

**Department of the Army
Pamphlet 25-2-17**

**Information Management: Army
Cybersecurity**

Incident Reporting

**Headquarters
Department of the Army
Washington, DC
8 April 2019**

UNCLASSIFIED

SUMMARY of CHANGE

DA PAM 25-2-17

Incident Reporting

This administrative revision, dated 28 October 2022—

- o Changes proponentcy from CIO/G-6 to Deputy Chief of Staff, G-6 (title page).

This new publication, dated 8 April 2019—


- o Provides guidance for cybersecurity incident reporting (throughout).
- o Provides procedures for reporting cybersecurity responsibilities once suspicious activity is identified (throughout).

Information Management: Army Cybersecurity
Incident Reporting

By Order of the Secretary of the Army:

JAMES C. MCCONVILLE
General, United States Army
Chief of Staff

Official:


MARK F. AVERILL
Administrative Assistant to the
Secretary of the Army

History. This publication is an administrative revision. The portions affected by this administrative revision are listed in the summary of change..

Summary. This pamphlet supports AR 25–2 and the Army Cybersecurity Program. This pamphlet outlines the process for reporting cybersecurity incidents.

Applicability. This pamphlet applies to the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated.

Proponent and exception authority. The proponent for this pamphlet is the Deputy Chief of Staff, G–6. The proponent has the authority to approve exceptions or waivers to this pamphlet 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 pamphlet 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.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) via email to usarmy.pentagon.hqda-dcs-g-6.mbx.publications-management@army.mil.

Distribution. This pamphlet is available in electronic media only and is intended for the Regular 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 and forms • 1–2, page 1

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

Records management (recordkeeping) requirements • 1–4, page 1

Chapter 2

Reporting, page 1

Incident Reporting • 2–1, page 1

Reporting Duties • 2–2, page 2

Appendixes

A. References, page 4

Glossary

*This pamphlet supersedes DA Pam 25–2–17, dated 8 April 2019.

Chapter 1 Introduction

1–1. Purpose

This pamphlet addresses the requirement and criteria for all personnel to report cybersecurity related events.

1–2. References and forms

See appendix A.

1–3. Explanation of abbreviations and terms

See glossary.

1–4. Records management (recordkeeping) requirements

The records management requirement for all record numbers, associated forms, and reports required by this publication are addressed in the Records Retention Schedule–Army (RRS–A). Detailed information for all related record numbers, forms, and reports are located in Army Records Information Management System (ARIMS)/RRS–A at <https://www.arims.army.mil>. If any record numbers, forms, and reports are not current, addressed, and/or published correctly in ARIMS/RRS–A, see DA Pam 25–403 for guidance.

Chapter 2 Reporting

2–1. Incident Reporting

Army cyber incident reporting and handling is subject to the requirements of CJCSM 6510.01B, CJCSI 6510.01F, and DODI 8530.01. Reporting is essential to the security of Army information systems (ISs) because it provides awareness and insight into an incident that has or is taking place.

a. CNSSI 4009 defines an IS incident as an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an IS or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Treat evidence or suspicion of an incident, intrusion, or criminal activity with care, and maintain the IS without change, pending coordination with supporting cybersecurity, regional cyber center (RCC), computer crimes investigation unit (CCIU), and counterintelligence (CI) office personnel. Commanders and cybersecurity personnel will enforce the policies governing unauthorized use of computer resources and implement the Department of the Army (DA) incident response plan (IRP).

b. Each cyber event or incident is associated with one or more incident categories as part of the incident handling process in accordance with CJCSM 6510.01B. Reportable events or incidents that may lead to criminal investigations require notification and reporting to law enforcement (LE) and CI. At a minimum, Category 1, 2, and 4 incidents are reported to DOD LE/CI as described and in accordance with established procedures in CJCSM 6510.01B.

c. Time-sensitive actions are necessary to limit the amount of damage or access. Commanders and cybersecurity personnel will report IS incidents to CCIU and the supporting CI office and will assist in compiling supporting evidence, impact assessments, associated costs, containment viability, and eradication and reconstruction measures to effectively manage the breach and provide evidentiary material to CCIU. Cybersecurity personnel must notify the personnel security manager of incidents potentially requiring personnel action.

(1) All personnel will safeguard IS incident reports as sensitive controlled unclassified information (CUI) or to the classification level at which the affected system is approved to operate.

