil)) and forward the memorandum to the

SAIS-IOA

Subject: Web Risk Assessment Findings


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: 717-865-1785  
Email: [REDACTED]@US.ARMY.MIL

  
THADDEUS A. DMUCHOWSKI  
COL, GS  
Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

SAIS-IOA

Subject: Web Risk Assessment Findings

## **WEB SITE CONTENT GUIDANCE**

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

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

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

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



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: 10 July 2002

June 21, 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 14 June 2002, the Headquarters, Department of the Army, Chief Information Officer (CIO)/G-6 Web Risk Assessment Cell conducted a routine assessment of your websites.

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial action. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to acknowledge receipt via email to the AWRAC ([REDACTED]@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 this memorandum. Copies of this memorandum will be furnished to the appropriate MACOM, PEO, PM IAPMs

SAIS-IOA

Subject: Web Risk Assessment Findings

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

5. Definitions:

- a. CRITICAL: Information that is either classified or, when combined with other sensitive information, may have significant operational impact. It is information that could put either personnel or facilities at risk.
- b. MAJOR: Information in itself or in aggregation that is FOR OFFICIAL USE ONLY (FOUO).
- c. MINOR: All other violations that do not fall in either of the above two categories. Information, which may not be posted, on official web sites open to public access. Also, information that is contrary to the web policy guidance. (Note: Commanders may elect to assume this level of risk.)

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



THADDEUS A. DMUCHOWSKI  
COL, GS  
Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

SAIS-IOA

Subject: Web Risk Assessment Findings

## **WEB SITE CONTENT GUIDANCE**

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

Army Regulation (AR) 25-1, 31 May 2002, Army Information Management

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

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



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

Office, Chief Information Officer / G6

SAIS-IOA

April 24, 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 19 March 2002, the Headquarters, Department of the Army, Chief Information Officer (CIO)/G-6 Web Risk Assessment Cell was notified by the JWRAC that persistent cookies may be located on the following website and being used for data collection. ([www.drum.army.mil](http://www.drum.army.mil)). The following registration and security concerns were noted and rated by category (see below).

CATEGORY	Document	FINDING	REFERENCE	
Personnel	URL	Persistent Cookies		

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g., questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to acknowledge receipt via email to the AWRAC [awrac@army.mil](mailto:awrac@army.mil)) and forward the memorandum to the

SAIS-IOA

Subject: Web Risk Assessment Findings

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: 717-865-1785

Email: [REDACTED]@S.ARMY.MIL



THADDEUS A. DWUCHOWSKI  
COL, GS  
Director, Information Assurance

CF: Appropriate MACOM/PEO/PM



SAIS-IOA

Subject: Web Risk Assessment Findings

## **WEB SITE CONTENT GUIDANCE**

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

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

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

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



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: April 21, 2002

April 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 (SEE ATTACHED FORSCOM DOC). 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	Document	FINDING	REFERENCE	
FORCE PROTECTION AND COMMUNICATIONS	SEE ATTACHED	DIRECTORY AND GILES REGISTRATION		
MINOR				

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g.,

SAIS-IOA

Subject: Web Risk Assessment Findings

questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to acknowledge receipt via email to the AWRAC

([REDACTED]@[REDACTED].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 IAPMS

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

5. Definitions:

- a. CRITICAL: Information that is either classified or, when combined with other sensitive information, may have significant operational impact. It is information that could put either personnel or facilities at risk.
- b. MAJOR: Information in itself or in aggregation that is FOR OFFICIAL USE ONLY (FOUO).
- c. MINOR: All other violations that do not fall in either of the above two categories. Information, which may not be posted, on official web sites open to public access. Also, information that is contrary to the web policy guidance. (Note: Commanders may elect to assume this level of risk.)

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



THADDEUS A. DMUCHOWSKI  
COL, GS  
Director, Information Assurance

SAIS-IOA  
Subject: Web Risk Assessment Findings

CF: Appropriate MACOM/PEO/PM

## **WEB SITE CONTENT GUIDANCE**

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

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

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

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



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

Office, Chief Information Officer / G6

SAIS-IOA

S: 15 July 2002

June 26, 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 14 June 2002, the Headquarters, Department of the Army, Chief Information Officer (CIO)/G-6 Web Risk Assessment Cell conducted a routine assessment of your website (See attached).

