

**Army Regulation 380–53**

**Security**

# **Communications Security Monitoring**

**Rapid Action Revision (RAR) Issue Date: 17 January 2013**

**Headquarters  
Department of the Army  
Washington, DC  
23 December 2011**

**UNCLASSIFIED**

# ***SUMMARY of CHANGE***

AR 380-53

Communications Security Monitoring

This rapid action revision, dated 17 January 2013--

- o Clarifies the military occupational specialties for communications security monitoring and identifies prohibitions (para 2-4h).
- o Provides policy for prohibitions on communications security monitoring missions being conducted by counterintelligence, human intelligence, and law enforcement personnel (with the exception of counterintelligence agents filling technical surveillance countermeasure billets) (para 2-11c).
- o Establishes policy for the Red Team monitoring activities to distribute Red Team reports to the appropriate DOD components (para 3-6).


Security

Communications Security Monitoring

By Order of the Secretary of the Army:

RAYMOND T. ODIERNO  
General, United States Army  
Chief of Staff

Official:

  
JOYCE E. MORROW  
Administrative Assistant to the  
Secretary of the Army

**History.** This publication is a rapid action revision (RAR). This RAR is effective 17 February 2013. The portions affected by this RAR are listed in the summary of change.

**Summary.** This regulation prescribes U.S. Army policy for communications security monitoring. It implements NTISSD 600 and DODI 8560.01.

**Applicability.** This regulation applies to the active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated. During mobilization or

national emergency, chapters and policies contained in this regulation may be modified by the proponent.

**Proponent and exception authority.** The proponent of this regulation is the Deputy Chief of Staff, G–2. The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity’s senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

**Army internal control process.** This regulation contains internal control provisions and identifies key internal controls that must be evaluated (see appendix C).

**Supplementation.** Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Deputy Chief of Staff, G–2 (DAMI–CDS), 1000 Army Pentagon, Washington, DC 20310–1000.

**Suggested improvements.** Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Headquarters, Department of the Army, Deputy Chief of Staff, G–2 (DAMI–CDS), 1000 Army Pentagon, Washington, DC 20310–1000.

**Distribution.** This publication is available in electronic media only and is intended for command levels A, B, C, D, and E for the active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

**Contents** (Listed by paragraph and page number)

**Chapter 1**

**Introduction, page 1**

Purpose • 1–1, page 1

References • 1–2, page 1

Explanation of abbreviations and terms • 1–3, page 1

Responsibilities • 1–4, page 1

**Chapter 2**

**Objectives and Requirements, page 2**

Introduction • 2–1, page 2

Objectives • 2–2, page 3

Authorization to conduct communications security monitoring • 2–3, page 3

Prerequisites • 2–4, page 3

\*This regulation supersedes AR 380–53, dated 29 April 1998. This edition publishes a rapid action revision of AR 380–53.

## **Contents—Continued**

Training and standards for communications security monitoring • 2–5, *page 4*  
Certification of notification procedures • 2–6, *page 5*  
Use of monitoring products • 2–7, *page 5*  
Acquisition of signals during maintenance and testing • 2–8, *page 7*  
Foreign language communications • 2–9, *page 7*  
Conduct of communications security monitoring, information operations Red Team activities, and Computer Defense Assistance Program • 2–10, *page 7*  
Prohibitions on communications security monitoring, information operations Red Team, or penetration testing • 2–11, *page 7*  
Communications security monitoring operations • 2–12, *page 7*  
Communications security monitoring working materials • 2–13, *page 8*  
Communications security monitoring reports • 2–14, *page 9*  
Safeguarding communications security monitoring equipment • 2–15, *page 9*

### **Chapter 3**

#### **Information Operations Red Team, *page 10***

Explanation • 3–1, *page 10*  
Attributes of effective Red Team activities • 3–2, *page 10*  
Authorization to conduct red teaming • 3–3, *page 10*  
Training and standards for Red Team activities • 3–4, *page 10*  
Red Team operations • 3–5, *page 11*  
Red teaming reports • 3–6, *page 12*

### **Chapter 4**

#### **Computer Defense Association Program, *page 12***

Introduction • 4–1, *page 12*  
Objective • 4–2, *page 12*  
Scope • 4–3, *page 13*  
Authorization • 4–4, *page 13*  
Computer Defense Association Program • 4–5, *page 13*  
Computer Defense Association Program network assistance visit • 4–6, *page 14*  
Penetration testing scope • 4–7, *page 15*  
Computer Defense Assistance Program persistent penetration testing • 4–8, *page 15*

### **Chapter 5**

#### **Reporting violations, *page 16***

Oversight • 5–1, *page 16*  
Reporting violations • 5–2, *page 16*

## **Appendixes**

- A.** References, *page 17*
- B.** Forms of Monitoring Notification, *page 20*
- C.** Internal Control Evaluation, *page 20*

## **Figure List**

Figure 4–1: Program organization and structure, *page 15*

## **Glossary**

## Chapter 1 Introduction

### 1–1. Purpose

This regulation sets forth policies, responsibilities, and procedures for conducting communications security (COMSEC) monitoring, information operations (IO) Red Team activities, and Computer Defense Association Program (CDAP) activities within the Army and in support of Joint and combined operations and activities. This regulation implements Department of Defense instruction (DODI) 8560.01 and National Telecommunications and Information Systems Security Directive (NTISSD) 600. The principles of this regulation apply to all forms of COMSEC monitoring conducted by Army elements.

### 1–2. References

Required and related publications and prescribed and referenced forms are listed in appendix A.

### 1–3. Explanation of abbreviations and terms

Abbreviations and special terms used in this regulation are explained in the glossary.

### 1–4. Responsibilities

*a. General Counsel.* The GC will—

(1) Review Department of the Army COMSEC monitoring policy for compliance with public law and national and Department of Defense (DOD) policies and regulations.

(2) Review and certify, in writing, biennially, that COMSEC monitoring notification procedures in effect are adequate throughout the Army.

(3) Review and approve COMSEC monitoring results for court use, in the event such results must be used for criminal prosecution.

(4) Review all requests for proposed COMSEC monitoring exercises, to include requests that are not based on an Army command (ACOM), Army service component command (ASCC), or direct reporting unit (DRU) request for approval (granted by the Deputy Chief of Staff, G–2 (DCS, G–2)).

*b. The Judge Advocate General.* TJAG will review all ACOM, ASCC, and DRU requests to conduct COMSEC monitoring exercises prior to DCS, G–2 approval.

*c. The Inspector General.* TIG will provide oversight of the Army's COMSEC monitoring program to ensure regulatory compliance.

*d. Deputy Chief of Staff, G–2.* As the Secretary of the Army's single designee for COMSEC monitoring, the DCS, G–2 will—

(1) Develop, promulgate, and maintain Army COMSEC monitoring policy.

(2) Grant waivers and exceptions to Army COMSEC monitoring policy after obtaining legal review from the GC and TJAG.

(3) Review and approve biennial requests from ACOMs, ASCCs, and DRUs to perform COMSEC monitoring.

(4) Certify the adequacy of Army COMSEC monitoring notification procedures of other DOD agencies when the Army monitoring elements operate jointly with DOD in support of Joint, combined, or multinational operations.

(5) Represent and defend the Army's interests pertaining to COMSEC monitoring at national and DOD Service meetings and working groups.

(6) Notify ACOM, ASCC, and DRU commanders before authorizing COMSEC monitoring that is not based on an ACOM, ASCC, or DRU request.

*e. Commanding General, U.S. Army Intelligence and Security Command.* The CG, INSCOM will—

(1) Provide Army support to the Joint COMSEC monitoring activity according to the most current Joint COMSEC monitoring activity memorandum of agreement.

(2) Develop and disseminate the Army's techniques for conducting COMSEC monitoring.

(3) Through the commander, 1<sup>st</sup> Information Operations Command (1<sup>st</sup> IO CMD), develop and disseminate for the Army, techniques and procedures for conducting Information System (IS) security penetration and verification testing as it pertains to applicable phases of CDAP (see chap 4).

*f. Commanding General, U.S. Army Training and Doctrine Command.* The CG, TRADOC will—

(1) Develop, produce, and maintain an exportable standardized COMSEC monitoring training package to address the provisions of this regulation.

(2) Coordinate with the CG, INSCOM to incorporate results outlined in paragraphs 1–4e(2) and 1–4e(3) into the standardized training package.

*g. Chief Information Officer/G–6.* The CIO/G–6 maintains overall responsibility and oversight for policy and management of the Army computer emergency response team (ACERT) program. The CIO/G–6 will—

(1) Promulgate rules and procedures in AR 25–1 and AR 25–2, outlining system and network administrators’ responsibilities (vulnerability analysis) to keep the Army’s IS operational and secure.

(2) Develop plans and policies to implement procedural and material protective measures and to validate requirements for protecting Army computers, communications, and command and control.

(3) Act as the Army’s focal point for command and control protect.

*h. Administrative Assistant to the Secretary of the Army.* The AASA (Director of Security Services) will—

(1) Act as the ACOM, ASCC, and DRU head to ensure Secretariat, Army Staff, and field operating agency COMSEC monitoring compliance.

(2) Ensure COMSEC monitoring notification procedures are implemented and upheld (see paras 2–6 and 2–10).

(3) Request authority to conduct COMSEC monitoring (see para 2–3).

(4) Ensure personnel authorized to conduct COMSEC monitoring comply with the provisions of this regulation.

(5) Ensure COMSEC monitoring products are used for their intended security purposes (see para 2–7).

*i. Deputy Chief of Staff, G–3/5/7.* The DCS, G–3/5/7 will—

(1) Act as the Army Staff’s operational focal point for IO.

(2) Exercise operational tasking authority over the 1<sup>st</sup> IO CMD, to include prioritization and validation of requests for 1<sup>st</sup> IO CMD COMSEC monitoring support.

