



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 website.

[http://www.USARC.army.mil/dcsint2/documents/security/Joint%20Pub%2003-07.2%20Joint%20Tac,%20Tech,%20and%20Proced%20for%20AT/APPENDIX J THREATCON SYSTEM.doc](http://www.USARC.army.mil/dcsint2/documents/security/Joint%20Pub%2003-07.2%20Joint%20Tac,%20Tech,%20and%20Proced%20for%20AT/APPENDIX%20J%20THREATCON%20SYSTEM.doc)

http://www.usarc.army.mil/dcsint2/RC_MI_Units/RC_MI_Units_RSC.htm#map

http://www.usarc.army.mil/dcsint2/ARISC_Pages/WARISC/W%20ARISC%20Brief.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).

SAIS-IOA

Subject: Web Risk Assessment Findings

CATEGORY		Document	FINDING	REFERENCE	
Force Protection	Major	APPENDIX J FOUO THREATCON SYSTEM, PPT presentation, RC MI Unit MAPS	Unsecured web page contains extensive documentation on THREATCON levels. FOUO, Ids MI units and locations, presentation contains intell information and floor plans.	Web Site Admin Policies & procedures w/amendments 11 JAN 2002	
				OSA0-0110	

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).

SAIS-IOA

Subject: Web Risk Assessment Findings

- 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

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: 17 October 2002

7 October 2002

MEMORANDUM FOR WEB SITE ACTIVITY COMMANDER/SUPERVISOR
(PER HQUSAEUR)

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 4th 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].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



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



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 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 PERSCOM 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]@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 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

3 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://iassure.usareur.army.mil/>. The following security concerns were noted and rated by category (see below).

CATEGORY	Document	FINDING	REFERENCE
IA Major	https://iassure.usareur.army.mil/	Unsecured web page Document marked FOUO	Web Site Admin Policies & procedures w/amendments 11 JAN 2002
major	IAVA Documents	FOUO	

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].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: 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://sill-www.army.mil/](https://http://sill-www.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	Web Site Admin Policies & procedures w/amendments 11 JAN 2002

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]@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]@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, 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: 17 October 2002

7 October 2002

MEMORANDUM FOR WEB SITE ACTIVITY COMMANDER/SUPERVISOR
(Space and Missile Defense Command)
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 4th 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 or limited distribution can not be on open web sites	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]@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

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



Office, Chief Information Officer / G6

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

NETC-ESTA-A

S: 30 JULY 2003

30 July 2003

MEMORANDUM FOR WEB SITE ACTIVITY COMMANDER/SUPERVISOR
(Fort Stewart)
SUBJECT: Web Risk Assessment Findings

1. References:

- a. DA Message, (U) Armywide Website OPSEC Review, DTGs 122240Z MAR 03 and 282237Z Feb 03.
- b. DoDI 5230.29 Security and Policy Review of DoD Information for Public Release, 6 March 1996
- a. Memorandum, Deputy Secretary of Defense, dated 24 September 1998, Information Vulnerability and the World Wide Web.
- b. Memorandum, Assistant Secretary of Defense, dated 28 December 2001, Removal of Personally Identifying Information of DOD Personnel from Unclassified Websites

2. The Department of the Army is currently reviewing U.S. Army Web sites for OPSEC compliance. On 17 May 03, an OPSEC analyst along with an senior Intel analyst found your website containing sensitive information regarding your organization which should not be posted on an open/public web site based on current DoD and Army Directives and Policies. The OPSEC concern for your organization's website has been classified as a Minor finding.

CATEGORY	Document	FINDING	REFERENCE
Major	http://www.stewart.army.mil/redeployment/redeployment07-29-03.htm	redeployment information	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

NETC-ESTA-A

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]@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. P [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: 30 July 2002

July 19, 2002

MEMORANDUM FOR WEB SITE ACTIVITY COMMANDER/SUPERVISOR (STRICOM)

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 July 2002, the Headquarters, Department of the Army, Chief Information Officer (CIO)/G-6 Web Risk Assessment Cell conducted a routine assessment of your websites per your request (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]@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

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]@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 SECDEF that persistent cookies may be located on the following website and being used for data collection. (www.stricom.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 ([\[REDACTED\]@us.army.mil](mailto:[REDACTED]@us.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: 30 September 2002

16 September 2002

MEMORANDUM FOR WEB SITE ACTIVITY COMMANDER/SUPERVISOR(TACOM)

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 17 August 2002, the Headquarters, Department of the Army, Chief Information Officer (CIO)/G-6 Web Risk Assessment Cell conducted a routine assessment of your websites per your request (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 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, 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



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

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.tasa.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 (as.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

NETC-ESTA-A

S: 15 December 2004
9 December 2004

MEMORANDUM FOR WEB SITE ACTIVITY COMMANDER/SUPERVISOR
NAME of unit

SUBJECT: Web Risk Assessment Findings

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

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

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

NETC-ESTA-A

Subject: Web Risk Assessment Findings

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

5. 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

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, 30 JUN 2004, Army Knowledge Management and Information Technology Management

Army Regulation (AR) 25-2 14 November 2003 Information Assurance

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

April 4, 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 website. As per the attached. 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	

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 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]@US.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



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 20, 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 June 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.

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]@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

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].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 20, 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 June 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. Documents with restricted distribution were located on the open website.

http://www.usace.army.mil/inet/usace-docs/eng-regs/er405-1-12/toc.htm	DISTRIBUTION		
http://www.usace.army.mil/inet/usace-docs/s-r/ec405-1-71/entire.pdf	DISTRIBUTION		
http://www.usace.army.mil/inet/usace-docs/s-r/ec405-1-71/toc.htm	DISTRIBUTION		
http://www.usace.army.mil/usace-docs/eng-regs/er405-1-12/toc.htm	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

SAIS-IOA

Subject: Web Risk Assessment Findings


[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]@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: 12 September 2003

2 September 2003

MEMORANDUM FOR WEB SITE ACTIVITY COMMANDER/SUPERVISOR

SUBJECT: Web Risk Assessment Findings (USARJ Band)

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.usarj.army.mil/organization/296band/chief.htm> <http://www.usarj.army.mil/organization/296band/sgm.htm>). The following registration and security concerns were noted and rated by category (see below).

CATEGORY	Document	FINDING	REFERENCE
Personnel Major	Leaderships BIO	Unsecured web page Documents: Bio for Commander and CSM contains full DOB Family member information.	Web Site 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]@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]@S.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

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.usma.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@usma.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]@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: 17 October 2002

7 October 2002

MEMORANDUM FOR WEB SITE ACTIVITY COMMANDER/SUPERVISOR
(V Corps)

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 4th 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]@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



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

Army Web Risk Assessment Cell
(AWRAC)
Concept of Operations
(CONOPS)

10 March 2002

Table of Contents

1. Executive Summary.....	1
2. Background.....	1
3. Joint Web Risk Assessment Cell Mission Concept.....	2
3.1 Website Patrolling.....	2
3.2 Bulk Analysis.....	2
3.3 Operations Security Analysis.....	3
4. Army Web Risk Assessment Cell Mission Concept.....	3
4.1 Force Protection.....	4
4.2 Enforcement of OSD-C3I Guidance.....	4
4.3 Ad-Hoc Tasking.....	4
5. Structure.....	4
6. Training.....	4
7. Responsibilities.....	5
7.1 Operations Security Checklist.....	6
7.2 Website Database.....	6
7.3 AWRAC Duties.....	6
7.3.1 Web Risk Analysis.....	7
7.3.2 Monthly Analysis.....	7
7.3.3 Random Website Inspections.....	8
7.3.4 Ad Hoc Taskings.....	8
Appendix A References.....	8
Appendix B Glossary.....	9
Appendix C Operations Security Checklist.....	10

Army Web Risk Assessment Cell Concept Of Operations

"This initiative represents both a new model and a total force solution for managing operations security in an environment of rapidly changing technology. It is essential that each of the military components and agencies get on board so that we can expedite the implementation of JWRAC and help it fulfill its important mission."