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g., questionable material removed, risk accepted by commander (06 or above), request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to acknowledge receipt via email to the AWRAC

[REDACTED]@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 IAFMs

SAIS-IOA

Subject: Web Risk Assessment Findings

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

5. Definitions:

- a. CRITICAL: Information that is either classified or, when combined with other sensitive information, may have significant operational impact. It is information that could put either personnel or facilities at risk.
- b. MAJOR: Information in itself or in aggregation that is FOR OFFICIAL USE ONLY (FOUO).
- c. MINOR: All other violations that do not fall in either of the above two categories. Information, which may not be posted, on official web sites open to public access. Also, information that is contrary to the web policy guidance. (Note: Commanders may elect to assume this level of risk.)

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



THADDEUS A. DMUCHOWSKI  
COL, GS  
Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

SAIS-IOA  
Subject: Web Risk Assessment Findings

## **WEB SITE CONTENT GUIDANCE**

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

Army Regulation (AR) 25-1, 31 May 2002, Army Information Management

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

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



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

April 24, 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 19 April 2002, the Headquarters, Department of the Army, Chief Information Officer (CIO)/G-6 Web Risk Assessment Cell was notified by the Joint Web Risk Assessment Cell that persistent cookies may be located on the following website and being used for data collection. (www.hq.c5.army.mil ). The following registration and security concerns were noted and rated by category (see below).

CATEGORY	Document	FINDING	REFERENCE	
Personnel	URL	Persistent Cookies		

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g., questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to acknowledge receipt via email to the AWRAC

[REDACTED]@hq.c5.army.mil) and forward the memorandum to the



SAIS-IOA

Subject: Web Risk Assessment Findings

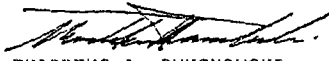
commander/ supervisor, or his/her designated representative, responsible for the website. Suspense dates for corrective actions/resolution of security concerns are provided in the memorandum. Copies of this memorandum will be furnished to the appropriate MACOM, PEO, PM IAPMs

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: 717-865-1785  
Email: [REDACTED] ARMY.MIL

  
THADDEUS A. DMUCHOWSKI  
COL, GS  
Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

SAIS-IOA

Subject: Web Risk Assessment Findings

## **WEB SITE CONTENT GUIDANCE**

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

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

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

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



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

Office, Chief Information Officer / G6

NETC-ESTA-A

S: 7 December 2002

20 November 2002

MEMORANDUM FOR WEB SITE ACTIVITY COMMANDER/SUPERVISOR  
(HQ ISIC)

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. During 4<sup>th</sup> quarter FY02, Headquarters, Department of the Army, Chief Information Officer Web Risk Assessment Cell was notified of security concerns on the following web sites. See Attached excel document.

CATEGORY	Document	FINDING	REFERENCE
Major	See attached	limited distribution and FOUO documents	Web Site Admin Policies & procedures w/amendments 11 JAN 2002 and AR25-1

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g., questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to

NETC-ESTA-A

Subject: Web Risk Assessment Findings

acknowledge receipt of email to the AWRAC  
[REDACTED] (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 IAPMs

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

5. Definitions:

- a. CRITICAL: Information that is either classified or, when combined with other sensitive information, may have significant operational impact. It is information that could put either personnel or facilities at risk.
- b. MAJOR: Information in itself or in aggregation that is FOR OFFICIAL USE ONLY (FOUO).
- c. MINOR: All other violations that do not fall in either of the above two categories. Information, which may not be posted, on official web sites open to public access. Also, information that is contrary to the web policy guidance. (Note: Commanders may elect to assume this level of risk.)

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



THADDEUS A. DMUCHOWSKI  
COL, GS  
Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

NETC-ESTA-A

Subject: Web Risk Assessment Findings

### **WEB SITE CONTENT GUIDANCE**

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

Army Regulation (AR) 25-1, 31 May 2002, Army Information Management

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

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



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: July 10, 2002

June 14, 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 14 June 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.hqda.army.mil/acsimweb/doc/Tab00CPost25JAN.ppt](http://www.hqda.army.mil/acsimweb/doc/Tab00CPost25JAN.ppt)). The following registration and security concerns were noted and rated by category (see below).