*j. Commanders of Army commands, Army service component commands, and direct reporting units.* The commanders of ACOMs, ASCCs, and DRUs will—

(1) Ensure COMSEC monitoring notification procedures are implemented and upheld (see paras 2–6 and 2–10).

(2) Request authority to conduct COMSEC monitoring (see para 2–3).

(3) Ensure personnel authorized to conduct COMSEC monitoring comply with the provisions of this regulation (see para 2–10).

(4) Ensure COMSEC monitoring products are used for their intended security purposes (see para 2–7).

*k. Commanders at all levels.* The commanders will—

(1) Ensure COMSEC monitoring results are used only for their intended security purposes (see para 2–14).

(2) Ensure a comprehensive and continuing COMSEC monitoring notification program is in effect (see paras 2–6 and 2–7).

(3) Ensure critical information is made available to COMSEC monitoring teams (see AR 530–1).

(4) Provide the necessary facilities and support (including security of COMSEC monitoring equipment and working materials) required by the monitoring element for the conduct of the mission.

## **Chapter 2**

### **Objectives and Requirements**

#### **2–1. Introduction**

*a.* DOD telecommunications systems are provided for official Government communications. When these systems are used by the Army components, they are subject to COMSEC monitoring, IO Red Team activities, and penetration testing as explained in this regulation.

*b.* COMSEC monitoring, IO Red Team activities, and penetration testing will be completed in a manner that satisfies the legitimate needs of the Army. Activities will be conducted to minimize the monitoring (purposely or inadvertently) of telecommunications not related to security objectives and will be performed in a manner that protects to the greatest degree possible the privacy and civil liberties of individuals whose telecommunications are subject to monitoring.

*c.* COMSEC monitoring, IO Red Team activities, and penetration testing are vulnerability assessment techniques that provide essential information not available through other sources for evaluating security within the Army.

*d.* COMSEC monitoring as discussed in this regulation does not pertain to the following:

(1) The interception of wire and oral communications for law enforcement (LE) purposes as described in AR 190–53.

(2) Operations center communications monitoring as described in AR 190–30.

(3) Electronic surveillance as described in AR 381–10.

(4) Technical surveillance countermeasures.

(5) TEMPEST (see glossary, sec II) as described in AR 380–27.

(6) Counterintelligence (CI) investigations.

(7) Radio communications monitoring by net control stations to enforce net discipline.

(8) System and network administrators performing defensive IO functions to keep their own automated IS infrastructure operational and secure. This exemption is limited to performing vulnerability analysis of the operating systems of the IS directly under the control of the system and/or network administrators.

(9) Use of intrusion detection systems on the IS when the intrusion detection system is only used to monitor communications protocols, systems control information, and specific command and control, or words associated with commonly accepted or known penetration techniques.

(10) Research and evaluation development testing of the Army's telecommunications and IS, when such activities are performed in a lab environment using test-generated users or data.

(11) Classification of information as described in AR 380-5.

## **2-2. Objectives**

COMSEC monitoring is undertaken to—

*a.* Collect operational signals needed to measure the degree of security being achieved by encryption, cryptographic equipment and devices, COMSEC techniques, and operations security (OPSEC) countermeasures.

*b.* Provide a basis from which to assess the type and value of information subject to loss through intercept and exploitation of official Government telecommunications.

*c.* Provide an empirical basis for improving the security of Army telecommunications against signals intelligence and other data exploitation.

*d.* Assist in determining the effectiveness of electronic attack; electronic protect, cover, and deception actions; electronic warfare support; and OPSEC measures.

*e.* Identify Army telecommunications signals that exhibit unique external signal parameters, signal structures, modulation schemes, radio fingerprints, and so forth that could provide adversaries the capability to identify specific targets for subsequent ge positioning and exploitation purposes.

*f.* Provide empirical data to properly train users of Army telecommunications systems on COMSEC techniques and measures.

*g.* Evaluate the effectiveness of Army COMSEC education and training programs.

*h.* Support defensive IO by identifying, verifying, and evaluating Army telecommunications and IS to exploit, degrade, or neutralize susceptibilities attempts.

## **2-3. Authorization to conduct communications security monitoring**

COMSEC monitoring operations may be performed under the provisions of this regulation at the commander's discretion throughout the 2-year approval cycle, provided the GC has certified adequacy of the command's notification procedures and the DCS, G-2 has granted the command the authority to conduct the monitoring (see para 2-6a(1)).

## **2-4. Prerequisites**

The following must occur before COMSEC monitoring, IO Red Team activities, and penetration testing can take place:

*a.* Users of official DOD telecommunications will be given notice that—

(1) Passing classified information over nonsecure DOD telecommunications systems (other than protected distribution systems or automated information systems accredited for processing classified information) is prohibited.

(2) Official DOD telecommunications systems are subject to monitoring at all times.

(3) Use of official DOD telecommunications systems constitutes consent by the user to monitoring at any time.

*b.* The GC has certified the adequacy of the notification procedures in effect, and the GC and TJAG have given favorable legal review of any proposed COMSEC monitoring that is not based on an ACOM, ASCC, or DRU request.

*c.* The DCS, G-2 has authorized monitoring to be conducted within the ACOM, ASCC, or DRU involved.

*d.* Monitoring telecommunications systems of U.S. Government contractors at their own facilities require the express written approval of the chief executive officer or designee of the company. Requests for such monitoring will include a statement from the chief executive officer or designee outlining the notification procedures that have been implemented within the contractor's organization to afford notice to the contractor's employees (see para 2-4a). Such requests will be forwarded through command channels to the DCS, G-2 (DAMI-CDS) for action. The DCS, G-2 (DAMI-CDS) will obtain a legal review from TJAG and GC prior to taking any action. Requests must arrive at the DCS, G-2 a minimum of 45 days prior to the date the monitoring is desired. The contractor's chief executive officer's approval is not required to monitor contractors who are performing duties in U.S. Government-controlled facilities.

*e.* Monitoring will not be conducted by Army personnel (Soldiers, civilians, or contractors employed by the Army) on the telecommunications of another DOD component without the express written approval of the head (or designee) of that department or agency, unless the other DOD component is conducting the monitoring and Army personnel are serving only in a subordinate role.

*f.* One ACOM, ASCC, or DRU will not monitor the telecommunications or conduct IS penetration testing of another ACOM, ASCC, or DRU without the consent of that ACOM, ASCC, or DRU. The exception to this restriction is when the activity is directed by the DCS, G-2.

g. Special attention will be provided to ensure monitoring operations avoid or filter out communications containing privileged doctor-patient, lawyer-client, and chaplain-petitioner information.

h. Army COMSEC monitoring operations may be conducted by the following personnel (see para 2-11c for prohibitions):

- (1) Properly trained and certified personnel.
  - (2) COMSEC monitoring personnel who possess the following military occupational specialties (MOS):
    - (a) Enlisted Soldiers in career management field 35.
    - (b) Warrant officers in MOS 350 or MOS 352.
    - (c) Commissioned officers in career management field 35.
    - (d) Personnel who have held MOS 05G or MOS 97G.
  - (3) Civilian intelligence specialists (IA-0132) (except those assigned to CI, HUMINT, or law enforcement duties) and security specialists (IA-0080).
  - (4) Contractors whose statement of work specifically addresses COMSEC monitoring.
- i. All personnel conducting the Army COMSEC monitoring operations will acquire and maintain a security clearance based on a single scope background investigation.

## **2-5. Training and standards for communications security monitoring**

COMSEC monitoring and related activities will be conducted in strict compliance with this regulation. Each individual involved in the conduct (collection and analysis) of COMSEC monitoring will receive formal training before participating in monitoring or penetration operations. All personnel will be knowledgeable and able to implement the provisions set forth in the following paragraphs, as instructed by a senior COMSEC certified person.

- a. At a minimum, personnel will be trained on the following:
  - (1) The provisions of this regulation, with particular emphasis on chapter 2.
  - (2) The provisions of AR 381-10.
  - (3) The provisions of AR 381-12.
- b. Formal training requirements to conduct monitoring operations may be fulfilled through either of the following:
  - (1) Completion of a DOD COMSEC monitoring course.
  - (2) Completion of an internal command training program using approved TRADOC course materials. The execution of command training programs will be approved by the DCS, G-2 (DAMI-CDS).
- c. For monitoring operations, the first lieutenant colonel (O-5) or civilian equivalent (GS-14) in the individual's chain of command will certify, in writing, the individual has been trained. A copy of this certification will be maintained on file at the monitoring unit, available for inspection by any inspector general (IG), oversight officer, or command inspector. Copies of these certifications will be provided to the DCS, G-2 (DAMI-CDS) upon request.
- d. When required, trained COMSEC monitoring mission supervisors may augment the COMSEC monitoring team's efforts with nontrained technical resources, provided—
  - (1) The mission supervisor informs all nontrained personnel on the restrictions applied to COMSEC monitoring operations.
  - (2) All nontrained personnel work directly under a trained COMSEC monitoring supervisor.
  - (3) The use of nontrained personnel is approved on a case-by-case basis by the ACOM, ASCC, or DRU commander.
- e. Personnel participating in COMSEC monitoring will annually receive unit-level refresher training.
- f. All personnel will cooperate fully with the Army and DOD GCs, intelligence oversight officers, and IGs, and will allow them access to all information necessary to perform their oversight responsibilities.
- g. COMSEC monitoring equipment training will use signals that are subject to COMSEC monitoring, whenever possible. When those signals are not available, training in the use of COMSEC monitoring equipment may be conducted using those signals identified in paragraph 2-8a. When those signals identified in paragraph 2-8a are used to conduct COMSEC monitoring training, the following restrictions apply:
  - (1) The signal acquisition will be limited in extent and duration necessary to train personnel in the use of the equipment.
  - (2) No particular U.S. person's communications will be targeted without the specific written consent of that person.
  - (3) The content of the telecommunications will be—
    - (a) Retained only when actually needed for training purposes.
    - (b) Disseminated only to persons conducting or participating in the training, except as provided in paragraph 2-7.
    - (c) Destroyed immediately upon completion of the training.
- h. Waivers to the provisions of paragraph 2-5 will be granted on an individual basis by the DCS, G-2 (DAMI-CDS).