John J. Hamre, Deputy Secretary of Defense

1. Executive Summary

The Internet continues to grow at an ever-increasing pace and people are becoming more connected with the world around them. The Department of Defense (DoD) has mandated that DoD websites be made available to the public and will provide accurate and timely information relating to its activities, objectives, policies, and programs. This in turn has increased the ease of access and availability of information throughout the Department of the Army (DA) and provides unprecedented access to military information that was not available to the general public just few years ago.

Unfortunately the growth and popularity of the Internet has also led to an increase in malicious activity, intrusions, and information warfare (IW) attacks directed against DA computer systems and networks. The benefits gained by using the Internet to convey information must be balanced against the potential threat of attack. The Army must implement comprehensive risk management and risk assessment programs to protect against potential exploitation of this information. The Army, in recognition of the potential threat, has implemented information assurance (IA) policies and procedures and has installed security tools such as firewalls, intrusion detection systems, access control mechanisms, and virus detection software to better protect its computer systems and networks.

Internet has increased the ease of access and availability of information throughout DoD. Department of the Army websites provide unprecedented access to military information to the general public that was not accessible just a few years ago. The benefits gained by using the Internet to convey information must be balanced by providing a comprehensive risk management and risk assessment program to protect against potential exploitation of this information. The Army Web Risk Assessment Cell (AWRAC) is the catalyst to ensure that Army websites are compliant with Federal, DoD, and DA policies, procedures, and best practices.

This document serves as the AWRAC Concept of Operations (CONOP) for Army Website (.mil) vulnerability analysis. This document provides an overview of the DoD Joint Web Risk Analysis Cell (JWRAC) to include it's concept, mission, and capabilities. The purpose of this document is to outline the concept, guidance, and procedures to establish an Army Web Risk Assessment Cell.

2. Background

The formation of the Joint Web Risk Assessment Cell (JWRAC) is a result of a September 24, 1998 directive from Dr. John J. Hamre, Deputy Secretary of Defense, to Charles L. Cragin, acting Assistant Secretary of Defense for Reserve Affairs, and Gen. Henry H. Shelton, Chairman of the Joint Chiefs of Staff. Dr. Hamre directed that they jointly develop a plan that uses Reserve forces personnel to conduct operations security and threat assessments of DefenseLINK and other official military Web sites.

On 12 February 1999, Secretary of Defense William S. Cohen approved the creation of a 22-member Reserve component team to monitor and evaluate DoD Websites to ensure that those sites do not compromise national security by revealing sensitive defense information. The team (JWRAC) is comprised of two full-time Reservists and 20 drilling Reserve and National Guard personnel from the Army, Navy, Air Force, and Marine Corps. The Defense Information Systems Agency (DISA) established the JWRAC in March 1999 and maintains operational control as it performs its day-to-day activities.

3. JWRAC Mission Concept

The JWRAC mission is to search DoD Websites for information and trends of data that could be used to breach security or pose a threat to Defense operations and personnel. In addition, the JWRAC evaluates website content to ensure compliance with departmental policies, procedures, and best practices. The JWRAC's core mission consists of website patrolling, bulk analysis, and operations security analysis.

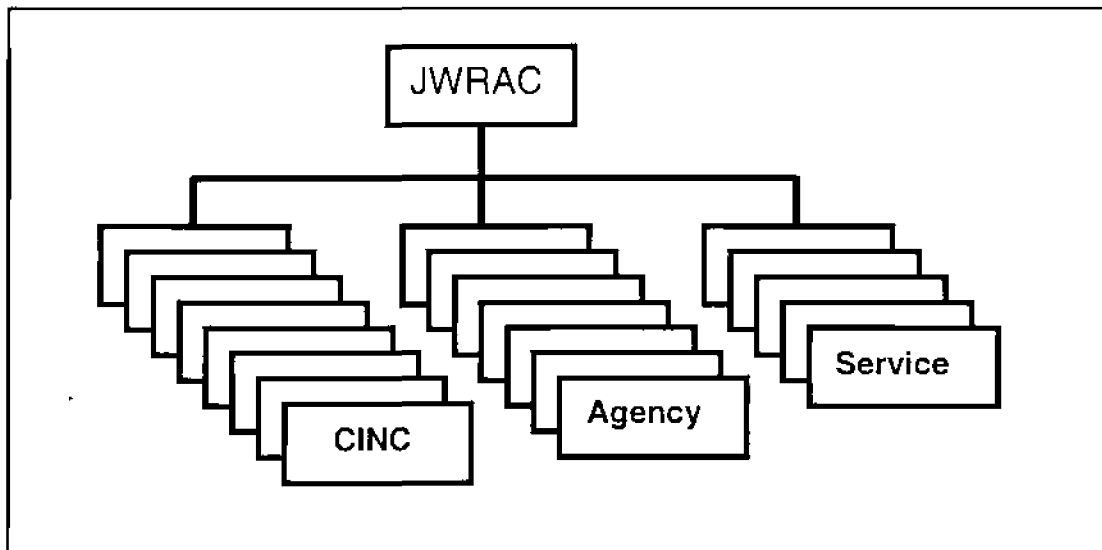


Figure1: JWRAC Responsibilities

3.1 Website Patrolling

JWRAC analysts perform site-by-site, page-by-page evaluation of website content. Using a browser, Operations Security (OPSEC) guidance, and a list of target websites, analysts will visit each DoD Website and manually evaluate the content of each page on the site for:

- Inappropriate links to commercial sites, personal sites, and sensitive or classified sites.
- Information on Operation Plans (OPLAN) or planning that includes: force readiness, pre-deployment activities, schedules for movement, support requirements, and any element of an OPLAN or Operation Order (OPORD).
- Information on current or future Joint, theater, or service major exercises. This will include schedules for force movements or exercise play, locations, support, and transportation requirements.
- Information pertaining to weapons technology to include; ranges, number of weapons deployed, locations and units where weapons are stored and/or used, transportation of weapons systems, cost, and instructions for their use, handling, safety, or maintenance.
- Information pertaining to non-DoD information relating to competitive contracting or information under limited release restrictions.
- Identify information counter-productive to counter terrorism and installation/site security.

3.2 Bulk Analysis.

Using automated tools to analyze DoD website content for patterns of characters. Templates known as "FINDER" are used for OPLAN personnel/personal information, sensitive information, and high risk format types. These Finders will identify possible incidents of target information within captured web content and provide a list of target Uniform Resource Locators (URL). The analysts will then verify if the information at the URL is an OPSEC concern. The analyst will operate with the following objectives:

- Identify all information in web content where discussions of DoD OPLANs and current operations are taking place. Evaluate this information for possible OPSEC concern.
- Identify web content where personal or personnel data may be present. Analyze that content for instances of information identifying dependent associations with service members, places of residence and birth, home telephone numbers, dates of birth, and social security number (SSN).
- Identify all information in web content where personal information is present. Evaluate this information for possible OPSEC violations.