CATEGORY	Document	FINDING	REFERENCE
Force Protection Major	Installation Security Open Vs. Closed Post	Unsecured web page Documents: Marked FOR OFFICIAL USE ONLY	AR25-1 31 March 2002 p.69 r(4)(b)

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g., questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to acknowledge receipt via email to the AWRAC ([AWRAC@us.army.mil](mailto:AWRAC@us.army.mil)) and forward the memorandum to the commander/ supervisor, or his/her designated representative,

SAIS-IOA

Subject: Web Risk Assessment Findings

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: 717-865-1785  
Email: [REDACTED]@ARMY.MIL



THADDEUS A. DMUCHOWSKI  
COL, GS  
Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

SAIS-IOA

Subject: Web Risk Assessment Findings

## **WEB SITE CONTENT GUIDANCE**

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

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

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

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





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

Office, Chief Information Officer / G6

NETC-ESTA-A

S: 31 December 2002

3 December 2002

MEMORANDUM FOR WEB SITE ACTIVITY COMMANDER/SUPERVISOR  
(ISED)  
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. During 4<sup>th</sup> quarter FY02, Headquarters, Department of the Army, Chief Information Officer Web Risk Assessment Cell was notified of security concerns on the following web sites. See Attached excel document.

CATEGORY	Document	FINDING	REFERENCE
Major	See attached	limited distribution and FOUO documents	Web Site Admin Policies & procedures w/amendments 11 JAN 2002 and AR25-1

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g., questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to

NETC-ESTA-A

Subject: Web Risk Assessment Findings

acknowledge receipt via email to the AWRAC

[REDACTED]@us.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 IAPMs

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

5. Definitions:

- a. CRITICAL: Information that is either classified or, when combined with other sensitive information, may have significant operational impact. It is information that could put either personnel or facilities at risk.
- b. MAJOR: Information in itself or in aggregation that is FOR OFFICIAL USE ONLY (FOUO).
- c. MINOR: All other violations that do not fall in either of the above two categories. Information, which may not be posted, on official web sites open to public access. Also, information that is contrary to the web policy guidance. (Note: Commanders may elect to assume this level of risk.)

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



THADDEUS A. DMUCHOWSKI  
COL, GS  
Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

NETC-ESTA-A

Subject: Web Risk Assessment Findings

### **WEB SITE CONTENT GUIDANCE**

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

Army Regulation (AR) 25-1, 31 May 2002, Army Information Management

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

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



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: July 10, 2002

June 14, 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 14 June 2002, the Headquarters, Department of the Army, Chief Information Officer (CIO)/G-6 Web Risk Assessment Cell conducted an assessment of your web site (<http://www.jagcnet.army.mil/JAGCLeadership>). The following registration and security concerns were noted and rated by category (see below).

CATEGORY	Document	FINDING	REFERENCE
Personnel  MINOR	Leaderships BIO	Unsecured web page Documents: Bio for MG Romig and CW5 Swartworth contains full DOB	Web Site Admin Policies & procedures w/amendments 11 JAN 2002 Para. 3.5.3.4

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

SAIS-IOA

Subject: Web Risk Assessment Findings

security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to acknowledge receipt via email to the AWRAC ([REDACTED]@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 IAPMs

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

5. Definitions:

- a. CRITICAL: Information that is either classified or, when combined with other sensitive information, may have significant operational impact. It is information that could put either personnel or facilities at risk.
- b. MAJOR: Information in itself or in aggregation that is FOR OFFICIAL USE ONLY (FOUO).
- c. MINOR: All other violations that do not fall in either of the above two categories. Information, which may not be posted, on official web sites open to public access. Also, information that is contrary to the web policy guidance. (Note: Commanders may elect to assume this level of risk.)

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



THADDEUS A. DMUCHOWSKI  
COL, GS  
Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

SAIS-IOA  
Subject: Web Risk Assessment Findings

## **WEB SITE CONTENT GUIDANCE**

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

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

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

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



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

April 24, 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 19 March 2002, the Headquarters, Department of the Army, Chief Information Officer (CIO)/G-6 Web Risk Assessment Cell was notified by the Office of SECDEF that persistent cookies may be located on the following website and being used for data collection. ([www.jag2.army.mil](http://www.jag2.army.mil)). The following registration and security concerns were noted and rated by category (see below).

