Headquarters
United States Army, Europe, and Seventh Army
United States Army Installation Management Agency
Europe Region Office
Heidelberg, Germany

Army in Europe Regulation 380-53*

11 November 2004

Security

Information Systems Security Monitoring

***This regulation supersedes AE Regulation 380-53, 17 December 2002.**

For the CG, USAREUR/7A:

E. PEARSON
Colonel, GS
Deputy Chief of Staff

Official:

GARY C. MILLER
Regional Chief Information
Officer - Europe

Summary. This regulation—

- Prescribes policy for information systems security (ISS) monitoring.
- Provides guidance for requesting ISS monitoring support.
- Prescribes procedures for certifying notification procedures every 2 years.

Summary of Change. This revision—

- Moves some responsibilities from the USAREUR G2 to the USAREUR G3 (para 4).
- Updates office designations throughout.
- Adds critical information list (CIL) to essential elements of friendly information EEFI references.

Applicability. This regulation applies to organizations and activities assigned to or supported by USAREUR or IMA-E.

Supplementation. Organizations will not supplement this regulation without USAREUR G2 (AEAGB-SAD-S) approval.

Forms. AE and higher-level forms are available through the Army in Europe Publishing System (AEPUBS).

Records Management. Records created as a result of processes prescribed by this regulation must be identified, maintained, and disposed of according to AR 25-400-2. Record titles and descriptions are available on the Army Records Information Management System Web site at *https://www.arims.army.mil.*

Suggested Improvements. The proponent of this regulation is the USAREUR G2 (AEAGB-SAD-S, DSN 370-7214). Users may suggest improvements to this regulation by sending DA Form 2028 to the USAREUR G2 (AEAGB-SAD-S), Unit 29351, APO AE 09014-9531.

Distribution. B (AEPUBS).

CONTENTS

Figures

Glossary

---

1. PURPOSE

This regulation prescribes policy for requesting information systems security (ISS) monitoring and assigns responsibilities for the 2-year certification of mandatory notification procedures. This regulation must be used with AR 380-53.

2. REFERENCES

a. Publications.

(1) AR 25-400-2, The Army Records Information Management System (ARIMS).

(2) AR 380-40, Policy for Safeguarding and Controlling Communications Security (COMSEC) Material.

(3) AR 380-53, Information Systems Security Monitoring.

b. Forms.

(1) DD Form 2056, Telephone Monitoring Notification Decal.

(2) DA Form 2028, Recommended Changes to Publications and Blank Forms.

3. EXPLANATION OF ABBREVIATIONS

The glossary defines abbreviations.

4. RESPONSIBILITIES

a. The USAREUR G2 (AEAGB-SAD-S) will—

(1) Ensure notification procedures for ISS monitoring are implemented throughout the European theater according to AR 380-53.

(2) Send the certification request to HQDA no later than 15 July each odd-numbered year.

(3) Ensure personnel conduct ISS monitoring according to AR 380-53.

(4) Ensure the results of ISS monitoring are used for their intended purposes according to AR 380-53.

(5) Ensure monitoring of Government telephone, cell phone, fax, satellite, wireless network, iridium, and information systems is according to AR 380-53.

(6) Prescribe procedures for—

(a) Requesting ISS monitoring.

(b) Certifying that mandatory ISS notification is implemented no later than 15 June each odd-numbered year.

(7) Conduct staff assistance visits throughout the European theater as part of the Army in Europe oversight policy to ensure compliance with AR 380-40 and this regulation.

b. The USAREUR G3 (AEAGC-P-IO) will—

(1) Request authority to conduct ISS monitoring on behalf of commanders, IMA-E, and HQ USAREUR/7A staff principals (d and e below). (Figure 1 is a sample message for requesting ISS monitoring.)

(2) In coordination with the Regional Computer Emergency Response Team, Europe (RCERT-E), identify Computer Defense Assistance Program (CDAP) requirements.

(3) Identify ISS monitoring requirements for the upcoming fiscal year by 1 July each year. ISS monitoring will be conducted according to the following priority order:

(a) Priority 1. Real-world operations, missions, and mission-readiness exercises.

(b) Priority 2. USEUCOM-directed joint task force (JTF) or combined task force (CTF) exercises.

(c) Priority 3. USAREUR participation in other non-USEUCOM-directed JTF or CTF exercises.