Army Web Risk Assessment Cell Concept Of Operations

- Identify all information in web content that is marked for limited distribution or as For Official Use Only (FOUO), Confidential, Secret, and/or Top Secret.

3.1 Operations Security Analysis

Using RetrivalWare and other tools and techniques to develop a complete analysis of service commands, major commands, or Commanders-in-Chief (CINC) operations planning from information in DoD web content. Analysts will:

- Develop lists of information through website patrolling and bulk analysis and use web search tools and analysis techniques to develop information that identifies current operations or contingency plans.
- Receive ad-hoc taskings from the DoD Computer Emergency Response Team (CERT) to identify and analyze web content information as it pertains to target concepts.

4. AWRAC Mission Concept

The mission of the Army Web Risk Assessment Cell is to ensure publicly accessible, non-restricted, U.S. Army world wide web (WWW) websites are compliant with Federal, DoD, and DA website administration policies, procedures, and best practices.

To accomplish this mission, the Army Web Risk Assessment Cell must mirror the efforts of the JWRAC (Web site patrolling, bulk analysis, Operations Security Analysis). The AWRAC must also provide detailed analysis for (1) force protection (2) enforcement of Office of the Secretary of Defense for Command, Control, and Communications, and Intelligence (OSD-C3I) and Army website administrative guidance (3) ad-hoc taskings and (4) registration with the Government Information Locator Service (GILS). The AWRAC will employ the same mission concepts as the JWRAC but will focus their efforts on Army websites.

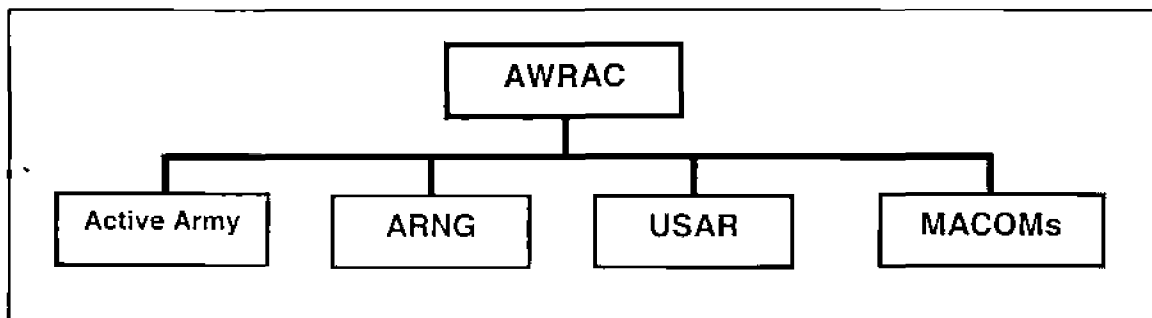


Figure 1: AWRAC Responsibilities

Army Web Risk Assessment Cell Concept Of Operations

4.1 Force Protection

The Army Web Risk Assessment Cell will monitor Army web content for OPSEC exposure of their organization's combat or exercise operations. Analysts will identify information that can be used to gain knowledge relating to:

- Army operations and exercises.
- Personnel and personal information.
- Non-Army proprietary information, or information protected by limited rights statements.
- Test and evaluation information involving competitive contracting or weapon systems.
- Tactical or strategic intelligence capabilities.
- Army deployments for combat operations and exercises.

4.2 Enforcement of OSD-C3I's and Army Website Administrative Guidance

Analysts will engage in random and systematic searches of Army websites for violations of the OSD-C3I Website Administrative Guidance, dated 25 November 1998. Additionally, the AWRAC will ensure that Army websites are in compliance with DA website guidance and policy (see reference).

4.3 Commander Support

The Army Web Risk Assessment Cell will accept tasking from Commanders to perform OPSEC analysis of command unique target information and concepts on an invitational basis.

4.4 Government Information Locator Service (GILS)

Analysts will ensure that all Army websites are registered with GILS in accordance with ODISC4 policy (Memorandum, ODISC4, Subject: Defending the Army's Systems and Networks, dated XX December 2001). Army websites that are not registered with GILS will be instructed to either register or be removed from the Internet.

5. Structure

The Army Web Risk Assessment Cell will consist of two soldier teams composed of Army Reserve (USAR), Army National Guard (ARNG), and/or Regular Army (RA) personnel. Each team will perform the duties defined in the Army Web Risk Assessment Cell Mission Statement.

6. Training

Each USAR, ARNG, and/or RA personnel initially identified to perform duties as a security analyst within the Army Web Risk Assessment Cell will be provided training at

Army Web Risk Assessment Cell Concept Of Operations

the JWRAC located at Headquarters, Defense Information Systems Agency (DISA) in Arlington, VA. Training at the JWRAC will be focused on DoD website analysis and reporting. Each analyst will receive comprehensive training relating to:

- Analysis of content and data resident on publicly accessible DoD websites
- OPSEC analysis of DoD websites
- Policy compliance and quality control of DoD websites
- Content evaluation of DoD websites
- Initial risk assessments
- Trend analysis
- Reporting through components of the Joint Task Force – Computer Network Operations (JTF-CNO), DISA, DoD Communications Emergency Response Team (CERT), the Global Network Operations and Security Center (GNOSC), and other services.
- Verification and accountability

Each analyst will take the expertise and knowledge gained back to his or her unit and apply their skills to develop the Army Web Risk Analysis Cell. A plan for integrating the training received at the JWRAC into the Army Web Risk Assessment Cell will be submitted to the Director, Information Assurance Directorate no less than thirty days after training has been completed.

7. Responsibilities

Army Regulation 380-5 states that all DA commanders who establish publicly accessible websites are responsible for ensuring that the information published on their sites do not compromise national security or place DA personnel at risk. The commander's responsibility extends beyond general public affairs considerations regarding the release of information into the realm of operational security and force protection. Commanders must apply comprehensive risk management procedures to ensure that the considerable mission benefits gained by using the web are carefully balanced against the potential security and privacy risks created by having aggregated DoD information more readily accessible to a worldwide audience than ever before.

It is imperative that all violations discovered on Army websites by the JWRAC be presented to that commander, director, or leader of that organization in a timely manner. The Webmaster of that organization's Website must also be notified.