(2) Cybersecurity personnel will ensure incident response procedures are exercised at least annually for low and moderate impact systems and every 6 months for high impact systems to assure continued effectiveness. Incident response exercises will be coordinated with organizational elements responsible for business continuity plans, contingency plans, disaster recovery plans, continuity of operations plans, crisis communications plans, critical infrastructure plans, and occupant emergency plans.

(3) Incidents will be reported using the Joint Incident Management System as required by CJCSM 6510.01B. Reports will not be considered complete until meeting the completion guidelines in CJCSM 6510.01B.

(4) All users will notify the information system security officer (ISSO) and follow local IRPs. IS incidents or events include, but are not limited to—

- (a) Known or suspected intrusion or access by an unauthorized individual.
 - (b) Authorized user attempting to circumvent security procedures or elevate access privileges.
 - (c) Unexplained modifications of files, software, and/or programs.
 - (d) Unexplained or erratic IS system responses.
 - (e) Presence of suspicious files, shortcuts, or programs.
 - (f) Malicious logic infection (for example, virus, worm, trojan).
 - (g) Receipt of suspicious e-mail attachments, files, or links.
 - (h) Violations of cybersecurity policy and mandatory procedures in AR 25–2, cybersecurity DA Pams, and official cybersecurity issuances such as memorandums; official orders; executive orders; all Army activity messages; tactics, techniques, and procedures; and so forth.
 - (i) Unauthorized disclosure of classified information (UDCI) incidents, commonly referred to as spillage.
 - (j) Negligent discharge of classified information (NDCI).
 - (k) Compromise, disclosure, or loss of unclassified sensitive information (non-public information), such as for official use only, CUI, personally identifiable information (PII), and protected health information. This includes discovery of Army sensitive information on unauthorized public or private websites and systems.
 - (l) Compromise of Secret Internet Protocol Router Network (SIPRNET) token, common access card (CAC), or alternative smart card login token.
 - (m) Loss of system accessibility, or system data or services availability for a period of time inconsistent with normal system operations.
 - (n) PII incident breaches.
- (5) A serious incident report will be generated and reported per AR 190–45 under the following conditions:
- (a) The incident may cause adverse effects to the Army's image such as web page defacements.
 - (b) Access or compromise of classified, sensitive, or protected information (for example, social security numbers, medical condition or status, doctor-patient or attorney-client privilege).
 - (c) Compromise originating from a foreign source.
 - (d) Compromise of systems that may risk safety, life and limb, has the potential for catastrophic effects, or contains information for which the Army is attributable (for example, publicly accessible waterways navigational safety information from the United States Army Corps of Engineers).
 - (e) Loss of any IS or media containing protected or classified information (for example, UDCI incidents).
- (6) UDCI incidents, commonly referred to as spillage, should follow guidance in CIO/G–6 memorandum, dated 2 May 2016.
- (7) Communications security (COMSEC) account managers and key management infrastructure operating account managers must report network or system incidents on the COMSEC workstation (local management device/key processor or management client/advanced key processor) as COMSEC incidents in accordance with AR 380–40 and TB 380–41 procedures and guidance.
- (8) Army special access program (SAP)/special access (SA) activities must report incidents involving special access required (SAR) information in accordance with AR 380–381.

2–2. Reporting Duties

- a. An individual who suspects or observes an unusual or obvious network or system incident or occurrence will stop all activities and notify his or her cybersecurity personnel (ISSO/information system security manager (ISSM)) immediately. The ISSO will contact the supporting RCC and Network Enterprise Technology Command (NETCOM) signal brigade. Supporting NETCOM signal brigades will notify their theater signal command. The initial notification must be conducted securely, preferably through out-of-band communication channels or use of encrypted messaging capabilities; for example, CAC-encrypted e-mails for initial communications on unclassified networks.
- b. Individuals not able to make immediate contact with cybersecurity personnel (for example, system administrator/network administrator, ISSO) for incident handling will contact their local network enterprise center (NEC) help desk to begin reporting until cybersecurity personnel assume the reporting. If there is no available NEC help desk, report to either the Army enterprise service desk or the theater RCC. Keep the system running until told otherwise.
- c. Cybersecurity personnel who observe, suspect, or are notified of a potential incident or intrusion will prohibit unnecessary activity on or to the asset(s) and immediately notify the supporting RCC, which will immediately notify CCIU and CI personnel. IS personnel will take no additional actions to investigate the incident or isolate the system (through physical or logical means, such as network/power) until directed by the RCC and following coordination with CCIU, as any action could compromise the investigation and integrity of forensic data. Nothing in this DA Pam prohibits or impedes the direct reporting of potential criminal information directly to CCIU and nothing prohibits the

independent authority of U.S. Army Criminal Investigation Command or CCIU to initiate and conduct criminal investigations.