(d) Priority 4. USAREUR-only exercises or activities.

(4) Submit technical information applicable to the ISS monitoring requirement ((2) above) to the USAREUR G2 (AEAGB-SAD-S) at least 45 days before the mission is scheduled to start.

(5) Distribute an Army in Europe unclassified and classified critical information list (CIL) according to AR 380-53.

NOTE: CILs are the answers to the essential elements of friendly information (EEFI) questions.

(6) Help commands develop a CIL for specific exercises or deployments.

(7) Receive results of ISS monitoring and direct appropriate action to correct vulnerabilities to Army information systems in the European theater.

(8) Be responsible for assessments of penetration tests of information systems.

c. The 5th Signal Command (NETC-SEC-O) will ensure RCERT-E provides CDAP support when directed by the USAREUR G3.

d. Commanders of organizations assigned to or supported by USAREUR or IMA-E will—

(1) Carry out their ISS responsibilities in their organizations according to AR 380-53.

(2) Establish adequate notification procedures in their organizations according to AR 380-53. (Figure 2 is a sample memorandum for certification of ISS monitoring-notification procedures.)

(3) Ensure mandatory means of notification are posted in their organizations. (Figure 2 prescribes the wording for notification banners in the sample certification memorandum.)

e. IMA-E and HQ USAREUR/7A staff principals will—

(1) Ensure mandatory means of notification are implemented and adhered to in their offices.

(2) Certify in writing to the USAREUR G2 (AEAGB-SAD-S) that adequate notification procedures are established throughout their offices according to AR 380-53 by 15 June each odd-numbered year.

(3) Ensure all personnel (including contractors) are aware of the provisions of AR 380-53.

FM [Enter unit and office symbol]
TO USAREUR G3(sc)
DCS G2(sc), ou=DA ARMY STAFF(sc)
INFO EUCOM J6 Directorate(mc)
ou=EUCOM J62 Information Operations Div(mc)
USAREUR G6(mc)
USAREUR G2(sc)
CDRUSAREUR DCSINT HEIDELBERG GE//AEAGB-SAD-S//
NCEUR VAIHINGEN GE//F262//
DIRNSA FT GEORGE G MEADE MD//C5/AGCI//
[Enter classification]
SUBJECT: REQUEST FOR INFORMATION SYSTEMS SECURITY MONITORING (U)
A. (U) AR 380-53, INFORMATION SYSTEMS SECURITY MONITORING (U), 29 APR 98.
B. (U) MEMO, [enter unit], [enter office symbol], [enter date], SUBJ: BIENNIAL CERTIFICATION TO USAREUR (U).
1. ( ) REQUEST INFORMATION SYSTEM SECURITY (ISS) MONITORING OF [enter type of monitoring required (for example , telephone, cell phone, fax, radio frequency, satellite terminal ID number or hex-decimal, computer, wireless network, iridium)] VOICE/DATA COMMUNICATIONS ORIGINATING AT [enter location] IN SUPPORT OF EXERCISE [enter exercise name or operation] DURING PERIOD OF [enter dates for monitoring].
2. ( ) [Enter next higher command] HAS ESTABLISHED A COMPREHENSIVE ISS MONITORING NOTIFICATION PROGRAM AS PRESCRIBED IN REFERENCE A TO INFORM USERS OF OFFICIAL TELECOMMUNICATIONS SYSTEMS THROUGHOUT THIS COMMAND THAT USE OF THESE SYSTEMS CONSTITUTES USER CONSENT TO ISS MONITORING. (REFERENCE B IS THE CERTIFIED BIENNIAL CERTIFICATION SENT TO USAREUR.)
3. ( ) MONITORING INCLUDES: [Enter the information relevant to the type of monitoring requested from the following: CIL, critical program information, technology systems, telephone numbers, frequencies, satellite terminal identification numbers, and computer Internet Protocol addresses corresponding to the respective telephone and fax, radio, satellite, and computer terminals to be monitored.]
4. ( ) [Enter if needed: The unit may request that a monitoring team conduct an onsite visit before the official monitoring, especially if the monitoring will be in an area of deployment (for example, Bosnia).]
5. ( ) [Enter requesting unit POC information.]

[**NOTE:** Apply classification marking and declassification instructions as required.]