7.1 OPSEC Checklist for Publicly Accessible Army Websites

The Army Web Risk Assessment Cell will utilize the OPSEC Checklist for Publicly Accessible Army Websites (Appendix D), to perform web risk analysis of Army websites. Each analyst will notify the unit commander and Webmaster, telephonically and/or by email, if violations are discovered. A copy of the checklist will be kept on record at the AWRAC for future reference. The following information will be included in the OPSEC Checklist:

- Name of the person performing the analysis
- Date/time of review
- Organization reviewed
- Point of Contact (Commander's name or representative and date of contact)
- Primary IP address/URL
- Specific details of the violation(s)
- Reference to specific National, DoD, or Army law, directive, memorandum, regulation, or policy relating to the violation

7.2 Website Analysis Database

The AWRAC is required to establish a Website analysis Database to maintain results of Army website analysis. The database will be used to perform trend analysis, contains all Army websites that are listed in the GILS registry. The Website Database will be used to store information on Army websites (.mil) that have been inspected under the AWRAC's duties (section 7.3). Specifically, the database will contain the following information:

- URL of the Army website
- Point of contact for the website
- Electronic copy of the OPSEC Checklist (completed)

The database will serve as a reference point for analysts to compare, record, and store information relating to Army website violations. Additionally, the website database will be used to perform analysis (trend, threat, statistical), reports, and provide lessons learned. Army websites that have not been registered with GILS (section 4.4) will be added to the database and will be monitored for compliance or removal.

7.3 AWRAC Duties

Army Web Risk Assessment Cell Concept Of Operations

The AWRAC is required to conduct website analysis as detailed in section 4 (AWRAC Mission Concept). To accomplish this mission, the AWRAC must react to inspections conducted by the JWRAC, perform scheduled and unscheduled inspections of Army websites, and assist Army units who request support. The AWRAC's primary mission is:

- React to analysis performed by the JWRAC
- Perform monthly Army website analysis
- Conduct random website inspections
- Perform ad hoc taskings by commanders.

7.3.1 Web risk analysis performed by the JWRAC

The JWRAC will provide the AWRAC with the results of web risk analysis conducted on Army websites. AWRAC security analysts will perform the following actions when a JWRAC report is received:

- Access the Army website reported and perform individual analysis (using the security checklist) to verify security violations exist.
- Notify the commander and Webmaster by telephone and/or by email detailing the security violations.
- Provide the Information Assurance Directorate (SAIS-IOA) with complete analysis of the JWRAC and AWRAC reports.
- Perform follow-up analysis of reported Army websites to verify that security violations have been corrected and the site is now compliant with Federal, DoD, and Army website policies.

7.3.2 Monthly AWRAC Analysis

The AWRAC must perform scheduled analysis of Army websites to ensure that those websites are compliant with DoD and DA policies, procedures, and best practices. Security analysts will perform monthly web risk assessments of all known Army websites. Analysts will use the Website Security Checklist while performing the risk assessments and will perform the following tasks:

- Complete the Website Security Checklist (section 7.1)
- Notify the Commander and Webmaster (telephone and/or email)
- Send completed report to Commander, IA Directorate (SAIC-IOA)
- Update Website database

Army Web Risk Assessment Cell Concept Of Operations

- Perform random website inspections (section 7.2.3) to ensure website violations are corrected.

7.3.3 Random Website Inspections

AWRAC analysts will perform random Army website inspections as part of their daily duties and responsibilities. Random website inspections are necessary for the following reasons:

- Perform follow up analysis of websites that have had documented violations in the past.
- Inspect new Army websites listed in GILS that have not been inspected before.
- Search for Army websites that are not listed in GILS.

Analysts will perform all of the tasks outlined in section 7.2.2 (Monthly AWRAC Analysis) and update the Website Database accordingly.

7.3.4 Commander Support

Commanders may request that the AWRAC perform inspections of their websites. This requirement falls outside of the monthly and random inspections and serves as an informal way to assist commanders to ensure that their websites are compliant with OSD-C3I and Army policy. AWRAC analysts will perform the following services when conducting Ad hoc taskings:

- Comprehensive website risk assessment
- Education (provide electronic list of Federal, OSD-C3I, and Army policies, procedures, and instructions relating to website security.
- Recommendations to meet compliance and lower risk
- Provide electronic copy of Website Security Checklist to commander and web administrator

The AWRAC is not required to forward the results of Commander taskings to the IA Directorate but should keep a copy of the Website Security Checklist for future reference.

8. Summary

The effort to protect the valuable information contained on DoD websites can only be successful through cooperation between the AWRAC, JWRAC, and other service and agency risk assessment cells. The information contained within Army websites is every bit as important as protecting the computer systems and networks that they reside on.

Army Web Risk Assessment Cell Concept Of Operations

The AWRAC is the catalyst to ensure that Army websites are compliant with DoD and DA policies, procedures, and best practices.

8. Appendix A: References

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

Memorandum, Office of the Director of Information Systems for Command Control, Communications, and Computers (DISC4), DRAFT, Subject: Defending the Army's Systems and Networks. A Force Protection Issue

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

9. Appendix B: Glossary

CINC Commander-in-Chief

DA Department of the Army

DefenseLINK DefenseLINK is the official web site for the Department of Defense and the starting point for finding U.S. military information online. The mission is to support the overall mission of the Department of Defense by providing official,

Army Web Risk Assessment Cell Concept Of Operations

timely and accurate information about defense policies, organizations, functions and operations. Also, DefenseLINK is the single, unified starting point for finding military information on-line.

DoD	Department of Defense
GILS	Government Information Locator Service. Identifies public information resources throughout the U.S. Federal Government, describes the information available in those resources, and provides assistance in obtaining the information.
OPLAN	Operations Plan
OPORD	Operations Order
OPSEC	Operations Security
OSD-C3I	Office of the Secretary of Defense for Command, Control, Communications and Intelligence
Risk Assessment	The process of identifying program risks within risk areas and critical technical processes, analyzing them for their consequences and probabilities of occurrence, and prioritizing them for handling.
Risk Management	All plans and actions taken to identify, assess, mitigate, and continuously track, control, and document program risks.
URL	Uniform Resource Locators. The method by which documents or data are addressed in the World Wide Web. URLs contain the Internet name of the site, type of service the resource is served by, Internet port number, and the location of the resource in the directory structure of the server.
WWW	World Wide Web

11. Appendix C: OPSEC Checklist for Publicly Accessible Army Websites

Operations Security (OPSEC) Checklist For			
Publicly Accessible Army Websites (v 5.0):			
Name:		Date/Time of Review:	
Organization Reviewed:		Primary IP Address/URL:	
POC:			
Issue/Concern:	Yes	No	Notes/Comments:
Management Controls (Note: 1): 1. Does the Website (WS) contain a clearly defined purpose statement that supports the mission of the DoD Component? 2. Are users of this WS provided with a privacy and security notice prominently			

Army Web Risk Assessment Cell Concept Of Operations

<p>displayed or announced on at least the first page of all major sections of each web information service.</p> <p>3. If applicable does this WS contain a Disclaimer for External Links notice, when a user request any site outside of the official DoD web information service (usually the .mil domain)?</p> <p>4. Is this WS free of commercial sponsorship and advertising?</p> <p>5. Is the WS registered with the Government Information Locator Service?</p>			
<p>DEPSECDEF Guidance (Note 2):</p> <p>1. Operational Information:</p> <p style="padding-left: 40px;">a. Does the WS contain any information indicating plans or lessons learned which would reveal military operations, exercises or vulnerabilities?</p> <p style="padding-left: 40px;">b. Does the WS reference any information that would reveal sensitive movements of military assets or the location of units, installations, or personnel where uncertainty regarding location is an element of the security of a military plan or program?</p> <p>2. Personal Information:</p> <p>Does the WS contain personal information in the following categories about U.S. citizens, DoD employees and military personnel:</p> <ul style="list-style-type: none"> • Social Security Account Numbers? • Dates of Birth? • Home Addresses? • Home Telephone Numbers? 			