## 2-6. Certification of notification procedures

ACOM, ASCC, and DRU commanders will implement procedures to ensure all personnel are aware of the provisions of this regulation. Commanders must verify that their notification procedures are adequate.

### a. Certification.

(1) The ACOM, ASCC, and DRU commanders will submit requests for certification to Headquarters, Department of the Army, DCS, G-2 (DAMI-CDS), 1000 Army Pentagon, Washington, DC 20310-1000. Requests will arrive no later than 15 July of each odd-numbered year. Approval periods will run from 1 October (of each odd-numbered year) or date of certification by the GC (whichever is later) through 30 September (of the next odd-numbered year) to correspond with the fiscal year. Requests will include a detailed description of the notification procedures within the ACOM, ASCC, or DRU including the following:

- (a) The exact wording of the warning notice on telephone directories.
  - (b) The exact wording of the banner notice on IS.
  - (c) The exact wording of the notice published quarterly in command bulletins, on command email (unclassified and classified), and similar publications and systems.
  - (d) A statement that DD Form 2056 (Telephone Monitoring Notification Decal) has been applied to all telephones and facsimile machines.
  - (e) A statement that command inprocessing includes a briefing that informs personnel that use of official telecommunications systems constitutes consent to monitoring.
  - (f) The identification of any other notification procedures used.
- (2) The DCS, G-2 (DAMI-CDS) will review all requests to verify the presence of required information. The requests will be consolidated and forwarded to the GC for legal certification.
- (3) Upon certification by the GC, the DCS, G-2 (DAMI-CDS) will grant approval for the ACOM, ASCC, or DRU to conduct COMSEC monitoring.

### b. Forms of notification.

#### (1) Mandatory forms of notification.

(a) *Telephone or communications directory notice.* Official Army telephone or communications directories, if published, will display the appropriate notice on the front cover or prominently within the general information section (see app B-1).

#### (b) DD Form 2056.

1. The DD Form 2056 will be applied to the front of all telephones (except tactical, cellular telephones, and portable electronic devices) within the Army.

2. The DD Form 2056 will also be applied to the front of all secure telephone equipment, and so forth; however, the banner at the top of the form containing the words "DO NOT DISCUSS CLASSIFIED INFORMATION" will be removed or obliterated.

3. The DD Form 2056 will be applied to the front of all data facsimile devices except those that are an internal part of another device (for example, a facsimile card in a personal computer). The DD Form 2056 will also be applied to the front of all secure data facsimile devices, but the words "DO NOT DISCUSS CLASSIFIED INFORMATION" will be removed.

(c) *Computer logon, banner notice.* See AR 25-2 for specific policy on the banner.

(d) *Periodic notices.* Periodic notices will be published at least quarterly in command bulletins (see wording in app B-1) via command unclassified and classified email and in similar publications and systems.

#### (2) Optional forms of notification.

Optional forms of notification include the following:

- (a) Periodic briefings and training classes for all assigned personnel.
- (b) Special memorandums from the commander or responsible senior staff officer to all personnel.
- (c) Local notification and consent procedures.
- (d) Statements in standing operating procedures, signal operation instructions, and similar publications or documents.
- (e) The statement in appendix B-2 may be placed on facsimile cover sheets.

(3) *Waiver of mandatory forms of notification.* Requests for waivers to the mandatory forms of notification will be forwarded to the DCS, G-2 (DAMI-CDS) for action.

## 2-7. Use of monitoring products

Communications security monitoring, IO Red Team activities, and CDAP products will be used only in pursuit of security objectives, except that—

a. Information obtained either by COMSEC monitoring, IO Red Team activities, or CDAP may be used in connection with disciplinary or administrative action against Army personnel for knowing, willful, or negligent actions that result in the unauthorized disclosure of classified information (see AR 380-5). In this case, the COMSEC monitoring, IO Red Team, or CDAP element is authorized to release names and recorded media regarding the

telecommunications involved to the supported commander or designated representative for use as evidence. Procedures will be strictly adhered to as follows:

(1) The supported commander, after having consulted with the servicing judge advocate, will provide the COMSEC monitoring, IO Red Team, or CDAP element with a written request, specifically identifying the telecommunications messages or communications required. The request will identify the servicing judge advocate consulted.

(2) The COMSEC monitoring, IO Red Team, or CDAP element will obtain a signed receipt from the supported commander or designated representative for the requested materials. The receipt will include a statement that the commander or representative is familiar with, and will comply with, the security requirements and privacy restrictions applicable to the material.

(3) The COMSEC monitoring, IO Red Team, or CDAP unit commander will notify the DCS, G-2 (DAMI-CDS), in writing, within 5 working days of providing the material to the supported command.

*b.* Information may be obtained incidental to an authorized COMSEC monitoring, IO Red Team activity, or CDAP mission that relates directly to a serious crime such as sabotage or threats or plans to commit offenses that threaten a life or could cause significant damage to or loss of official U.S. Government property (this includes data on official U.S. Government IS). This information will be reported immediately by the senior member of the COMSEC monitoring, IO Red Team, or CDAP team element present when the information is discovered.

(1) The commander of the COMSEC monitoring, IO Red Team, or CDAP element releasing the recorded media containing suspected criminal activity will notify the DCS, G-2 (DAMI-CDS), in writing, of the circumstances within 24 hours of release of the material. The DCS, G-2 (DAMI-CDS) will subsequently notify the GC. Notification will include the following:

- (a) Nature of the suspected offense.
- (b) Identification of the material released.
- (c) Date, time, and location where information was obtained.
- (d) Anticipated action resulting from disclosure of the information.
- (e) Location, name, and telephone number of the responsible individual where the materials are being held.

*Note.* Names or other data sufficient to identify any individuals who participated in the monitored communication will not be included in the report.

(2) When evaluating or assessing the security of Army IS, the COMSEC monitoring, IO Red Team, or CDAP element may detect computer anomalies that could potentially be unauthorized intrusions into and from Army IS. When COMSEC monitoring, IO Red Team, or CDAP elements detect such anomalies, they must contact the systems administrator and/or information assurance security officer, or information assurance manager and regional computer emergency response team (RCERT) immediately. If the RCERT is not available then the systems administrator and/or network administrator, and/or information assurance security officer will contact the ACERT directly. In addition, report per local supervisory reporting policies in effect. The system administrator and/or RCERT will then follow the procedures of AR 25-2 for incident and intrusion reporting by taking measures to ascertain whether the anomaly is in fact an unauthorized intrusion, and by notifying CI and the criminal investigation division so that those organizations may conduct an investigation of the incident. The COMSEC monitoring, IO Red Team, or CDAP elements will not investigate and must discontinue monitoring the suspected intrusion as soon as the system administrator or RCERT is notified.

*c.* Whenever any information is officially reported to the commander under paragraphs 2-7a and 2-7b, above—

(1) Stop all COMSEC monitoring, IO Red Team activities, or CDAP testing of the frequency, circuit, network, node, and/or individual device (unless under the exception of para 2-7b(2)) over which the information was obtained. Monitoring will not resume until—

- (a) All actions by the commander or LE agency related to the incident have been completed.
- (b) The party involved in the incident no longer has access to the circuit, frequency, or network.
- (c) The commander has authorized resumption of the mission.

(2) The COMSEC monitoring, IO Red Team, or CDAP element team leader will immediately identify, mark as working papers, classify at a minimum of “Confidential,” segregate, hold in suspense, and protect all recording media pertaining to the incident. If these materials are required for evidence, the following procedures will be used:

(a) The investigating commander or LE agency will request the recorded media, in writing, after having consulted with the local servicing judge advocate.

(b) COMSEC monitoring, IO Red Team, or CDAP element leader will obtain a signed receipt from the supported commander or designated representative for the requested materials. The receipt will include a statement that the commander or representative is familiar with, and will comply with, security requirements and privacy restrictions.

(c) The requesting agency will be informed that the recorded media will be returned to the monitoring element for final disposition when the materials are no longer required as evidence.

(3) The results of COMSEC monitoring, IO Red Team, or CDAP may not be used in a criminal prosecution without prior consultation with the GC and TJAG.

## **2-8. Acquisition of signals during maintenance and testing**

Maintenance and calibration of COMSEC monitoring equipment may require the acquisition of signals by maintenance personnel.

*a.* The following signals may be used without restriction:

- (1) Laboratory-generated signals.
- (2) Communications signals with the consent of all parties involved.
- (3) Commercial and public service broadcasts.
- (4) Noncommunication signals such as beacons, telemetry, and radar.

*b.* Requests to use signals other than those listed above will be forwarded to the DCS, G-2 (DAMI-CDS) for action.

## **2-9. Foreign language communications**

*a.* Translation of foreign language conversations, messages, or data files that are recorded on official U.S. Government-owned or U.S. Government-leased telecommunication systems under the authority of this regulation is authorized.

*b.* Such communications may be translated by—

- (1) A U.S. person with an appropriate U.S. security clearance.
- (2) A foreign national employee of the U.S. Armed Forces with a limited access authorization for this purpose (see AR 380-67).

*c.* Translation must be done under the direct supervision of COMSEC monitoring personnel. Recordings and other working materials, including translations, will not be released outside the monitoring element, except as provided in paragraph 2-7 of this regulation. Transcripts will be treated as COMSEC monitoring working materials.

## **2-10. Conduct of communications security monitoring, information operations Red Team activities, and Computer Defense Assistance Program**

*a.* COMSEC monitoring, IO Red Team activities, and CDAP may be conducted only for certified ACOMs, ASCCs, or DRUs that have notification procedures in place and approved by the GC, and when authorized by the DCS, G-2.