CATEGORY	Document	FINDING	REFERENCE
Personnel	URL	Persistent Cookies	

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g., questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to acknowledge receipt via email to the AWRAC [awrac@army.mil](mailto:awrac@army.mil)) and forward the memorandum to the

SAIS-IOA

Subject: Web Risk Assessment Findings  
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: 717-865-1785  
Email: [REDACTED]@ARMY.MIL



THADDEUS A. DMUCHOWSKI  
COL, GS  
Director, Information Assurance

CF: Appropriate MACOM/PEO/PM



SAIS-IOA

Subject: Web Risk Assessment Findings

## **WEB SITE CONTENT GUIDANCE**

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

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

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

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



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: 26 JUNE 2002

May 29, 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 29 May 2002, the Headquarters, Department of the Army, Chief Information Officer (CIO)/G-6 Web Risk Assessment Cell conducted a routine assessment of the attached websites. Of the URLs reviewed most were out of date publications with restrictions on distribution.

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g., questionable material removed, risk accepted by commander (06 or above), request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to acknowledge receipt via email to the AWRAC

([REDACTED], 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 IAPMs

SAIS-IOA

Subject: Web Risk Assessment Findings

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

5. Definitions:

- a. CRITICAL: Information that is either classified or, when combined with other sensitive information, may have significant operational impact. It is information that could put either personnel or facilities at risk.
- b. MAJOR: Information in itself or in aggregation that is FOR OFFICIAL USE ONLY (FOUO).
- c. MINOR: All other violations that do not fall in either of the above two categories. Information, which may not be posted, on official web sites open to public access. Also, information that is contrary to the web policy guidance. (Note: Commanders may elect to assume this level of risk.)

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



THADDEUS A. DMUCHOWSKI  
COL, GS  
Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

SAIS-IOA  
Subject: Web Risk Assessment Findings

## **WEB SITE CONTENT GUIDANCE**

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

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

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

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



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: May 10, 2002

May 1, 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 25 April 2002, the Headquarters, Department of the Army, Chief Information Officer (CIO)/G-6 Web Risk Assessment Cell conducted an assessment of your web site.

([https://dsc.mtmc.army.mil/lessonslearned/DST\\_Holding\\_Area/DST\\_KF\\_OR\\_06.htm](https://dsc.mtmc.army.mil/lessonslearned/DST_Holding_Area/DST_KF_OR_06.htm)) 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	Document	FINDING	REFERENCE
Minor	K FOR	Document has lesson learned for port operation	Web Site Admin Policies & procedures w/amendments 11 JAN 2002 para 3.5.3.1

SAIS-IOA

Subject: Web Risk Assessment Findings

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g.,

questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to acknowledge receipt via email to the AWRAC

(~~XXXXXXXXXX~~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 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 their 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.)

SAIS-IOA

Subject: Web Risk Assessment Findings

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



THADDEUS A. DMUCHOWSKI  
COL, GS  
Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

### WEB SITE CONTENT GUIDANCE

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

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

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

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



REPLY TO  
ATTENTION OF:

DEPARTMENT OF THE ARMY  
NETWORK ENTERPRISE TECHNOLOGY COMMAND/  
9<sup>TH</sup> ARMY SIGNAL COMMAND  
2133 CUSHING STREET  
FORT HUACHUCA, ARIZONA 85613-7070





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: 17 October 2002

7 October 2002

MEMORANDUM FOR WEB SITE ACTIVITY COMMANDER/SUPERVISOR  
(ODCOSOPS HQUSAREUR)  
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. During 4<sup>th</sup> quarter FY02, Headquarters, Department of the Army, Chief Information Officer (CIO)/G-6 Web Risk Assessment Cell was notified of security concerns on the following web sites. See Attached excel document.

CATEGORY	Document	FINDING	REFERENCE
Major	See attached	Documents marked FOUO	Web Site Admin Policies & procedures w/amendments 11 JAN 2002 and AR25-1

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g., questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to

SAIS-IOA

Subject: Web Risk Assessment Findings

acknowledge receipt via email to the AWRAC

[REDACTED] s.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 IAPMs

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

5. Definitions:

- a. CRITICAL: Information that is either classified or, when combined with other sensitive information, may have significant operational impact. It is information that could put either personnel or facilities at risk.
- b. MAJOR: Information in itself or in aggregation that is FOR OFFICIAL USE ONLY (FOUO).
- c. MINOR: All other violations that do not fall in either of the above two categories. Information, which may not be posted, on official web sites open to public access. Also, information that is contrary to the web policy guidance. (Note: Commanders may elect to assume this level of risk.)

