

SUBJECT: U.S. Army Information Assurance Program: Army Interim Guidance for Conducting Automated Computer and Network Vulnerability Assessments.

SEE DISTRIBUTION

1. Purpose.

This letter provides policy and guidance for the use of vulnerability assessment tools on U.S. Army networks. A number of Army organizations are considering the utility of purchasing their own copies of various vulnerability assessment tools and conducting their own assessments. This policy addresses concerns and guidelines to be reviewed before conducting computer and network vulnerability assessments. This letter applies to the active Army, the Army National Guard of the United States (ARNGUS), and the United States Army Reserve (USAR). This is an information operations triad (HQDA DISC4, DCSOPS, DCSINT) coordinated letter.

2. Proponent and exception authority.

The proponent of this letter is the Director of Information Systems for Command, Control, Communications, and Computers (DISC4)(SAIS-ZA). The proponent has delegated exception authority to the director of Information Assurance (SAIS-IOA) for all matters pertaining to Army networks security.

3. References.

- a. Army Regulation 380-19: Information Systems Security, 27 Feb 1998.
- b. Army Regulation 25-1: Army Information Management, 15 Feb 2000.

SUBJECT: U.S. Army Information Assurance Program: Army Interim Guidance for Conducting Automated Computer and Network Vulnerability Assessments.

- c. Army Regulation 380-53: Information Systems Security Monitoring, 29 Apr 1998.

4. Explanation of abbreviations.

a.	ACERT	Army CERT
b.	AR	Army Regulation
c.	ARNGUS	Army National Guard of the United States
d.	BPA	Blanket Purchase Agreement
e.	C2	Command and Control
f.	CDAB	Computer Defense Assistance Branch
g.	CDAP	Computer Defense Assistance Program
h.	CERT	Computer Emergency Response Team
i.	CND	Computer Network Defense
j.	COTS	Commercial off the Shelf
k.	DCSINT	Deputy Chief of Staff for Intelligence
l.	DISC4	Director of Information Systems, Command, Control, Communications, and Computers
m.	DITYVAP	Do-It-Yourself Vulnerability Assessment Program
n.	DoD	Department of Defense
o.	IAW	In Accordance With
p.	LIWA	Land Information Warfare Agency
q.	RCERT	Regional CERT
r.	USAR	United States Army Reserve
s.	VAC	Vulnerability Assessment Certification

5. Responsibilities.

a. All Army activities that are testing, evaluating, or have fielded assessment tools must be aware that DISC4 has approved and made available on the BPA selected scanning tools. See <https://www.acert.belvoir.army.mil/tools/csla.htm#network> for current scanning tools available on the BPA. Contact the Land Information Warfare Activity's (LIWA) Army Computer Emergency Response Team (ACERT) for information regarding the availability of shared scanning tool licenses. The LIWA Regional CERTs (RCERT) also provides this support. See the ACERT Computer

SUBJECT: U.S. Army Information Assurance Program: Army Interim Guidance for Conducting Automated Computer and Network Vulnerability Assessments.

Defense Assistance Branch (CDAB) web page at

<https://www.acert.belvoir.army.mil/cdap> for more information.

b. The ACERT CDAB has two approved Army programs for requesting vulnerability assessments, the Computer Defense Assistance Program (CDAP) and the Do-It-Yourself Vulnerability Assessment Program (DITYVAP), and one certification program, the Vulnerability Assessment Certification (VAC). Army units are required to utilize these free Army programs prior to requesting independent support from non-Army or contractor organizations. These programs use ISS Internet Scanner as the DISC4 approved primary assessment tool.

(1) The Computer Defense Assistance Program (CDAP). This program provides full support for remote or onsite assessments, analysis, and penetration testing by the ACERT or servicing RCERT. The CDAP program is currently defined in AR 380-19, Appendix G and AR 380-53, Appendix B.

(2) The Do-It-Yourself Vulnerability Assessment Program (DITYVAP). This program allows an Army unit to use the approved tool to conduct non-penetration assessments on their network(s). Training and full instructions on tool usage is provided by the ACERT-CDAB and the Regional CERTs. See <https://www.acert.belvoir.army.mil/cdap/dityvapsop/dityvapsop.htm> for more information.

SUBJECT: U.S. Army Information Assurance Program: Army Interim Guidance for Conducting Automated Computer and Network Vulnerability Assessments.

(3) The Vulnerability Assessment Certification (VAC) program defines the certification levels and training required to conduct Army vulnerability assessments under the above programs. Personnel not certified to perform scanning or penetration testing are prohibited from doing so on any Army network, system, or device.

(4) Penetration testing by non-Army or contractor organizations must be approved on a case-by-case basis by the DCSINT of the Army. Army personnel must be certified IAW AR 380-53 to conduct penetration testing.

c. All Army supported programs (CDAP, DITYVAP) now require that the raw vulnerability data be provided back to the RCERT (or ACERT) for use in the Army-wide Computer Network Defense (CND) Database. Continued participation in the DITYVAP program requires data to be provided within 10 days of assessment completion. This data is not shared with any organization outside of the ACERT or the requesting unit. Data confidentiality is maintained at all times. Instructions for transferring the data will be provided on the ACERT-CDAB web site referenced in paragraph 5.a above or by contacting the ACERT-CDAP technical representative indicated in paragraph i below.

d. Independent users of the ISS Internet Scanner assessment tool who decide to continue to maintain their own licenses rather than participate in the free Army programs must also provide vulnerability data to the ACERT (see paragraph 6.c.4 below). Users of other tools must participate in one of the Army programs to provide vulnerability data. Loss of critical vulnerability data from independent units could seriously damage the

SUBJECT: U.S. Army Information Assurance Program: Army Interim Guidance for Conducting Automated Computer and Network Vulnerability Assessments.