Figure 1. Sample Message for Requesting ISS Monitoring

5. MEANS OF NOTIFICATION

a. Specific means of notification are required to inform users that use of official DOD telecommunications systems constitutes consent to ISS monitoring. Detailed descriptions and requirements for mandatory and optional means of notification are in AR 380-53. Means of notification include the—

(1) Telephone-directory notice.

(2) DD Form 2056 on telephones and fax machines.

(3) Computer log-on banners.

(4) Notices published each quarter (for example, in a unit bulletin, an area support group bulletin, a unit or activity e-mail notice, and the Army in Europe Bulletin).

(5) Initial security briefing to new personnel.

b. USAREUR and IMA-E commanders and staff principals (paras 4d, e, and f) will certify that the mandatory means of notification are in effect and send the certification to the USAREUR G2 (AEAGB-SAD-S), Unit 29351, APO AE 09014-9351, by 15 June each odd-numbered year.

6. HQDA 2-YEAR CERTIFICATION REQUIREMENT

HQDA must approve and give a 2-year certification before ISS monitoring may be conducted. Commanders will implement the mandatory means of notification and certify that notification procedures are established. Failure to execute notification procedures or failure to certify procedures when required can jeopardize the Army in Europe authority to conduct ISS monitoring.

Letterhead

OFFICE SYMBOL DATE

MEMORANDUM FOR USAREUR G2 (AEAGB-SAD-S), Unit 29351, APO AE 09014-9351

SUBJECT: Certification of Information Systems Security Monitoring-Notification Procedures

1. Information systems security (ISS) monitoring procedures prescribed in AR 380-53 are implemented within the [ENTER UNIT] and subordinate commands. These notification procedures ensure all personnel, including contractors, are aware of the provisions of AR 380-53; these notification procedures are deemed adequate to ensure all users of official DOD telecommunications understand that their use of official DOD telecommunications systems constitutes consent to ISS monitoring. A detailed description of implemented notification procedures follows:

a. Telephone or communications directory notices. Official Army telephone and communications directories contain the following notice on the front cover or on the first or second page:

ATTENTION!
DO NOT PROCESS, STORE, OR TRANSMIT CLASSIFIED INFORMATION ON NONSECURE TELECOMMUNICATIONS SYSTEMS. OFFICIAL DOD TELECOMMUNICATIONS SYSTEMS—INCLUDING TELEPHONES, FACSIMILE MACHINES, COMPUTER NETWORKS, AND MODEMS—ARE SUBJECT TO MONITORING FOR TELECOMMUNICATIONS SECURITY PURPOSES AT ALL TIMES. USE OF OFFICIAL DOD TELECOMMUNICATIONS SYSTEMS CONSTITUTES CONSENT TO TELECOMMUNICATIONS SECURITY MONITORING.

b. DD Form 2056 (Telephone Monitoring Notification Decal) has been applied to the front of the following:

(1) Telephones (except tactical).

(2) Secure telephone units (STUs) and secure terminal equipment (STE). The banner at the top of the form that states “DO NOT DISCUSS CLASSIFIED INFORMATION” has been removed or marked out.

(3) Faxing devices, except those that are an integral part of another device.

(4) Secure faxing devices. The banner at the top of the form that states “DO NOT DISCUSS CLASSIFIED INFORMATION” has been removed or marked out.

c. Computer log-on banner notice. All computers attached or accessible through Government-owned or -leased telecommunications networks display the following banner:

ATTENTION!
THIS IS A DOD COMPUTER SYSTEM. BEFORE PROCESSING CLASSIFIED INFORMATION CHECK THE SECURITY ACCREDITATION LEVEL OF THE SYSTEM. DO NOT PROCESS, STORE, OR TRANSMIT INFORMATION CLASSIFIED ABOVE THE ACCREDITATION LEVEL OF THIS SYSTEM. THIS COMPUTER SYSTEM AND ITS RELATED EQUIPMENT, NETWORKS, AND NETWORK DEVICES, INCLUDING INTERNET ACCESS, ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR LAWFUL PURPOSES, INCLUDING TO ENSURE THAT THEIR USE IS AUTHORIZED; FOR MANAGEMENT OF THE SYSTEM TO PROTECT AGAINST UNAUTHORIZED ACCESS; AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY, AND OPERATIONS SECURITY. MONITORING INCLUDES BUT IS NOT LIMITED TO ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED, AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION PLACED ON OR SENT OVER THIS SYSTEM, MAY BE MONITORED. USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING. UNAUTHORIZED USE OF THIS DOD COMPUTER SYSTEM MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL, OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR ALL LAWFUL PURPOSES.