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



THADDEUS A. DMUCHOWSKI  
COL, GS  
Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

SAIS-IOA

Subject: Web Risk Assessment Findings

### **WEB SITE CONTENT GUIDANCE**

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

Army Regulation (AR) 25-1, 31 May 2002, Army Information Management

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

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



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: April 15, 2002

March 30, 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 <http://cpolrhp.army.mil/west/FPIInformation/DownloadWinframe/DownloadWinFrameInstructions/WinFrameInstructions.doc>. 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	Document	FINDING	REFERENCE
Force Protection  MINOR		Unsecured web page Document marked FOUO No information that constitutes a security violation	Web Site Admin Policies & procedures w/amendments 11 JAN 2002
			Ref. OSAO- 0039

SAIS-IOA

Subject: Web Risk Assessment Findings

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g., questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to acknowledge receipt via email to the AWRAC

([REDACTED]@[REDACTED].s.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 IAPMs


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

5. Definitions:

- a. CRITICAL: Information that is either classified or, when combined with other sensitive information, may have significant operational impact. It is information that could put either personnel or facilities at risk.
- b. MAJOR: Information in itself or in aggregation that is FOR OFFICIAL USE ONLY (FOUO).
- c. MINOR: All other violations that do not fall in either of the above two categories. Information, which may not be posted, on official web sites open to public access. Also, information that is contrary to the web policy guidance. (Note: Commanders may elect to assume this level of risk.)

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

SAIS-IOA  
Subject: Web Risk Assessment Findings

  
THADDEUS A. DMUCHOWSKI  
COL, GS  
Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

## WEB SITE CONTENT GUIDANCE

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

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

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

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



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: April 15, 2002

March 30, 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 <http://gordon.army.mil/stt/31c/c03lp1sa2.htm>. 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	Document	FINDING	REFERENCE
Force Protection  MINOR		Unsecured web page Document marked FOUO No information that constitutes a security violation	Web Site Admin Policies & procedures w/amendments 11 JAN 2002
			Ref. OSAO- 0040

SAIS-IOA

Subject: Web Risk Assessment Findings

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g., questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to acknowledge receipt of email to the AWRAC [REDACTED] (my.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 IAPMs

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

5. Definitions:

- a. CRITICAL: Information that is either classified or, when combined with other sensitive information, may have significant operational impact. It is information that could put either personnel or facilities at risk.
- b. MAJOR: Information in itself or in aggregation that is FOR OFFICIAL USE ONLY (FOUO).
- c. MINOR: All other violations that do not fall in either of the above two categories. Information, which may not be posted, on official web sites open to public access. Also, information that is contrary to the web policy guidance. (Note: Commanders may elect to assume this level of risk.)

6. POC: Mr. [REDACTED] Army Web Risk Assessment  
Analyst, COM: 717-865-1705  
Email: [REDACTED]@S.ARMY.MIL



SAIS-IOA

Subject: Web Risk Assessment Findings



THADDEUS A. DMUCHOWSKI  
COL, GS  
Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

### **WEB SITE CONTENT GUIDANCE**

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

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

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

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



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: April 15, 2002

March 30, 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 <http://www.amc.army.mil/amc/rda/rda-ap/parc3/acq-issues.ppt> and <http://www.amc.army.mil/amc/rda/rda-ap/parc3/mang-amc-kts.ppt>. 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	Document	FINDING	REFERENCE	
Force Protection  MINOR	FY 2000 IG finding, power point slides, Phone dir w/names & positions	Unsecured web page Document marked FOUO No information that constitutes a security violation	Web Site Admin Policies & procedures w/amendments 11 JAN 2002	
			Ref. OSAO-0041/42	

SAIS-IOA

Subject: Web Risk Assessment Findings

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g., questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to acknowledge receipt via email to the AWRAC [REDACTED].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 IAPMs

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

5. Definitions:

- a. CRITICAL: Information that is either classified or, when combined with other sensitive information, may have significant operational impact. It is information that could put either personnel or facilities at risk.
- b. MAJOR: Information in itself or in aggregation that is FOR OFFICIAL USE ONLY (FOUO).
- c. MINOR: All other violations that do not fall in either of the above two categories. Information, which may not be posted, on official web sites open to public access. Also, information that is contrary to the web policy guidance. (Note: Commanders may elect to assume this level of risk.)