Army's ability to gauge its security program effectiveness and provide predictive and analytical support.

e. The LIWA ACERT-CDAB and Regional CERTs will provide all the necessary support for full CDAP assessment missions or training and support for DITYVAP requests.

6. Assessment Policy.

a. The vast majority of COTS vulnerability assessment products are not approved by DISC4. This creates a problem with data compatibility and standardization of testing. AR 380-19 paragraph G-1a(2) and G-2a(2) authorizes use of DISC4 approved C2 Protect tools only.

b. Units not currently using ISS Internet Scanner will use one of the approved Army programs for conducting assessments. Current licensees of the product must contact the ACERT-CDAB for instructions on using Army standard scan policies for consistency in testing and data capture, and instructions on providing copies of the raw vulnerability data to the ACERT.

c. In the interim, all Army activities considering conducting their own assessments must adhere to the following guidelines pending the publication of AR 25-IA.

(1) Continue to use currently licensed versions of Internet Scanner or use one of the free Army programs for conducting assessments.

(2) Use of IA/C2 Protect applications/tools, including, but not limited to shareware and freeware, not approved by DISC4 or provided by ACERT-CDAB are prohibited and must be discontinued.

SUBJECT: U.S. Army Information Assurance Program: Army Interim Guidance for Conducting Automated Computer and Network Vulnerability Assessments.

(3) Contact the ACERT-CDAB for instructions on using the Army standard scan policy with Internet Scanner.

(4) Provide a copy of the vulnerability data to the ACERT IAW guidelines on the ACERT-CDAP web page specified above in paragraph 5.a.

(5) Cease all penetration testing activities until certified by the Chief, ACERT IAW paragraph 3-3c and 3-3d(2) of AR 380-53.

(6) Assessment tools designed to specifically view data content or such features available in any authorized tools are prohibited from use by AR 380-19 paragraph G-1a (2) and G-2a (2).

i. DISC4 policy POCs for this letter is: LTC John Quigg, SAIS-IAS, telephone: (703) 604-8377, DSN: 664-8377; e-mail: John.Quigg@HQDA.army.mil or LTC Tom Riddle, DAMO-ODI, telephone (703) 697-1113, e-mail: Thomas.Riddle@hqda-aoc.army.pentagon.mil.

LIWA ACERT technical policy POC for this letter is: Mr. Rick Evans, ACERT-CDAB, telephone: (703) 706-2057, DSN: 235-2057; e-mail: cdap@liwa.belvoir.army.mil

**SUBJECT: U.S. Army Information Assurance Program: Army Interim Guidance
for Conducting Automated Computer and Network Vulnerability
Assessments.**

Distribution:

HQDA (SASA)
HQDA (DACS-ZA)
HQDA (DACS-ZB)
HQDA (SACW)
HQDA (SAFM-AOA)
HQDA (SAILE)
HQDA (SAMR)
HQDA (SARD)
HQDA (SAGC)
HQDA (SAAA-PP)
HQDA (DACS-ZD)
HQDA (SAIS-ZA)
HQDA (SAIG-ZA)
HQDA (SAAG-ZA)
HQDA (SALL)
HQDA (SAPA)
HQDA (SADBU)
HQDA (DAMI-ZA)
HQDA (DALO-ZA)
HQDA (DAMO-ZA)
HQDA (DAPE-ZA)
HQDA (DAEN-ZA)
HQDA (DASG-ZA)
HQDA (NGB-ZA)
HQDA (DAAR-ZA)
HQDA (DAJA-ZA)
HQDA (DACH-ZA)
HQDA (DAIM-ZA)
HQDA (JDIM-RM)

COMMANDER IN CHIEF

U.S. ARMY, EUROPE AND SEVENTH ARMY

COMMANDERS

**EIGHTH U.S. ARMY
U.S. ARMY FORCES COMMAND
U.S. ARMY MATERIEL COMMAND
U.S. ARMY TRAINING AND DOCTRINE COMMAND
U.S. ARMY CORPS OF ENGINEERS**

**SUBJECT: U.S. Army Information Assurance Program: Army Interim Guidance
for Conducting Automated Computer and Network Vulnerability
Assessments.**

U.S. SPECIAL OPERATIONS COMMAND
U.S. ARMY PACIFIC
MILITARY TRAFFIC MANAGEMENT COMMAND
U.S. ARMY CRIMINAL INVESTIGATION COMMAND
U.S. ARMY HEALTH SERVICES COMMAND
U.S. ARMY INTELLIGENCE AND SECURITY COMMAND
U.S. ARMY MILITARY DISTRICT OF WASHINGTON
U.S. ARMY SOUTH
U.S. ARMY RECRUITING COMMAND
U.S. ARMY COMMUNITY AND FAMILY SUPPORT CENTER