(1) Exception to activity prohibition and direction of isolation may be given to specific mission-critical assets or specific assets whose isolation would directly impact the operational mission, such as servers, watch stations, and weapons systems. RCC may override such exceptions for systems not formally designated as mission-critical. RCC may also override such exceptions for mission-critical systems in case of known immediate threat to other mission-critical Army assets and operations, such as systems used in active warfighting. Mitigating actions must still be implemented in lieu of activity prohibition and isolation.

(2) Potential UDCI and NDCI incidents should follow immediate containment procedures prior to any isolation, except where isolation is believed to be the quickest route to prevent further exposure. Isolation will only be directed for UDCI/data spillage if the nature of the incident may allow further exposure, and isolation will remain in place until the exposure can be mitigated.

(3) Organizations that cause or originate a UDCI/data spillage will become the lead agency responsible for all initial and final actions to identify, contain, eradicate, report, and collect remediation costs. Recipients of a UDCI/data spillage incident will support the identified lead agency's efforts. Army organizations that are the "first point of entry" from external agencies, and subsequently infect other organizations, may assume the lead for Army initiatives and actions, unless otherwise directed or exceeding their capabilities. All recipients affected by the UDCI/data spillage must undergo the same remediation procedures, collection, and reporting of remediation costs, and completion reporting to the lead agency. For additional guidance please see CIO/G-6 memorandum, dated 2 May 2016.

d. Isolation measures that may be directed by the RCC may include restricting direct physical access, disconnecting the network connection, disabling server functions, disabling media or devices, disabling or restricting user accounts, logical isolation (for example, access controls, switch/router configuration), shutting down, or disconnecting power.

e. The existence (and regularly updated status) of potential cybersecurity incidents must be communicated to all cybersecurity personnel (for example, ISSM, ISSO) where classification and caveats allow.

f. Each RCC is generally responsible for collecting and recording all the required information; coordinating all incident response procedures between the organization, the NEC, CCIU, respective theater signal command, and Army Cyber Command (ARCYBER); and for conducting all intrusion containment, eradication, and verification measures.

g. The incident reporting format and additional reporting requirements are available on the supporting RCC Non-classified Internet Protocol Router Network (NIPRNET) and SIPRNET websites.

h. Immediately report incidents involving SAP/SA information to the program security officer (PSO), who will follow the incident reporting guidelines outlined in AR 380-381. The PSO will also notify the ISSO/ISSM of the servicing information technology organization for the application of UDCI procedures to be implemented.

i. The Army Reserve Enterprise Network Operations and Security Center (ENOSC) will serve as the single point of reporting and coordination between ARCYBER and the states; and will report as a theater-level ENOSC to the Army Computer Emergency Response Team - Computer Network Operation, Army Cyberspace Operations and Integration Center, and ARCYBER.

j. The Army National Guard (ARNG) State Director of Information Management will serve as a single point of reporting and coordination between state tenants and ARNG Network Operations Security Center (NOSC), and will report as a state-wide area network-level network operations center directly to ARNG NOSC.

k. Army SAP/SA activities must initiate spillage inquiries involving SAR information in accordance with AR 380-381.

l. Army PII and breach information is contained in AR 25-22.

Appendix A

References

Section I

Required Publications

AR 25–2

Army Cybersecurity (Cited on title page.)

AR 190–45

Law Enforcement Reporting (Cited in para 2–1c(5).)

AR 380–40

Safeguarding and Controlling Communications Security Materiel (Cited in para 2–1c(7).)

AR 380–381

Special Access Programs (SAPS) and Sensitive Activities (Cited in para 2–1c(8).)

CIO/G–6 memorandum, dated 2 May 2016

Data Spillage and Unauthorized Disclosure Policy (Cited in para 2–1c(6).) (Available at <http://ciog6.army.mil/policylegislation/tabid/64/default.aspx>.)

CJCSI 6510.01F

Information Assurance (IA) and Support to Computer Network Defense (CND) (Cited in para 2–1.) (Available at <http://www.jcs.mil/library/cjcs-instructions/>.)