*b.* COMSEC monitoring, IO Red Team activities, and CDAP will be conducted only in support of security objectives. COMSEC monitoring, IO Red Team activities, and CDAP will not be performed to support LE, criminal, or CI investigations.

*c.* COMSEC monitoring, IO Red Team activities, and CDAP will be conducted in—

- (1) The least-intrusive manner possible.
- (2) A way that minimizes the monitoring of communications not relevant to security objectives.
- (3) A manner that ensures maximum privacy consistent with monitoring objectives.

*d.* COMSEC monitoring, IO Red Team activities, and CDAP conducted by Army elements in support of Joint or combined operations and activities will be conducted in accordance with Joint or combined COMSEC monitoring and information assurance procedures, as long as those procedures have been reviewed and approved by the appropriate legal counsel.

## **2-11. Prohibitions on communications security monitoring, information operations Red Team, or penetration testing**

*a.* COMSEC monitoring, IO Red Team, or CDAP activities, or the products of such activities, will not be used to enforce DOD policy limiting the use of official DOD telecommunications systems to the conduct of official business.

*b.* The results of COMSEC monitoring, IO Red Team, or CDAP activities will not be used to produce foreign intelligence or CI, as defined in executive order 12333 (EO 12333).

*c.* CI agents (with the exception of CI agents filling technical surveillance countermeasures billets), HUMINT, and LE personnel are prohibited from performing or participating in COMSEC monitoring, but may engage in IO Red Team or CDAP activities.

## **2-12. Communications security monitoring operations**

COMSEC monitoring operations include monitoring and/or recording telecommunications as well as the analysis of the material obtained.

*a.* COMSEC monitoring will be limited to official DOD telecommunications systems that are owned or leased by the U.S. Government for use by DOD personnel or the military departments.

*b.* Communications conducted over DOD telecommunications systems are assumed to be official communications subject to monitoring. However, recorded telecommunications will not be retained for a period greater than 30 days or disseminated if telecommunications have no relation to COMSEC monitoring objectives (except related to a crime) (see paras 2-2 and 2-7b).

*c.* COMSEC monitoring of wire line telephone systems will be conducted by bridging telephone lines before the point of connection between the DOD lines and the outside lines, as done at the main distribution frame. DOD

telecommunications may not be monitored when combined, multiplexed, or otherwise mixed with non-DOD telecommunications in such a way that monitoring of the non-DOD telecommunications is likely.

*d.* COMSEC monitoring of radio transmissions (other than those associated with cellular telephone systems) such as single channel voice radio, microwave, or similar means, will be limited to circuits dedicated only to DOD use and to transmissions that are sent and received by transmitting and receiving facilities dedicated to DOD use. No incidentally acquired non-DOD communication will be further monitored when it is determined that it is a non-DOD communication. A record of the inadvertently acquired information may be kept for signal identification and avoidance purposes; the record may describe the signal parameters (frequency, modulation, type, and timing) but will not identify the parties to the communication or contain any portion of the communication content between the parties.

*e.* COMSEC monitoring of trunked circuits (in which communication devices share the same frequency, but are divided into channels at a central control point) must be conducted on those circuits exclusive to the requesting ACOM, ASCC, or DRU. If units other than the requesting unit are using the trunked radio system, the commander(s) of the other using unit(s) must grant permission, in writing, for the COMSEC monitoring on the trunked circuits. The written permission(s) will be attached to the initial request.

*f.* COMSEC monitoring of other signals such as wireless computer networking devices, wireless voice over internet protocol, personal area network devices (“hands-free”), wireless peripheral devices, will be limited to circuits dedicated only to DOD use and to transmissions that are sent and received by transmitting and receiving facilities dedicated to DOD use.

*g.* COMSEC monitoring of cellular telephone systems will employ signal collection equipment that incorporates special design features that allow for the targeting of specific command cellular telephone numbers. The equipment will be programmed by the user to activate only on calls made to and from command-owned or command-leased cellular telephones. At no time will cellular telephone transmissions be monitored or collected using techniques that do not allow for filtering of non-DA or non-DOD cellular phone signals.

*h.* COMSEC monitoring of IS (for example, email and data transfer) will employ monitoring technologies designed to intercept network subscribers’ incoming and outgoing messages or data. COMSEC monitoring will only be conducted on a network that originates or terminates on a DOD-owned or DOD-leased telecommunication. COMSEC monitoring of networks will not be performed with the intent to identify, track, or locate unauthorized users.

*i.* Procedures for conducting automated information systems penetration testing will be developed and disseminated by 1<sup>st</sup> IO CMD. This may include, but is not limited to, the following:

(1) Use of a wardialer or similar device to determine the presence of telephonic carrier devices connected to land line telephones being used by the monitored unit. COMSEC monitoring will be performed only on those telephone numbers positively identified as belonging to the unit being monitored. No other telephone numbers will be retained for any purpose.

(2) A wardialer is defined as software or hardware designed to dial a specified set of telephone numbers to determine the presence of telephonic carrier devices. These devices include, but are not limited to, modems and facsimile machines.

(3) Placing a network security monitor on the unit’s network to perform searches of data traversing the system. Key word searches may be used as an analysis and time management tool. Selected key words may include standard terms associated with the identification of classified information and words directly relating to the supported unit’s critical information list or other mission objectives.

(4) Keystroke-capturing software or devices will only be used on the host computer. No keystroke capturing software or device will allow for remote access by outside computers.

*j.* Telecommunications selected for analysis will not be routinely transcribed, except as provided for in paragraph 2–7. When transcripts are made, they will not be included in interim or final COMSEC monitoring reports. Transcripts of communications (except those discussed in para 2–7) will be prepared and distributed as follows:

(1) If the supported commander’s review of interim or final reports indicates that a knowing, willful, or negligent disclosure of classified information may have occurred, the commander or designee may request and be provided with transcripts of the telecommunications. Initial transcripts will not include the names of participants in the conversations or other information that would identify the participants, except in an official capacity.

(2) The data (for example, recordings, disks, or printouts) may be provided as specified in paragraph 2–7.

*k.* Telecommunication data not related to the monitoring mission that are present on recordings will not be transcribed or otherwise annotated unless needed to support actions described in paragraph 2–7 and will be handled in accordance with paragraph 2–7 of this regulation.

### **2–13. Communications security monitoring working materials**

*a.* Routine access to COMSEC monitoring working materials such as operator logs, operator or analyst notes, and recordings will be limited to those personnel specifically approved under paragraph 2–4. Working materials will not be released except as provided in paragraph 2–7. Working materials will be stored and maintained in a manner to ensure that the access restrictions are maintained in accordance with paragraph 2–14.

(1) COMSEC monitoring working materials will be controlled as working papers under the provisions of AR 380–5.

A minimum classification of CONFIDENTIAL (or the classification of the information identified) will be assigned for all COMSEC working materials. The material in question will then be coordinated with the supported command and the appropriate classification determined.

(2) All recording media will be marked with the highest classification of material recorded and will retain this classification until degaussed, purged, or destroyed.

b. COMSEC monitoring working materials will be purged, destroyed or degaussed 30 calendar days after the final report is issued. An extension of up to 30 days may be granted in writing by the ACOM, ASCC, or DRU commander having operational control over the COMSEC monitoring element. Any extension beyond that must be submitted to the DCS, G-2 (DAMI-CDS).

c. All written COMSEC monitoring working materials produced in the course of monitoring and analysis operations will be reviewed within 60 working days of the date produced to ensure that any information not pertinent to the monitoring mission is deleted. These written materials will be annotated with the name of the person conducting the review and the date the review was conducted.

d. Access to COMSEC monitoring working materials may be granted to commanders and other personnel exercising direct management authority over the COMSEC monitoring element if—

(1) Such access is for the purpose of supervising, directing, and checking the efficiency, regulatory compliance, and mission effectiveness of COMSEC monitoring personnel.

(2) All personnel concerned are advised of the limitations on the release of information derived from COMSEC monitoring (see para 2-7).

e. When COMSEC monitoring is conducted as part of an OPSEC survey or other vulnerability assessment, results obtained from the monitoring may be shared with other elements of the team to ensure that a fully integrated and comprehensive assessment or survey is made.

f. Working materials will be reviewed to ensure they are devoid of data extraneous to COMSEC monitoring objectives before the materials are released outside of the COMSEC monitoring element.

## **2-14. Communications security monitoring reports**

The composition, format, and frequency of submission of COMSEC monitoring reports will be determined by the supported command after coordination with the team lead of the monitoring element. Interim reports may be requested on a daily or weekly basis. A final comprehensive mission report will be submitted to the command. Suspense and distribution of final reports will be determined through coordination with the supported command.

a. COMSEC monitoring reports will contain information only on the monitoring mission, the adequacy of security procedures within the command monitored, and recommended countermeasures.

(1) Report title pages and headers and footers of all pages of reports will prominently state, "COMSEC MONITORING INFORMATION. CONFIDENTIAL (AR 380-53)."

(2) All reports, logs, and materials produced in the course of COMSEC monitoring will be afforded protection commensurate with the classification of the information and the sensitivity of the monitored activity. Reports or materials produced from COMSEC monitoring which identify security weaknesses of the monitored activity will be classified at least "CONFIDENTIAL" and downgraded to "UNCLASSIFIED" when security weaknesses are corrected (see NTISSD 600).

(3) Descriptions or gists of information disclosed that are necessary to understand the nature of any weakness may be included in the final report.

(4) Reports submitted under paragraph 2-7 are not considered COMSEC monitoring reports in the context of this paragraph.

(5) When COMSEC monitoring is conducted as part of a vulnerability assessment effort, OPSEC survey, or other security support, a separate report of the results of the monitoring need not be prepared. Any report produced from COMSEC monitoring material must be marked and prepared according to this regulation.

b. Reports and information acquired through COMSEC monitoring will not be disseminated outside the Army, except—

(1) In support of mutual OPSEC objectives and the goals of other military Services, Joint commands, and DOD agencies. This includes the exchange of technical information and reports (including working materials) within COMSEC monitoring channels.