Army Web Risk Assessment Cell Concept Of Operations

<ul style="list-style-type: none"> Names, Locations, or any other identifying information about family members of DOD employees or military personnel? <p>3. Technological Data (Note 3):</p> <p>Does the WS contain any technical data such as:</p> <ul style="list-style-type: none"> Weapon Schematics? Weapon System Vulnerabilities? Electronic Wire Diagrams? Frequency Spectrum Data? 			
<p>OPSEC Considerations:</p> <p>“Tip Off Indicators” (Note 4):</p> <p>Does the WS contain relevant information in the following categories that might reveal an organizations plans and intentions?</p> <p>1. Administrative:</p> <ul style="list-style-type: none"> Personnel Travel (personal and official business). Attendance at planning conferences. Commercial support contracts. <p>2. Operations, Plans, and Training:</p> <ul style="list-style-type: none"> Operational orders and plans. Mission specific training. Exercise and simulations activity. Exercise, deployment or training 			

Army Web Risk Assessment Cell Concept Of Operations

<p>schedules.</p> <ul style="list-style-type: none">• Unit relocation/deployment.• Inspection results, findings, deficiencies.• Unit vulnerabilities or weaknesses. <p>3. Communications:</p> <ul style="list-style-type: none">• RF emissions and associated documentation.• Changes in activity or communications patterns.• Use of Internet and/or e-mail by unit personnel (personal or official business).• Availability of secure communications.• Hypertext links with other agencies or units.• Family support plans.• Bulletin board/messages between soldiers and family members. <p>4. Logistics/Maintenance:</p> <ul style="list-style-type: none">• Supply and equipment orders/deliveries.• Transportation plans.• Mapping, imagery and special documentation support.• Maintenance and logistics requirements.• Receipt or installation of special equipment.			
--	--	--	--

Army Web Risk Assessment Cell Concept Of Operations

Key Word Search: Using the following "key words" conduct a search using the search tool. As a result of this search conduct a random screen of any documents found: <ul style="list-style-type: none">• Deployment Schedules• Exercise Plans• Contingency Plans• Training Schedules• Inspection results, findings, deficiencies• Biographies• Family Support Activities• Phone Directories, Lists	14		
--	----	--	--

-NOTES PAGE-

Note 1: Management Controls are contained in the policy published by the Office of the Secretary of Defense, titled: Establishing and Maintaining A Publicly Accessible Department Of Defense Web Information Service, 9 January 1998.

Note 2: These elements were pulled directly from the DEPSECDEF memo, Information Vulnerability and the World Wide Web, dated, 24 Sept 98.

Note 3: Technical data creates a unique challenge to the OPSEC posture of an organization and to National Security as a whole. Certain technical data, when compiled with other unclassified information, may reveal an additional association or relationship that meets the standards for classification under Section 1.8 (e) E.O. 12958.

Note 4: "Tip-off" indicators are pulled directly from AR 530-1, Operations Security (OPSEC) regulation, dated 3 Mar 95. Tip-off indicators highlight information that otherwise might pass unnoticed. These are most significant when they warn an adversary of impending activity. This allows him to pay closer attention and to task additional collection assets.

Army Web Risk Assessment Cell Concept Of Operations

By necessity this list is generic in nature. There are many other indicators possible for the wide range of military operations and activities. While this list is rather large—when placed in the context of a commands ***pre-established*** critical information, this list may then be applied with a greater level of accuracy. This checklist is not a panacea for complete organizational OPSEC program. If an organization has not invested the effort to analyze it's own critical information, then this list may only tend to exacerbate the problem.

Within the context of information assurance, the World Wide Web should not be treated any differently from any other potential vulnerability. Security of information on publicly accessible web sites must be viewed in the context of an organization's overall OPSEC posture.

Army Web Risk Assessment Cell
Standard Operating Procedures
(SOP)

18 October 2006

Version 2.2

**Army Web Risk Assessment Cell
Standard Operating Procedures**

Table of Contents

1. PURPOSE.....	5
2. APPLICABILITY.....	5
2.1 Website Patrolling.....	5
2.2 Website Analysis.....	6
3. Training Requirements.....	6
3.1 Mandatory AWRAC Training.....	6
3.2 Optional AWRAC Training.....	7
4. AWRAC Duties.....	7
4.1 AWRAC.....	7
4.2 AWRAC Teams.....	8
5. Categories of OPSEC Concerns.....	8
5.1 Severity Priorities.....	9
6. Notification Procedures.....	9
6.1 Commander Support	10
6.2 Web Assessment Missioning	11
7. Joint Web Joint Web Discrepancy Tracking System.....	12
Appendix A: References.....	13

**Army Web Risk Assessment Cell
Standard Operating Procedures**

Appendix B: Glossary.....14

Appendix C: Memorandum of Website Findings.....16

Appendix D: AWRAC SOP Acknowledgement Form.....19

**Army Web Risk Assessment Cell
Standard Operating Procedures**

"This initiative represents both a new model and a total force solution for managing operations security in an environment of rapidly changing technology. It is essential that each of the military components and agencies get on board so that we can expedite the implementation of JWRAC and help it fulfill its important mission."

John J. Hamre, Deputy Secretary of Defense

Army Web Risk Assessment Cell Standard Operating Procedures

1. PURPOSE

This Standing Operations Procedure (SOP) identifies the duties and responsibilities for the Army Web Risk Assessment Cell (AWRAC) and its subordinate teams. The mission of the AWRAC is to ensure that publicly accessible, non-restricted, U.S. Army websites and sites maintained by current Army personnel (i.e. Weblogs, Video Logs, and Websites) are compliant with Federal, DoD, and DA website administration policies, procedures, and best practices in accordance with AR 25-1, Army Knowledge Management and Information Technology, and AR 530-1 paragraph 2-21.

2. APPLICABILITY

This SOP applies to Army AWRAC personnel and all attached or assigned AWRAC Teams. All personnel must read and sign the AWRAC SOP Acknowledgment form on the last page to ensure comprehension and compliance with this SOP. The original copy of this form will be held in a training record in the Office of Information Assurance and Compliance (OIA&C).

2.1 Website Patrolling

AWRAC team analysts will perform site-by-site, page-by-page evaluation of Department of the Army (DA) website content. Using a browser, Operations Security (OPSEC) guidance and web crawling software, analysts will visit each assigned website and evaluate the content on the site for:

- a. Inappropriate links to commercial sites, personal sites, and sensitive or classified sites.
- b. Information on Operation Plans (OPLAN) or planning that includes: force readiness, pre-deployment activities, schedules for movement, support requirements, and any element of an OPLAN or Operation Order (OPORD).
- c. Information on current or future Joint, theater, or service major exercises. This will include schedules for force movements or exercise play, locations, support, and transportation requirements.
- d. Information pertaining to weapons technology to include; ranges, number of weapons deployed, locations and units where weapons are stored and/or used, transportation of weapons systems, cost, descriptions and capabilities, vulnerabilities, and instructions for their use, handling, safety, or maintenance.
- e. Information pertaining to non-DoD information relating to competitive contracting or information under limited release restrictions.
- f. Identify information counter-productive to counter terrorism and installation/site security.
- g. Information that poses a risk or harm to DoD personnel and their families.
- h. Documents marked as Sensitive, Classified, or FOUO.