Figure 2. Sample Memorandum for Certification of ISS Monitoring-Notification Procedures

OFFICE SYMBOL
SUBJECT: Certification of Information Systems Security Monitoring-Notification Procedures

d. The following notice is published in unit or command bulletins at least four times a year:

DO NOT PROCESS, STORE, OR TRANSMIT CLASSIFIED INFORMATION ON NONSECURE TELECOMMUNICATIONS SYSTEMS. OFFICIAL DOD TELECOMMUNICATIONS—INCLUDING TELEPHONES, FACSIMILE MACHINES, COMPUTER NETWORKS, AND MODEMS—ARE SUBJECT TO MONITORING FOR TELECOMMUNICATIONS SECURITY PURPOSES AT ALL TIMES. USE OF OFFICIAL DOD TELECOMMUNICATIONS SYSTEMS CONSTITUTES CONSENT TO INFORMATION SYSTEMS SECURITY MONITORING.

e. Periodic notices are also published at least four times a year over command unclassified and classified e-mail and in similar publications and systems as follows:

ATTENTION!
THIS IS A DOD COMPUTER SYSTEM. BEFORE PROCESSING CLASSIFIED INFORMATION, CHECK THE SECURITY ACCREDITATION LEVEL OF THIS SYSTEM. DO NOT PROCESS, STORE, OR TRANSMIT INFORMATION CLASSIFIED ABOVE THE ACCREDITATION LEVEL OF THIS SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS, AND NETWORK DEVICES, INCLUDING INTERNET ACCESS, ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR LAWFUL PURPOSES, INCLUDING TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY, AND OPERATIONAL SECURITY. MONTORING INCLUDES BUT IS NOT LIMITED TO ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED, AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED. USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING. UNAUTHORIZED USE OF THIS DOD COMPUTER SYSTEM MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL, OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR ALL LAWFUL PURPOSES.

f. Initial briefings to all new personnel include informing them that use of authorized telecommunications systems constitutes their consent to ISS monitoring.

g. The following statement may be placed on facsimile coversheets:

ATTENTION!
DO NOT PROCESS, STORE, OR TRANSMIT CLASSIFIED INFORMATION ON UNSECURED TELECOMMUNICATIONS SYSTEMS. OFFICIAL DOD TELECOMMUNICATIONS SYSTEMS, INCLUDING FACSIMILE MACHINES, ARE SUBJECT TO MONITORING FOR INFORMATION SYSTEMS SECURITY MONITORING AT ALL TIMES. USE OF THIS SYSTEM CONSTITUTES CONSENT TO INFORMATION SYSTEM SECURITY MONITORING.

2. The point of contact is [enter name], DSN XXX-XXXX, or e-mail: XXX.XXX@us.army.mil.

JOHN M. SMITH
LTC, SC
Commanding

Figure 2. Sample Memorandum for Certification of ISS Monitoring-Notification Procedures (Continued)

7. REQUESTING ISS MONITORING

The USAREUR G3 (AEAGC-P) will request ISS monitoring from the Joint COMSEC Monitoring Activity (JCMA). The JCMA mission is to monitor joint military encrypted and unencrypted telecommunications systems to determine their vulnerability. The JCMA recommends sensible, cost-effective countermeasures to improve communications security.

GLOSSARY

AE	Army in Europe
AR	Army regulation
CDAP	Computer Defense Assistance Program
CIL	critical information list
COMSEC	communications security
CTF	combined task force
DOD	Department of Defense
EEFI	essential elements of friendly information
HQDA	Headquarters, Department of the Army
HQ USAREUR/7A	Headquarters, United States Army, Europe, and Seventh Army
IMA-E	United States Army Installation Management Agency, Europe Region Office
ISS	information systems security
JCMA	Joint COMSEC Monitoring Activity
JTF	joint task force
RCERT-E	Regional Computer Emergency Response Team, Europe
STE	secure terminal equipment
STU	secure telephone unit
U.S.	United States
USAREUR	United States Army, Europe
USEUCOM	United States European Command