(2) When required by a court order and approved by the DOD GC.

(3) For counterintelligence, LE, or criminal purposes (see para 2-7).

## **2-15. Safeguarding communications security monitoring equipment**

Equipment designed specifically for COMSEC monitoring will be safeguarded to prevent unauthorized use. Required safeguards are as follows:

a. Equipment installed in facilities or installations for COMSEC monitoring operations must be safeguarded by any of the following methods:

- (1) Lock and key.
  - (2) Internal logon/logout security software.
  - (3) Removal of a component that renders the equipment inoperative.
- b.* Records will be maintained by each monitoring element that possesses equipment designed specifically for COMSEC monitoring. These records will include the following:
- (1) An inventory of the equipment on hand.
  - (2) Location of each item in use.
  - (3) Names of persons in charge of each item of equipment in use.
- c.* Only those personnel assigned to COMSEC monitoring and/or maintenance duties will have access to COMSEC monitoring equipment in use.

## **Chapter 3**

### **Information Operations Red Team**

The procedures in this chapter apply to IO Red Team activities on official DOD information systems within the Army.

#### **3–1. Explanation**

An IO Red Team is an independent, threat-based, simulated opposition force that uses passive, active, technical, and nontechnical capabilities on a formal, time-bounded basis to expose and identify the vulnerabilities of friendly forces from an IO threat perspective. Red Team operations expose an organization's vulnerabilities and challenge its readiness by focusing on the identification of critical and classified information.

#### **3–2. Attributes of effective Red Team activities**

For Red Team activities to most effectively challenge and assess an organization's IS, the following conditions must be established:

- a. Independence.* Effective Red Team activities require that the Red Team act independently from the target organization for the duration of the assessment.
- b. Rules of engagement.* A defined rules of engagement (ROE) (support agreement and charter) must be developed and signed prior to all Red Team assessments. The ROE must be signed by the Red Team lead and approved by the proper level of authority for the target organization through the use of a trusted agent (as defined in para 3–5*b*). The ROE must address the adversary threat level (as defined in para 3–5*a*) to be portrayed by the Red Team.

#### **3–3. Authorization to conduct red teaming**

Individual Red Team members must be Army penetration test certified and IO Red Team certified. Red Teams must be National Security Agency or United States Strategic Command certified. Certified Red Team members are only authorized to conduct Red Team activities as part of a certified Red Team sanctioned mission.

- a. Certification time period.* Organizations may conduct Red Team activities for 3 years or until certification expires, whichever is sooner.
- b. Certification authority.* The National Security Agency is the certification authority for all DOD Red Team activities.
- c. Certification eligibility.* Army organizations seeking Red Team certification must have the capability to perform full spectrum Red Team vulnerability assessments. Full spectrum refers to the ability to portray an adversary from the perspectives of the 5 pillars of IO: operations security, electronic warfare, military deception, computer network operations, and psychological operations.
- d. Threat computer network operations teams.* Threat computer network operations teams are authorized to conduct threat simulation in support of the Army and DOD acquisition testing certification process under the authority of the DCS, G–2 (DAMI–FIT). Authority is granted to employ threat testing techniques and procedures over open networks in support of Army acquisition, logistics, and technology test events. Computer network scans and attacks are authorized and may be employed to infiltrate, expose, and identify vulnerabilities of systems.

#### **3–4. Training and standards for Red Team activities**

Red Team activities and related activities will be conducted in strict compliance with this regulation.

- a. Knowledge of regulations, laws, and other guidance.* In addition to team certification, each individual involved in the conduct of Red Team activities will receive formal training prior to participating in Red Team operations. At a minimum, personnel will be trained on the following:
  - (1) The provisions of this regulation.
  - (2) AR 25–2.
  - (3) AR 25–55.
  - (4) AR 340–21.

- (5) AR 381–10.
- (6) EO 12333.
- (7) DODD 3600.01.
- (8) Section 2511, Title 18, United States Code (18 USC 2511).
- (9) Omnibus Crime & Safe Street Act of 1968.
- (10) Public Law 100–235 (PL 100–235).
- (11) PL 104–106.
- (12) PL 107–347.

*b. Training certifications.* For Red Team operations, the first lieutenant colonel (O–5) or civilian equivalent (GS–14) in the individual’s chain of command will verify in writing the individual has been trained in accordance with the provisions of paragraphs 3–3 and 3–4a of this regulation. A copy of this certification will be maintained on file at the unit, available for inspection by any IG, oversight officer, or command inspector. Individual certification is valid for 3 years or until the certified individual is no longer involved in Red Team activities, whichever is sooner. Individual certification is held separate from unit certification and has no effect thereon.

*c. Nontrained personnel.* When required, Red Team mission supervisors may augment the Red Team efforts with nontrained personnel, provided all nontrained personnel work under the direct supervision of trained and certified Red Team personnel.

*d. Refresher training.* Personnel participating in Red Team activities will receive annual unit-level refresher training and are required to renew individual certification every 3 years.

*e. Violation reporting.* Any information gathered as “data-at-rest” (DAR) or “data-in-motion” will be processed in accordance with paragraph 2–7b of this regulation.

*f. Access for oversight.* All Red Team personnel will cooperate fully with the Army and DOD GCs, intelligence oversight officers, and IGs in performing their necessary oversight responsibilities.

### **3–5. Red Team operations**

Red Team operations expose vulnerabilities by challenging an organization’s readiness and ability to protect information. Red Team activities focus on identifying an organization’s critical and classified information to show the operational impact of physical, information and operations security shortcomings.

*a. Threat-level replication.* Red Team threat levels are categorized into 3 tiers.

(1) *Tier 1: “Script Kiddy.”* Tier 1 adversaries are individuals who use tools that are publicly available. Tier 1 adversaries may not have a thorough understanding of the principles behind their actions, but are familiar enough with a tool to take hostile actions against a target.

(2) *Tier 2: “Hacker for Hire.”* Tier 2 adversaries are funded organizations with the capability of developing custom tools to use in conjunction with tools that are publicly available. Tier 2 adversaries have a deep understanding of the principles behind their actions and pose a serious threat to their target’s information.

(3) *Tier 3: “Nation State.”* Tier 3 adversary is a government or organization with state sponsorship whose purpose is to gather information on foreign nations and adversely impact their operations.

*b. Trusted agents.* A trusted agent is a member of the target organization who is knowledgeable of the operation and is responsible for assisting the Red Team in coordinating all requirements for the assessment. Trusted agents are required to keep the knowledge of Red Team operations restricted to only personnel read in on the operation. Additional persons may be made aware of Red Team operations after discussion with an authorization by the Red Team lead. The trusted agent is also responsible for deconflicting real world activities from Red Team activities during the assessment. All trusted agents must sign a trusted agent confidentiality agreement form, agreeing to the aforementioned responsibilities prior to being briefed on any Red Team operation.

*c. Information targeting.* The ROE established prior to the assessment will determine the parameters for Red Team activities. A target or targets will be established between the Red Team leader and trusted agent as part of the planning phase of the assessment. The Red Team will use several support systems, each having a distinct methodology, to gather information guarded by the target and assess vulnerabilities in the target’s established defense mechanisms. Red Team methods may include, but are not limited to the following:

(1) *Close access.* Consists of testing target tactics, techniques, and procedures in the areas related to OPSEC and physical security in close proximity. Examples of methods used are “dumpster diving,” physical penetration of facilities, social engineering and/or elicitation, passive observation and/or monitoring, photography, and creation, and use of, false credentials.

(2) *Computer exploitation.* Employment of information assurance readiness testing (under DODI 8560.01, E2.9) and Red Team techniques consistent with computer network attacks to ensure adequate protection of critical and classified information. Methods include penetration testing, exploitation, reverse engineering, electronic reconnaissance, data analysis, privilege escalation, establishing a foothold through back doors, key loggers, Trojans, and Phishing. Red Team activities include monitoring data-in-motion and mining DAR.

(3) *Wireless communications or networking.* Wireless communications or networking comprises employment of

wireless network discovery and techniques consistent with information assurance and/or computer network defense (CND) to ensure adequate protection of critical and classified information is provided via the wireless spectrum. This includes the interception and exploitation of wireless communication signals.

*d. Additional constraints.* All vulnerabilities introduced into an organization's IS will be removed prior to the end of the assessment to prevent an adversary from exploiting the assessed organization.

*e. Minimum deconfliction.* To ensure that organizational resources are not diverted or distracted from handling real world issues in response to Red Team activities, the following deconfliction will be conducted.

(1) When conducting operations that include activities on the LandWarNet (LWN), Red Teams will coordinate and deconflict with the ACERT and U.S. Army Cyber Command. Additionally, Red Teams will gain authority from ACERT. These organizations will be provided source Internet protocol addresses; target Internet protocol addresses; point of contact names; and contact information so that network defenders can differentiate between authorized Red Team activities and real world threat activity.

(2) When conducting operations that may be reported as criminal acts or espionage on military installations, Red Teams will coordinate with the local provost marshal offices, CI detachments, criminal investigation divisions, and directorate of emergency services. Deconfliction is not necessary if these organizations are subject to the assessment; however, the Red Team will establish a trusted agent within each.

*f. Network operations.* To replicate a true adversary, certified Red Teams have the authority to access .mil networks from public domains through the use of remote operations. Remote operations refer to the transmission of traffic across multiple domains or subdomains from origin to destination.

### **3–6. Red teaming reports**

Red Team vulnerability assessment reports consist of the analysis of all key vulnerabilities found and recommendations for risk reduction control measures.

*a.* When conducting cyber security inspections or Red Team operations, Red Team findings will be released as follows:

(1) An out-briefing and coordinated final report will be provided to the inspected or Red Team targeted organization.

(2) Copies of the final report will be provided to the following:

*(a)* Combatant command for the subordinate combatant command organization and Service component.