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

SAIS-IOA

Subject: Web Risk Assessment Findings



THADDEUS A. DMUCHOWSKI

COL, GS

Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

### **WEB SITE CONTENT GUIDANCE**

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

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

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

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



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: April 15, 2002

March 30, 2002

MEMORANDUM FOR WEB SITE ACTIVITY COMMANDER/SUPERVISOR

SUBJECT: Web Risk Assessment Findings

1. References:

- a. DoD 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 [http://www.leav.army.mil/tsmmcsweb/ftp/Merged\\_EORs\\_01\\_26\\_01\\_Access97\\_v107.mdb](http://www.leav.army.mil/tsmmcsweb/ftp/Merged_EORs_01_26_01_Access97_v107.mdb). 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	Document	FINDING	REFERENCE
----------	----------	---------	-----------

SAIS-IOA

Subject: Web Risk Assessment Findings

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g., questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to acknowledge receipt via email to the AWRAC

[REDACTED] 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: 717-865-1785  
Email: [REDACTED].ARMY.MIL

SAIS-IOA

Subject: Web Risk Assessment Findings



THADDEUS A. DMUCHOWSKI

COL, GS

Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

### WEB SITE CONTENT GUIDANCE

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

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

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

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



Office, Chief Information Officer / G6

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

SAIS-IOA

S: April 10, 2002

March 27, 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 <http://tsc.wes.army.mil/downloads/CADDSymposium2000/register.mdb>. 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	Document	FINDING	REFERENCE
Personnel Minor	Directory	Info on personnel.	Web Site Admin
Administration Minor	Web Site	No evident of GILS registration	Policies & procedures w/amendments 11 JAN 2002
			Osao-0049

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g.,



SAIS-IOA

Subject: Web Risk Assessment Findings

questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to acknowledge receipt via email to the AWRAC

(~~XXXXXXXXXX~~.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 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. ~~XXXXXXXXXX~~ Army Web Risk Assessment Analyst, COM: 717-865-1785  
Email: ~~XXXXXXXXXX~~ @US.ARMY.MIL

SAIS-IOA

Subject: Web Risk Assessment Findings



THADDEUS A. DMUCHOWSKI  
COL, GS  
Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

### WEB SITE CONTENT GUIDANCE

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

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

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

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



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: April 10, 2002

March 27, 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 [http://www.apg.army.mil/Phones/Directory\\_Access97.mdb](http://www.apg.army.mil/Phones/Directory_Access97.mdb). 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	Document	FINDING	REFERENCE
Personnel Minor	Directory	Info on personnel.	Web Site Admin
Administration Minor	Web Site	No evident of GILS registration	Policies & procedures w/amendments 11 JAN 2002
			Osao-0050

3. The Army Web Risk Assessment Cell (AWRAC) program requires that commanders/supervisors of affected websites be notified of security concerns and take appropriate remedial actions, e.g.,

SAIS-IOA

Subject: Web Risk Assessment Findings

questionable material removed, risk accepted by commander, request for clarifying information. The AWRAC will report security concerns via e-mail memorandum to the point of contact (POC) posted on the website. Website POCs are directed to acknowledge receipt via email to the AWRAC

[REDACTED].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 IAPMs

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

5. Definitions:

- a. CRITICAL: Information that is either classified or, when combined with other sensitive information, may have significant operational impact. It is information that could put either personnel or facilities at risk.
- b. MAJOR: Information in itself or in aggregation that is FOR OFFICIAL USE ONLY (FOUO).
- c. MINOR: All other violations that do not fall in either of the above two categories. Information, which may not be posted, on official web sites open to public access. Also, information that is contrary to the web policy guidance. (Note: Commanders may elect to assume this level of risk.)

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

SAIS-IOA

Subject: Web Risk Assessment Findings



THADDEUS A. DMUCHOWSKI

COL, GS

Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

## WEB SITE CONTENT GUIDANCE

Memorandum, Office of the Secretary of Defense, November 25, 1998, Subject: Web Site Administration Policies and Procedures

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

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

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

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

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

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

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

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

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