2.2 Website Analysts

DA websites will be continuously monitored using an automated web crawling tool. This tool will identify potential OPSEC issues. The website analysts will then verify whether the information at the URL is an

Army Web Risk Assessment Cell Standard Operating Procedures

OPSEC concern. If the analyst identifies an OPSEC concern the incident will be logged into the Joint Web Discrepancy Tracking System. The analyst will operate with the following objectives:

- a. Identify all information in web content where discussions of sensitive information or current operations are taking place. Evaluate this information for possible OPSEC concern.
- b. Identify web content where personal, personnel data, or OPSEC concerns may be present. Analyze that content for instances of information identifying dependent associations with service members, places of residence and birth, home telephone numbers, dates of birth, and social security numbers (SSN).
- c. Identify all information in web content that is marked for limited or restricted distribution or as For Official Use Only (FOUO), Confidential, Limited Distribution, Secret, and/or Top Secret, Procurement Sensitive, etc.
- d. Receive tasks from the Army Computer Emergency Response Team (CERT) to identify and analyze web content information as it pertains to target concepts.

3. TRAINING REQUIREMENTS

Each team member performing AWRAC duties must hold the minimum of a secret clearance and will be provided training as determined by the AWRAC Team Chief. Training for the AWRAC will be focused on Army website analysis and reporting.

3.1 Mandatory AWRAC Training

- a. **OPSEC 1301 Training (CBT).** Required Prerequisite NONE. 4 hours self-paced, CD-ROM. This course provides students with a basic working knowledge of OPSEC and how it applies to executive branch agencies and departments. It focuses on the history of OPSEC and the OPSEC process as described in NSDD-298. Students have an opportunity to choose scenarios to practice OPSEC in different environments. This training is available by registering at www.iooss.gov.
- b. **Web Security Course (CBT).** Required Prerequisite NONE. 4 hours self-paced, web based or CD-ROM. Throughout this course, students will gain an awareness of Web site security - what is meant by security for the site and the security of material content on that site. In this course students will look at some of the legal issues, visit sites for current policy and guidance in the maintenance of a Web site, become aware of the importance of operational security, as well as client and server side security. Most topics have an interactive introduction to help students focus on the topic material. Throughout the course students will visit external Web sites that provide additional resources. This training is available by registering at <https://iatraining.us.army.mil>.
- c. **Web Content and OPSEC Certification Training (CBT).** The Webmaster training familiarizes students with DOD and Army web policies. This four module training site provides

Army Web Risk Assessment Cell Standard Operating Procedures

guidance and Best Practices that should be followed by Webmasters in order to be in compliance with current regulations. The training focuses on Operations Security (OPSEC) and explains the types of content that is permitted on an official publicly accessible web site and explain identity theft issues that may be associated with posting certain unauthorized material. This training is available at <https://iatraining.us.army.mil>.

- d. **Joint Web Joint Web Discrepancy Tracking System (JWDTS) Training Course.** Required (resident phase) – Prerequisite NONE. 16 hours, local instructor. This is internal training.
- e. **Web Risk Assessment Course OPSE-3500.** Principles of reviewing web pages for OPSEC vulnerabilities are the primary subject of this course. Use of checklists, commercially available software, and government-developed software are addressed as evaluation and review techniques. The course also provides an overview of the nature and use of the internet to give the student an appreciation of why release of information on a web page might represent an unanticipated risk. This training is available at www.iooss.gov.

3.2 Optional AWRAC Training

- a. **OPSEC 2380 Practitioners Course** (resident phase). Prerequisite OPSEC 1301. 36 hours (4.5 days) resident course, site and location of school are site dependent. The course focuses on the skills and knowledge needed by the OPSEC practitioner. Students learn to: apply the systems analysis methodology to their organizations and activities; identify sources of information and support materials for OPSEC practitioners; and conduct an OPSEC analysis of a program, activity or operation. The course includes major modules on the OPSEC survey, the role of the OPSEC officer, and tools useful to OPSEC analysis. The student is afforded the opportunity to apply OPSEC tools and lessons through a variety of practical exercises and case studies. Requires a U.S. SECRET Clearance; however, classes can be taught at the UNCLASSIFIED level with prior coordination. This training is available at www.iooss.gov.
- b. **Web Content Vulnerability Course 1500.** Required (resident phase) – Prerequisite Web Security Course. 16 hours (2 days) resident course, site and location of school is site dependent. This course addresses the vulnerabilities associated with using web pages to provide information to the public and those associated with using the Internet to do open source research. The focus is on content rather than technical security. Requires a U.S. SECRET Clearance; however, classes can be taught at the UNCLASSIFIED level with prior coordination. This training is available at www.iooss.gov.

Additional training may be required by home units.

4. AWRAC Duties

4.1 AWRAC: Is responsible for the year-round monitoring and scanning of official Army websites and privately maintained Army websites and blogs. To accomplish this mission, the process originates from the OIA&C and is disseminated to the AWRAC teams for analysis. The AWRAC's primary mission is:

- a. Identify the Army web presence.
- b. Perform monthly Army website OPSEC analysis and reporting.
- c. Conduct random website inspections.

Army Web Risk Assessment Cell Standard Operating Procedures

- d. Test and review tools and policy.
- e. Manage and assign workloads to AWRAC teams.
- f. Notify and remediate OPSEC concerns.

4.2 AWRAC Teams

AWRAC teams: Will provide AWRAC with the results of web risk analysis conducted on Army websites and privately maintained Army websites and blogs. AWRAC website analysts will perform the following actions when a mission tasker is received:

- a. Assess the Army website reported and perform individual analysis to verify OPSEC concerns exist per Army web policy and guidance.
- b. Prepare a detailed report to the AWRAC outlining the specific OPSEC concerns for all sites reviewed.
- c. Enter all concerns into the Joint Web Discrepancy Tracking System for action.
- d. Provide a WEEKSUM, as applicable, to OIA&C of their team's activities, including both AWRAC and non-AWRAC missions.
- e. Teams will perform a follow-up on all Army websites reported to JWDTs to verify that OPSEC concerns have been corrected.

5. Categories of OPSEC Concerns

The categories in this section are used by analysts to classify an item for notification purposes.

- a. **Classification** – Include FOUO, Secret, Top Secret, NOFORN, Classified, Limited Distribution, and other material with a designated classification.
- b. **Personnel** – This includes any information that could put army personnel or their family at risk. Information concerning family, social security number, date and place of birth, biographical data, phone listings (per Army Web Site Guidance) is considered sensitive and should not be accessible via the web.
- c. **Operations** – Critical information pertaining to military actions- current, contingent, or logistical –or the execution of strategic operational, tactical, service, training, logistical or administrative function. The disclosure of this information would drastically curtail the ability of friendly forces to accomplish their mission. This category includes: OPORDERS, OPLANS, Intel Estimates, etc. It also involves references to place, time, route, or other information that indicates operations or other movement of personnel and equipment.
- d. **Critical Infrastructures** – These systems include: 1) information and communication, 2) physical distribution, 3) energy, 4) information systems, 5) and communication systems. Essentially these infrastructures are so vital that

Army Web Risk Assessment Cell Standard Operating Procedures

their incapacitation or destruction would have a debilitating impact on the defense and national security of the United States.