*(b)* Service or agency for the subordinate Service or agency organization.

*(c)* U.S. Strategic Command; Defense Information Systems Agency (for Defense Information Systems Network-connected IS); National Security Agency; Defense Threat Reduction Agency; and Office of the Director, Operation, Test and Evaluation within the Office of the Secretary of Defense following coordination with combatant command for assessed subordinate combatant command organization and Service component or Service or agency for assessed subordinate Service or agency organization, as applicable.

*b.* Report results for cyber security inspections or Red Team operations on contractor and other non-DOD ISs will be provided to: the authorizing official (designated approval authority); the sponsoring combatant commands, Services, defense agencies; DOD field activities; Joint activities; U.S. Strategic Command; Defense Information Systems Agency (Connection Approval Office); and Defense Security Service (for classified contractor facilities). Sponsors will share the results with the respective contract management organization (if applicable) and the sponsor's supporting information assurance management organization.

*c.* The final Red Team vulnerability assessment report should be submitted within 30 days of the completion of the Red Team operation, unless directed otherwise by the requesting unit.

## **Chapter 4 Computer Defense Association Program**

### **4–1. Introduction**

The CDAP provides technical support for mitigating identified vulnerabilities to the following:

*a.* Requesting individual units and activities.

*b.* The DCS, G–3/5/7 or CND service providers.

### **4–2. Objective**

*a.* Evaluate the CND posture and CND response actions of the Army LWN resources by testing and attempting to circumvent Army networks by emulating the methods of hostile actors. Identified deficiencies will be evaluated to determine the depth and degree of potential compromise to provide the appropriate assistance in securing the LWN. This may include, but is not limited to, recommending modifications of methods, techniques and configuration modifications; training of users and system administrators, and/or providing subject matter experts to assist. The CDAP



teams evaluate installations and leverage lessons learned to improve local organizations' abilities and influence CND operations across the Army.

b. The major objectives are to—

(1) Confirm and demonstrate methods of intrusion and compromise that could be accomplished by unauthorized users.

(2) Confirm and demonstrate the depth and degree of intrusion.

(3) Assess the network's ability to detect and respond to intrusions.

(4) Evaluate non-user data files such as system-level files, user identification, and login/logoff scripts. User data files (including email) will not be examined, read, modified, recorded, or deleted as part of the penetration testing effort.

#### **4-3. Scope**

The CDAP is executed to protect and defend all unclassified and classified information systems used to plan, direct, coordinate, control, and support Army forces operating on the Army LWN for active Army, U.S. Army Reserve, and Army National Guard.

#### **4-4. Authorization**

a. CDAP missions are conducted in accordance with this regulation, AR 25-2, Chairman of the Joint Chiefs of Staff Instruction 6510.01F, and are authorized by the service provider, consent and COMSEC exceptions to Electronic Communications Privacy Act (18 USC 2511(2)(a)(i), 18 USC 2511(2)(c), and 18 USC 107(b)(1) of PL 99-508, Section 107 (b)(1)), as well as PL 100-235, and as amended by PL 104-106.

b. Headquarters, Department of the Army Computer Network Operations Standing EO 096-08 authorizes 1<sup>st</sup> IO CMD to conduct persistent penetration testing (PPT).

#### **4-5. Computer Defense Association Program**

a. A program executed to evaluate the CND posture of Army LWN IS used to plan, direct, coordinate, control, and support Army forces (active Army and Reserve Components) across the full spectrum of conflict. Identified deficiencies (vulnerabilities) will be assessed to determine the depth and degree of potential compromise to provide the appropriate assistance in securing the LWN. This may include, but is not limited to, recommending modification of methods, techniques and configurations; and training of users and system administrators. CDAP missions can be requested by the unit commander or the designated approving authority. CDAP missions can also be directed by the DCS, G-3/5/7 or CND service provider. The CDAP consists of multiple mission types based on requirements with recognition to the growing complexity of computer network operations and the ability to counter threat forces that are determined to undermine and compromise network operations. RCERTs, by using uniform procedures and required metrics, provide the computer Warfighters a consistent and uniform view of the network security posture. Required topics of the mission metrics are defined in the CDAP methodology.

b. The CDAP consists of 3 mission types—

(1) *Network assistance visit.* A mission responding to an organization's request that a team of subject matter experts test and evaluate the CND posture of their network and network devices, and provide assistance to improve the organization's security posture. The goal is to prevent unauthorized access by emulating the methods of hostile entities to assess the target network. A network assistance visit (NAV) consists of the following phases:

(a) Phase 1: Pre-coordination, ROE, and in brief.

(b) Phase 2: Network survey, technical support, custom training and assistance, and organizational repairs.

(c) Phase 3: Penetration testing and verification.

(d) Phase 4: Executive summary, outbrief, and final report (on compact disk within 30 to 60 days).

(2) *Network damage assessment.* The goal of a network damage assessment (NDA) is to validate suspected compromises and identify the depth of intrusions to gain knowledge for use in mitigation, recovery, and future prevention of possible compromises. NDAs are detailed examinations of installations initiated after a suspected or confirmed network compromise. NDAs are collaborative missions conducted by Network Enterprise Technology Command, 1<sup>st</sup> IO CMD, RCERTs, computer crime investigative units, the garrison commander, and the regional director, or any particular vendor associated with the systems being affected. The final report will be classified as required by findings and intended for general distribution and use by CND professionals.

(3) *Persistent penetration testing.* DCS, G-3/5/7 or 1<sup>st</sup> IO CMD directed missions (authorized by EO 096-08, dated 25 Jan 08) for execution of tactical overwatch operations and network surveillance of the LWN (and networked devices connected to the LWN) to conduct open network testing that can be launched from any location and at anytime. PPT missions are based on mission triggers (for example, sensor data, intelligence, and signal spillage or beaconing signals from an IS) that can be performed on a 24 hours a day/7 days a week basis to include, but not limited to, identifying the signal and shutting down the source; verifying network deficiencies by identifying potential weaknesses and circumventing the defensive posture to gain access onto the network; and recommending mitigating actions.

c. CDAP missions are conducted by RCERTs that dispatch mission support teams comprised of subject matter experts and select units operating under 1<sup>st</sup> IO CMD memorandum of agreement.

d. All IS contact with the target network may be from outside the target network as deemed appropriate by the CDAP team and in accordance with ROEs and regulations. Other methods such as Phishing, Web site hijacking, pretexting, and so forth, may also be used.

e. During the penetration testing phase, the requesting unit or activity must explicitly give consent to the application of techniques and procedures specified in the ROE (unless the mission has been directed by the DCS, G-3/5/7, in which case, consent is not required).

f. The CDAP team will cease activity if an unauthorized intrusion is detected during any phase of the program. The CDAP team will follow established procedures for notifying the unit and protecting the affected network. The CDAP team's efforts on the affected network will not continue until authorization is received by the ACERT and/or the RCERT.

g. The CDAP team does not have the authority to investigate criminal or foreign intelligence service involvement.

h. Only personnel with a current top secret security clearance will conduct the network penetration testing.

i. Network penetration testing and PPT is conducted by Army certified penetration testing technicians.

j. All CDAP team members will be trained and certified in accordance with the requirements of this regulation, AR 25-2, and 1<sup>st</sup> IO CMD CDAP methodology.

k. When conducting support in accordance with paragraph 2-10 of this regulation, records of all penetration testing (type, time, and duration) against Army IS will be maintained as required for statistical purposes.

#### **4-6. Computer Defense Association Program network assistance visit**

a. When preparing for a CDAP NAV, the following procedures will be adhered to:

(1) The ACERT and/or RCERTs will organize and manage the NAV team, as directed by the program manager under the authorization of the commander, 1<sup>st</sup> IO CMD.

(2) The CDAP manager or designee will—

(a) Coordinate with the requesting unit's or activity's designated point of contact to obtain mission overview and necessary requirements.

(b) Ensure training, certification, and qualification of all team members.

(3) The requesting unit or activity will—

(a) Be responsible for all information systems within the target network (unless directed by the DCS, G-3/5/7 or the CIO/G-6).

(b) Request support via memo (available at ACERT home page <https://www.acert.1stiocmd.army.mil/index.jsp>), signed by the commander or chief of staff (unless directed by the DCS, G-3/5/7 or the CIO/G-6).

(c) Appoint a point of contact to work all requests, requirements, and issues.

b. The following program organization and structure will be adhered to (see fig 4-1):

(1) *Phase 1 – Request/authorization.* Provides authorization and information about the target IS network and establishes the “operating and mission parameters” or ROE. The CDAP team provides a pre-brief to unit commander and support staff on details of each phase, expected outcomes, schedule, and limitations.

(2) *Phase 2 – Network survey.* Obtains information about the design and implementation of the target network and discovers (scans for) information about devices on the network and its possible weaknesses. This information is used to compare differences between design and implementation and evaluates the network's susceptibility to intrusion.

(3) *Phase 3 – Network penetration testing.* This phase examines the degree and depth of information compromise which could be obtained by potential intruders; evaluates the ability of the targeted network to detect the presence of an intruder; and acts as threat “actors” attempting to circumvent the targeted networks defenses by several means—

(a) *Wireless communication.* Wireless networking, cellular communication detection, personal area network device paging and other such portable electronic devices.

(b) *Social engineering (for example, Phishing, Web site hijacking, pretexting, and so forth) defense.* The CDAP Team will provide verification of suspected vulnerabilities, analysis of network protection capabilities, to include user awareness, and technical support to assist in remediation procedures. All findings and activities will be documented.

(4) *Phase 4 – Final Report.* The requesting unit or activity will receive an executive summary outlining impacts and recommendations for securing the target network. The full report will provide detailed information on impacts, risk assessments, and recommended fixes to secure the target network or subnet. This report is sensitive and dissemination of the information will be controlled by 1<sup>st</sup> IO CMD.

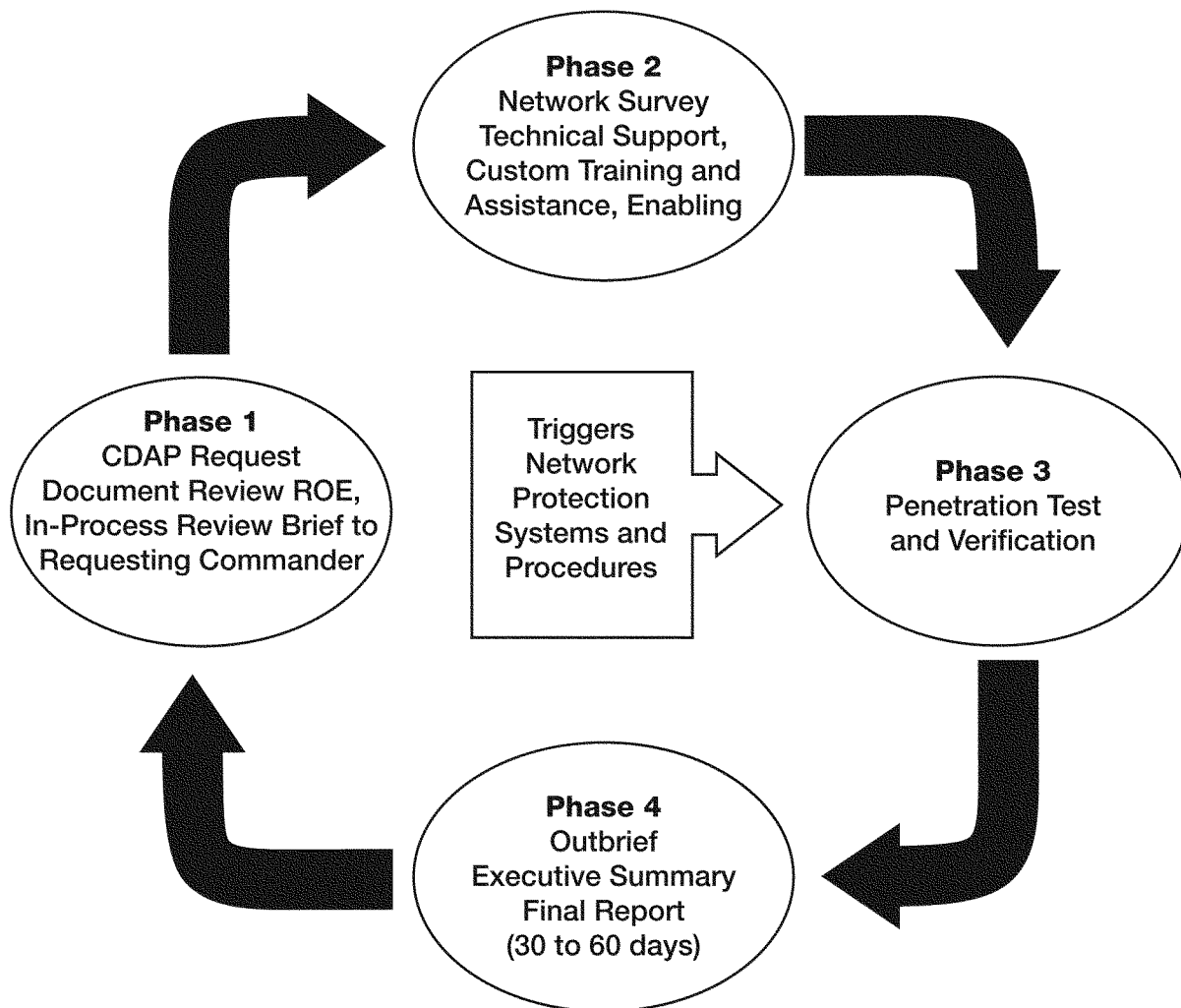


Figure 4-1. Program organization and structure

#### 4-7. Penetration testing scope

Security testing, as defined by Committee on National Security Systems Instruction (CNSSI) 4009, in which evaluators attempt to circumvent the security features of an IS based on their understanding of the system design and implementation. Its purpose is to confirm and demonstrate through penetration testing techniques and procedures the degree of IS defensive postures, vulnerabilities, and mitigating processes.

#### 4-8. Computer Defense Assistance Program persistent penetration testing

The execution of tactical overwatch operations and network surveillance of Army networks and networked devices connected to the LWN that may be performed on a 24 hours a day/7 days a week basis.

a. The PPT is a command-directed or mission-triggered (for example, sensor data, intelligence, spillage, or beaconing signals from an IS) activity.

b. The persistent presence force consists of subject matter experts that are certified penetration testing technicians drawn from 1<sup>st</sup> IO CMD (Detachment-B and RCERTs). They conduct testing of the LWN and they can be launched from any location at anytime for example—

- (1) Identify spillage or beaconing signals from an IS.
- (2) Track the signal and shut down the source.

- (3) Verify network deficiencies by identifying potential weaknesses.
  - (4) Circumvent those weaknesses.
  - (5) Recommend mitigating actions
- c.* A unit's or activity's explicit consent to monitor during PPT is not required in accordance with AR 25-2.

## **Chapter 5**

### **Reporting violations**

#### **5-1. Oversight**

All activities, materials, and records covered in this regulation are subject to IG, intelligence, and security oversight inspections at any time.

#### **5-2. Reporting violations**

Individuals who discover a violation of the activities described in this regulation will promptly report the violation to the unit commander, IG, intelligence oversight officer, or the command security manager.

*a.* The commander, IG, or intelligence oversight officer will ensure that a competent inquiry or investigation into the reported violation is conducted. They will ensure that the circumstances of the violation are reported within 5 working days, through command channels to the DCS, G-2 (DAMI-CDS), with information copies to GC and TIG. Reports will contain the following:

- (1) Nature of the violation (for example, unauthorized monitoring).
- (2) Dates and times of the incident.
- (3) Location (name of installation or activity) where the incident occurred.
- (4) Individuals (last name, first name, middle initial) involved in the incident.
- (5) Brief summary of the incident.
- (6) Corrective actions taken.
- (7) Current status of the inquiry.

*b.* Questionable activity and information relating to violations of Federal law as addressed in AR 381-10 will be reported under the provisions of AR 381-10.

*c.* The DCS, G-2 (DAMI-CDS); GC; TJAG; and TIG will work together to ensure appropriate action is taken to correct the violation and to prevent future occurrences of the same violation.

*d.* Within 5 working days of discovery of the incident, the GC, in coordination with TIG, will send a copy of the initial report and the proposed corrective actions to the Assistant Secretary of Defense for Networks and Information Integration.

## **Appendix A References**

### **Section I Required Publications**

#### **AR 25-2**

Information Assurance (Cited in paras 1-4g(1), 2-6b(1)(c), 2-7b(2), 3-4a(2), 4-4b, 4-5j, and 4-8c.)

#### **AR 25-55**

The Department of the Army Freedom of Information Act Program (Cited in para 3-4a(3).)

#### **AR 25-400-2**

The Army Records Information Management System (ARIMS) (Cited in para C-4d.)

#### **AR 190-30**

Military Police Investigations (Cited in para 2-1d(2).)

#### **AR 190-53**

Interception of Wire and Oral Communications for Law Enforcement Purposes (Cited in para 2-1d(1).)

#### **AR 340-21**

The Army Privacy Program (Cited in para 3-4a(4).)

#### **AR 380-5**

Department of the Army Information Security Program (Cited in paras 2-1d(11), 2-7a, and 2-13a(1).)

#### **AR 380-27**

Control of Compromising Emanations (FOUO)( (Cited in para 2-1d(5).)

#### **AR 380-67**

The Department of the Army Personnel Security Program (Cited in para 2-9b(2).)

#### **AR 381-10**

U.S. Army Intelligence Activities (Cited in paras 2-1d(3), 2-5a(2), 3-4a(5), and 5-2b.)

#### **AR 381-12**

Threat Awareness and Reporting Program (Cited in para 2-5a(3).)

#### **AR 530-1**

Operations Security (OPSEC) (Cited in para 1-4k(3).)

#### **DODI 8560.01**

Communications Security (COMSEC) Monitoring and Information Assurance (IA) Readiness Testing (Cited in paras 1-1, 3-5c(2).) (Available at [http://www.dtic.mil/whs/directives/.](http://www.dtic.mil/whs/directives/))

#### **NTISSD 600**

Communications Security (COMSEC) Monitoring (Cited in paras 1-1, 2-14a(2).) (Available at [http://www.cnss.gov/.](http://www.cnss.gov/))

### **Section II Related Publications**

A related publication is a source of additional information. The user does not have to read it to understand this regulation.