- e. **Force Protection** – Force protection are those elements that address physical and operational security, countermeasures against terrorists, strategic and tactical planning measures and procedures, vulnerabilities and procedures that minimize damage and restore operations after accidents and attacks. Force protection encompasses any information that could provide adversarial forces with an advantage over friendly units. This category includes all of the following: unit size and strength, weapon system, location, leadership, R & R locations and facilities, etc.

5.1 Severity Priorities

In order to establish the amount of time in which a concern needs to be resolved, the analyst will need to classify an item by the categories above and by the severities listed below.

- a. **Critical** – Critical findings can generally be defined as those where the information in itself or in aggregate is either classified or may have significant operational impact or place personnel, facilities, or systems at risk from attack. Must be resolved in 24-48 hours. (Ex. OPORD, Troop Movement, Maps, Equipment Vulnerabilities)
- b. **Major** – Major findings can be defined as those on which the information in itself or in aggregation is FOR OFFICIAL USE ONLY (FOUO) or that is information which is typically FOUO as defined in Part V of the Web Site Administration Policies and Procedures Guide. Must be resolved in 7 days. (Ex. SSN, Phone Number, Personal Email Address)
- c. **Minor** – Minor findings are all other concerns that do not fall in either of the above 2 categories and are defined as information which may not be posted on official web sites open to public access and are contrary to the web policy guidance. Must be resolved in 30 days. (Ex. Service Member Names, Dates of Birth)

6. Notification Procedures

The AWRAC performs scheduled analysis of Army websites to ensure that those websites are compliant with DoD and DA policies, procedures, and best practices. Website analysts will perform monthly reviews of Army websites. Analysts will use the web crawling software reports to perform the reviews and will then perform the following tasks:

- a. Notify the IAPM and website administrator of the site in question via email about the OPSEC concerns found on their site.
- b. The website analyst will maintain a list of completed items in JWDTS.
- c. The analyst will review the item to ensure the concerns are corrected.

Army Web Risk Assessment Cell Standard Operating Procedures

Web Logs, also known informally as Wild Blogs, and Video Logs are those sites published by publicly acknowledged members of the Army and (on rare occasions) those of their families. The information scanned on these sites is the same as those of the official sites. The notification process is similar, as in the blogger is asked to review his or her site, and make corrections if necessary. If the corrections are not made, then the blogger's chain of command is notified when possible. Some bloggers cannot be identified either by name or unit. All notifications will be done by the AWRAC or designated Team Chiefs.

Most bloggers are cooperative in removing the information. Concerns found are usually of the following nature:

- a. Images showing classified information in the background, or pictures showing the layout of a base in the background.
- b. Information which could provide the enemy with insights, such as the timing and frequency of patrols.
- c. Discussions of TTPs.

On rare occasions, the information on a blogger's site has been found to be racist or so derogatory to the military that a unit has been notified and asked to resolve the issue. AWRAC has no UCMJ powers, and works directly with bloggers when possible to modify or remove information that might cause OPSEC problems. The Public Affairs Officer and JAG are notified before the service member is contacted. The number of unofficial blogs is much smaller than that of official sites, which is reflected in the smaller number of scans conducted monthly.

During a scan, the AWRAC team can only look to see what's publicly posted on the site and available to the world. The team is not authorized to enter any private sections of the site that require "registration" or "affirmation" of some status that would require falsification. Furthermore, the analysts are not authorized to hack into a site to learn who the owner is. Any attempt to contact the ISP to identify the owner of the site has to follow the statutory requirements by using a subpoena, court order or the like (see 18 USC § 2703 and 18 USC § 2704). Under NO circumstances will the AWRAC or Team members try to identify unknown website hosts or bloggers by contacting ISP's.

6.1 Commander Support

Commanders may request that the AWRAC perform inspections of their websites via the scan request form on the Army Knowledge Online (AKO) AWRAC Knowledge Center. This requirement falls outside of the monthly and random inspections and serves as support to commanders by ensuring that their websites are compliant with DoD and Army policy. AWRAC analysts will perform the following services when conducting assigned tasks:

- b. Comprehensive website risk assessment.
- c. Education by providing an electronic list of DoD and Army policies, procedures, and instructions relating to website security.
- d. Provide recommendations to meet compliance and lower risk.

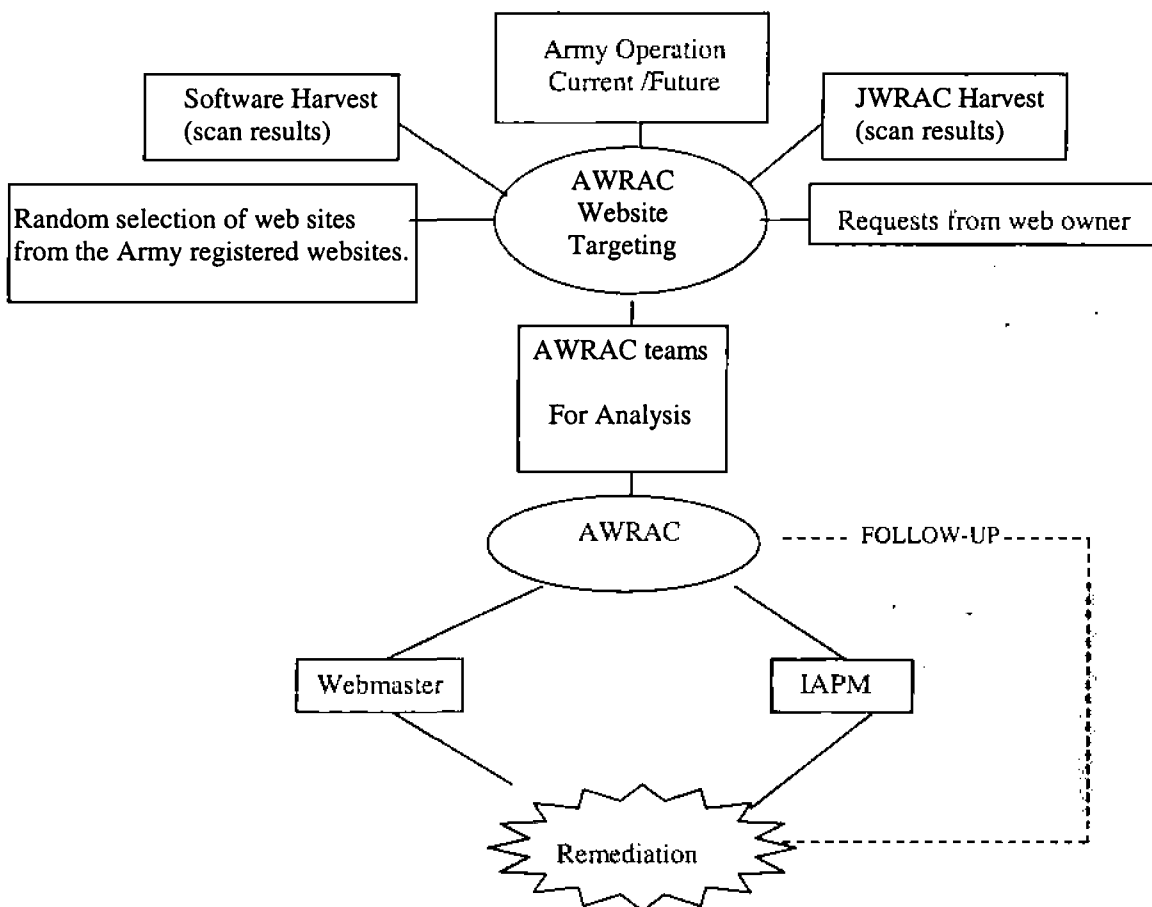
Army Web Risk Assessment Cell Standard Operating Procedures

- e. Provide electronic copy of the Memorandum of Web Risk Assessment Findings to commander, web administrator, or director.