#### **AR 25-1**

Army Knowledge Management and Information Technology

#### **AR 381-14**

Technical Counterintelligence (TCI) (U)

**AR 381–20**

(S/NF) The U.S. Army Counterintelligence Program (U)

**AR 381–143**

Nonstandard Material Policies and Procedures (U)

**CJCSI 6510.01F**

Information Assurance (IA) and Support to Computer Network Defense (CND) (Available at [http://www.dtic.mil/cjcs\\_directives/.](http://www.dtic.mil/cjcs_directives/))

**CNSSI 4009**

National Information Assurance (IA) Glossary (Available at [http://www.cnss.gov/.](http://www.cnss.gov/))

**DODD 3600.01**

Information Operations (IO) (Available at [http://www.dtic.mil/whs/directives/.](http://www.dtic.mil/whs/directives/))

**EO 096–08**

Project Labor Agreements (Available at [http://www.gpoaccess.gov/uscode.](http://www.gpoaccess.gov/uscode/))

**EO 12333**

United States intelligence activities (Available at [http://www.gpoaccess.gov/uscode.](http://www.gpoaccess.gov/uscode/))

**PL 90–351**

Law Enforcement Assistance (Available at [http://thomas.loc.gov/bss/.](http://thomas.loc.gov/bss/))

**PL 99–508**

Electronic Communications Privacy Act of 1986 (Available at [http://thomas.loc.gov/bss/.](http://thomas.loc.gov/bss/))

**PL 100–235**

Federal Computer System Security Training (Available at [http://thomas.loc.gov/bss/.](http://thomas.loc.gov/bss/))

**PL 104–106**

National Defense Authorization Act for Fiscal Year 1996 (Available at [http://thomas.loc.gov/bss/.](http://thomas.loc.gov/bss/))

**PL 107–347**

E–Government Act of 2002 (Available at [http://thomas.loc.gov/bss/.](http://thomas.loc.gov/bss/))

**18 USC(b)(1)**

Crimes and Criminal Procedure (Available at [http://www.gpoaccess.gov/uscode.](http://www.gpoaccess.gov/uscode/))

**18 USC 107**

Intelligence activities: intercept encrypted or other official communications of United States executive branch entities or United States Government contractors for communications security purposes (Available at [http://www.gpoaccess.gov/uscode.](http://www.gpoaccess.gov/uscode/))

**18 USC 2511**

Interception and disclosure of wire, oral, or electronic communications prohibited (Available at [http://www.gpoaccess.gov/uscode.](http://www.gpoaccess.gov/uscode/))

**18 USC Chapter 119**

Wire and electronic communications interception and interception of oral communications, definitions (Available at [http://www.gpoaccess.gov/uscode.](http://www.gpoaccess.gov/uscode/))

**Section III****Prescribed Forms**

Except where otherwise indicated below, the following forms are available as follows: DA Forms are available on the APD Web site (<http://www.apd.army.mil>); DD Forms are available on the Office of the Secretary of Defense Web site (<http://www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm>).

**DD Form 2056**

Telephone Monitoring Notification Decal (Cited in paras 2-6a(1)(d), 2-6b(1)(b)1, 2-6b(1)(b)2, and 2-6b(1)(b)3.)

**Section IV****Referenced Forms**

Except where otherwise indicated below, the following forms are available as follows: DA Forms are available on the APD Web site (<http://www.apd.army.mil>); DD Forms are available on the Office of the Secretary of Defense Web site (<http://www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm>).

**DA Form 11-2**

Internal Control Evaluation Certification

**DA Form 2028**

Recommended Changes to Publications and Blank Forms

## **Appendix B Forms of Monitoring Notification**

This appendix provides guidance for application of banners concerning information systems security monitoring certification notifications, standard mandatory notice and consent provisions, and facsimile cover sheets.

### **B-1. Telephone or communications directory notice**

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 INFORMATION SYSTEMS MONITORING.

### **B-2. Facsimile cover sheet**

ATTENTION!

DO NOT PROCESS, STORE, OR TRANSMIT CLASSIFIED INFORMATION ON UNSECURED 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 SYSTEMS SECURITY MONITORING.

## **Appendix C Internal Control Evaluation**

### **C-1. Function**

The function covered by this evaluation is for COMSEC monitoring.

### **C-2. Purpose**

The purpose of the evaluation is to assist unit commanders in evaluating key internal controls. It is not intended to cover all controls.

### **C-3. Instructions**

Answers must be based on actual testing of the key internal controls such as document analysis, direct observation, interviewing, sampling, and simulation. Answers that indicate deficiencies must be explained and the corrective action indicated in supporting documentation. These internal controls must be evaluated at least once every 5 years. Certification that the evaluation has been conducted must be accomplished on DA Form 11-2 (Internal Control Evaluation Certification).

### **C-4. Test questions**

*a.* Are key management controls identified in the governing Army regulation? (Headquarters, Department of the Army functional proponent only.)

*b.* Are required publications, as shown in AR 380-53, appendix A, available to COMSEC monitoring personnel? (They do not have to be maintained on hand.)

*c.* Have discrepancies noted in the most recent COMSEC monitoring audit/inspection or command COMSEC monitoring inspection been corrected?

*d.* Are records created and managed in accordance with AR 25-400-2?

*e.* Are procedures in place to ensure all personnel, including contractors, are aware of the provisions of this publication?

*f.* Does the command have a COMSEC monitoring certification request approved by the DCS, G-2 on file?

*g.* Have all personnel involved in the conduct (collection and analysis) of COMSEC monitoring received formal training and formally certified in accordance with this publication?

*h.* Have appropriate security personnel (for example, information assurance security officers) been appointed?

*i.* Are all personnel participating in COMSEC monitoring receiving annual refresher training?

*j.* Are incidents and violations reported properly?

### **C-5. Supersession**

Not applicable.



**C-6. Comments**

Help make this a better tool for evaluating internal controls. Submit comments to Headquarters, Department of the Army, DCS, G-2 (DAMI-CDS), 1000 Army Pentagon, Washington, DC 20310-1000.

## **Glossary**

### **Section I Abbreviations**

#### **1<sup>st</sup> IO CMD**

1<sup>st</sup> Information Operations Command

#### **AASA**

Administrative Assistant to the Secretary of the Army

#### **ACERT**

Army computer emergency response team

#### **ACOM**

Army command

#### **ASCC**

Army service component command

#### **CDAP**

Computer Defense Association Program

#### **CG**

Commanding General

#### **CI**

counterintelligence

#### **CIO/G-6**

Chief Information Officer, G-6

#### **CND**

computer network defense

#### **CNSSI**

Committee on National Security Systems Instruction

#### **COMSEC**

communications security

#### **DAR**

data-at-rest

#### **DCS, G-2**

Deputy Chief of Staff, G-2

#### **DCS, G-3/5/7**

Deputy Chief of Staff, G-3/5/7

#### **DOD**

Department of Defense

#### **DODI**

Department of Defense instruction

#### **DRU**

direct reporting unit

#### **EO**

executive order

**GC**  
General Counsel

**GS**  
general schedule

**IG**  
inspector general

**IO**  
information operations

**INSCOM**  
U.S. Army Intelligence and Security Command

**IS**  
Information System

**LE**  
law enforcement

**LWN**  
LandWarNet

**MOS**  
military occupational specialty

**NAV**  
network assistance visit

**NDA**  
network damage assessment

**NTISSD**  
National Telecommunications and Information Systems Security Directive

**O-5**  
LTC lieutenant colonel

**OPSEC**  
operations security

**PL**  
public law

**PPT**  
persistent penetration testing

**RCERT**  
regional computer emergency response team

**ROE**  
rules of engagement

**TIG**  
The Inspector General

**TJAG**  
The Judge Advocate General

## **USC**

United States Code

## **Section II Terms**

### **Communications security monitoring**

The act of listening to, copying, or recording transmissions of one's own official telecommunications to provide material for analysis to determine the degree of security being provided to those transmissions.

### **Computer Defense Association Program**

Conducted by the ACERT to ensure the overall security of the LWN. The program consists of the following 3 mission types:

- a. *Network assistance visits.* Identify and provide remediation for computer network security weaknesses.
- b. *Network damage analysis.* Identify, remediate, and recommend countermeasures to LWN compromises.
- c. *Persistent penetration testing.* Tactical overwatch of the LWN under the order of the DCS, G-3/5/7 or the 1<sup>st</sup> IO CMD.

### **Consent**

An agreement by a person to permit DOD communications security components to monitor official communications. Consent may be oral, written, or implied. Consent is implied when adequate notice is given that the use of official Government communications carries with it the presumption of consent.

### **Content**

The data contained in a telecommunications message, computer folder, or file. Telecommunication messages include, but are not limited to, telephone (both cellular and conventional), radio, pager, and computer network traffic.

### **Data-at-rest**

All data stored on hard drives, thumb drives, digital video disks, compact disks, floppy diskettes, and other similar storage media.

### **Data-in-motion**

Data that transverses a network either internally or externally, and is not in a state of storage, such as DAR. This includes active communications via telephone (both cellular and conventional), radio, and pager, as well as computer traffic that is transmitted between any network nodes.

### **Electronic surveillance**

The acquisition of the contents of nonpublic communication by electronic means without the consent of a person who is a party to the communication, but not including the use of radio direction finding equipment solely to determine the location of a transmitter.

### **Government telecommunications**

Telecommunications of an employee, officer, contractor, or other entity of the U.S. Government which concern an official purpose of U.S. Government and which are transmitted over a telecommunications system owned or leased by the U.S. Government or a U.S. Government contractor.

### **Information operations Red Team (IO Red Team)**

An independent, threat-based, and threat-simulated opposition force that uses passive, active, technical, and nontechnical capabilities on a formal, time-bound basis to expose and exploit the vulnerabilities of friendly forces from an IO threat perspective.

### **Keystroke monitoring**

A specialized form of audit trail software or specially designed device (tool) that records every keystroke struck by a user and every character of the response that the IS returns to the user. Keystroke monitoring on the Army's LWN is only authorized by RCERTS, certified Red Team members, and other official activities operating in official capacities.

### **Mission support teams**

A set or ad hoc team of subject matter experts who conduct various missions (to include CDAP).

### **Penetration testing**

Security testing in which evaluators attempt to circumvent the security features of an IS based on the evaluators

understanding of the system design and implementation. Its purpose is to confirm and demonstrate through penetration testing techniques and procedures the degree of IS defensive postures, vulnerabilities, and procedures.

**Persistent penetration testing**

A directed mission based on mission triggers (for example, sensor data, intelligence, and signal spillage or beaconing signals from an IS) that can be performed on a 24 hours a day/7 days a week basis to include, but not limited to, identifying the signal and deactivating the source, verifying network deficiencies by identifying potential weaknesses and circumventing the defensive posture to gain access onto the network, and recommending mitigating actions.

**TEMPEST**

A name referring to the investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment (see CNSSI 4009).

**Section III**

**Special Abbreviations and Terms**

This section contains no entries.

**UNCLASSIFIED**

**PIN 004092-000**