6.2 Web Assessment Missioning

Below is a flow chart displaying how the Army Web Risk Assessment Cell works.

WEB ASSESSMENT MISSIONING



Army Web Risk Assessment Cell Standard Operating Procedures

7. Joint Web Joint Web Discrepancy Tracking System

The JWRAC established the Joint Web Joint Web Discrepancy Tracking System (JWDTS) as a mechanism that adjudicates disagreements between the JWRAC and Web-site owners on potentially inappropriate disclosures at Web sites. The AWRAC will comply with the standard operating procedures of the Joint Web Risk Assessment Cell for discrepancy reporting and tracking, and maintain an up-to-date database of reported concerns on the JWDTS website. Team Chiefs will use this tool to track and maintain an internal log of websites that have not complied with Army policies and procedures, using the Severity Priorities and categories noted in Section 6 above.

Appendix A: References

Army Web Risk Assessment Cell Standard Operating Procedures

DoD Web Site Administration Policies & Procedures (11/25/1998) including all updates (01/11/2002)

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

Memorandum, Office of the Director of Information Systems for Command Control, Communications, and Computers (DISC4), DRAFT, Subject: Defending the Army's Systems and Networks. A Force Protection Issue

Army Regulation (AR) 25-1, 30 JUN 2004, Army Information Management

Army Regulation (AR) 25-2, 14 November 2003 Information Assurance: Management of Subdisciplines

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

Army Regulation (AR) 530-1, 20 August 2005 OPERATIONS SECURITY (OPSEC)

Department of the Army Pamphlet 25-1-1, 20 March 2006 Information Technology Support and Services

Army Web Risk Assessment Cell Standard Operating Procedures

Appendix B: Glossary

AWRAC	Army Web Risk Assessment Cell responsible for command and control for all AWRAC teams and personnel.
AWRAC team	Detachments of the Army Reserve and National Guard assigned to perform the Web Risk Assessment mission acting under AWRAC direction and control.
Blog	An online diary; a personal chronological log of thoughts published on a web page; also called Weblog or Web Log, to include video and photo postings.
DA	Department of the Army
DefenseLINK	DefenseLINK is the official web site for the Department of Defense and the starting point for finding U.S. military information online. The mission is to support the overall mission of the Department of Defense by providing official, timely and accurate information about defense policies, organizations, functions and operations. Also, DefenseLINK is the single, unified starting point for finding military information on-line.
DoD	Department of Defense
IAPM	The Information Assurance Project Manager maintains respective IA programs and serves as commander, director, or activity head's IA representative. The IAPM will be accountable for establishing and assessing the effectiveness of the IA program within that organization.
OPLAN	Operations Plan
OPORD	Operations Order
OPSEC	Operations Security
Risk Assessment	The process of identifying program risks within risk areas and critical technical processes, analyzing them for their consequences and probabilities of occurrence, and prioritizing them for handling.
Risk Management	All plans and actions taken to identify, assess, mitigate, and continuously track, control, and document program risks.
TTP	Tactics, Techniques, and Procedures.
URL	Uniform Resource Locators. The method by which documents or data are addressed in the World Wide Web. URLs contain the Internet name of the site, type of service the resource is served by, Internet port number, and the location of the resource in the directory structure of the server.
WWW	World Wide Web

Army Web Risk Assessment Cell Standard Operating Procedures

Random Website Inspections Inspections conducted where an official site or a blog is selected for review on an individual basis.

**Army Web Risk Assessment Cell
Standard Operating Procedures****Appendix C: Memorandum of Website Findings (SAMPLE)**

NETC-EST-A

S: July 17, 2006

July 17, 2006

MEMORANDUM FOR WEB SITE ACTIVITY COMMANDER/SUPERVISOR

SUBJECT: Web Risk Assessment Findings

1. References:

- a. AR 25-1, Army Knowledge Management and Information Technology Management
- b. DA PAM 25-1-1 Installation Information Services

2. On **DATE**, the Headquarters, Department of the Army, Information Assurance Office (NETC-EST-A) Web Risk Assessment Cell conducted an assessment of -your web site (WWW...). Also evaluated was your required registration with APMS. The following registration and security concerns were noted and rated by category (see below).

CATEGORY	WEB ADDRESS	FINDING	REFERENCE	

Army Web Risk Assessment Cell Standard Operating Procedures

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@hqda.army.mil) and forward the memorandum to the commander/ supervisor, or his/her designated representative, responsible for the website. Suspense dates for corrective actions/resolution of security concerns are provided in the memorandum. Copies of this memorandum will be furnished to the appropriate MACOM, PEO, 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 concerns that do not fall in either of the above two categories. Information, which may not be

**Army Web Risk Assessment Cell
Standard Operating Procedures**

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: **ANALYST'S NAME**, Army Web Risk Assessment Analyst, COM:
ANALYST'S PHONE NUMBER,

Email: **ANALYST'S EMAIL ADDRESS**

"SIGNATURE BLOCK"

COL, GS

Director, Information Assurance

CF: Appropriate MACOM/PEO/PM

**Army Web Risk Assessment Cell
Standard Operating Procedures**

Appendix D: SOP Acknowledgement Form

**Army Web Risk Assessment Cell
SOP Acknowledgement Form**

Version 2.2/ October 2006

1. I acknowledge that I have read and understand the AWRAC Standard Operating Procedures.
2. I acknowledge that the AWRAC mission is to search DoD Websites and internet websites and Blogs for information and trends of data that could be used to breach security or pose a threat to United States Armed Forces' defensive and offensive operations and United States and its allies military personnel.
3. I acknowledge that AWRAC website monitors will perform site-by-site, page-by-page evaluation of Department of the Army (DA) website content looking for inappropriate links to commercial sites, personal sites, and sensitive or classified sites. I acknowledge that I will also perform evaluations that look for inappropriate disclosure of information concerning OPLANS, Service Member Information, and Force Protection, following procedures set forth in the AWRAC SOP.
4. I acknowledge that while reviewing websites, I might find questionable material or material that is deemed inappropriate according to Federal or state law, or Army and/or DoD Computer Usage Guidelines. I understand that I may access inappropriate material only in connection with my official duties, and that I may not access or retain any such information for personal use. The viewing and reporting of this material shall not constitute a concern of prohibitions against accessing or retaining such material as long as the material in question is handled per appropriate Army and DoD regulations.
5. I understand under NO circumstances will the AWRAC or Team members try to identify unknown website hosts or bloggers by contacting ISP's.

Signature of Team Member: _____ Date: _____

Printed Name: _____ Rank: _____

Email: _____ Phone Number: _____

Supervisor Name: _____ Phone Number: _____

FOUO

**Army Web Risk Assessment Cell
Standard Operating Procedures**