CJCSM 6510.01B

Cyber Incident Handling Program (Cited para 2–1.) (Available at <http://www.jcs.mil/library/cjcs-manuals/>.)

CNSSI 4009

Committee on National Security Systems (CNSS) Glossary (Cited in para 2–1a.) (Available at <https://www.cnss.gov/cnss/issuances/instructions.cfm>.)

DODI 8530.01

Cybersecurity Activities Support to DOD Information Network Operations (Cited in para 2–1.) (Available at <http://www.esd.whs.mil/dd/dod-issuances/>.)

TB 380–41

Security: Procedures for Safeguarding, Accounting, and Supply Control of COMSEC Material (Cited in para 2–1c(7).)

Section II

Related Publications

A related publication is a source of additional information. The user does not have to read it to understand this publication. Unless otherwise indicated, DA publications are available on the Army Publishing Directorate website (<https://armypubs.army.mil>). DOD publications are available on the Office of the Secretary of Defense website (<http://www.esd.whs.mil/dd/>).

AR 12–15

Joint Security Cooperation Education and Training

AR 25–22

The Army Privacy Program

AR 25–30

Army Publishing Program

AR 380–10

Foreign Disclosure and Contacts with Foreign Representatives

AR 380–67

Personnel Security Program

DA Pam 25–2–1
Army Cross Domain Solution and Data Transfer Management

DA Pam 25–2–2
Cybersecurity Tools Unified Capabilities Approved Products List Process

DA Pam 25–2–3
Reuse of Army Hard Drives

DA Pam 25–2–6
Cybersecurity Training and Certification Program

DA Pam 25–2–7
Army Information System Privileged Access Agreement

DA Pam 25–2–8
Cybersecurity: Sanitization of Media

DA Pam 25–2–9
Wireless Security Standards

DA Pam 25–2–11
Cybersecurity Strategy for Programs of Records

DA Pam 25–2–12
Authorizing Official

DA Pam 25–2–13
Army Identity and Access Management and Public Key Infrastructure Implementing Instructions

DA Pam 25–2–14
Risk Management Framework for Army Information Technology

DA Pam 25–2–16
Communications Security

DA Pam 25–2–18
Foreign Personnel Access to Information Systems

DOD 8570.01–M
Information Assurance Workforce Improvement Program

DODD 5230.09
Clearance of DOD Information for Public Release

DODD 5230.11
Disclosure of Classified Military Information to Foreign Governments and International Organizations

DODD 5230.25
Withholding of Unclassified Technical Data From Public Disclosure

DODI 5000.02
Operation of the Defense Acquisition System

DODI 8500.01
Cybersecurity

DODI 8510.01
Risk Management Framework (RMF) for DOD Information Technology (IT)

DODM 5200.02
Procedures for The DOD Personnel Security Program (PSP)

8 USC
Aliens and Nationality (Available at <http://uscode.house.gov/>.)

22 USC Chapter 39
Arms Export Control (Available at <http://uscode.house.gov/>.)

22 USC 2551

Congressional statement of purpose (Available at <http://uscode.house.gov/>.)

Section III**Prescribed Forms**

This section contains no entries.

Section IV**Referenced Forms**

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate website (<https://armypubs.army.mil>).

DA Form 2028

Recommended Changes to Publications and Blank Forms

Glossary

Section I

Abbreviations

AR

Army regulation

ARCYBER

Army Cyber Command

ARNG

Army National Guard

CAC

common access card

CCIU

computer crimes investigation unit

CI

counterintelligence

CIO

Chief Information Officer

CJCSI

Chairman of the Joint Chiefs of Staff instruction

CJCSM

Chairman of the Joint Chiefs of Staff manual

CNSSI

Committee on National Security Systems instruction

COMSEC

communications security

CUI

controlled unclassified information

DA

Department of the Army

DA Pam

Department of Army pamphlet

DOD

Department of Defense

DODD

Department of Defense directive

DODI

Department of Defense instruction

ENOSC

Enterprise Network Operations and Security Center

IRP

incident response plan

IS

information system

ISSM

information system security manager

ISSO

information system security officer

LE

law enforcement

NDCI

negligent discharge of classified information

NEC

network enterprise center

NETCOM

Network Enterprise Technology Command

NIPRNET

Nonclassified Internet Protocol Router Network

NOSC

Network Operations Security Center

PII

personally identifiable information

PSO

program security officer

RCC

regional cyber center

SA

special access

SAP

special access program

SAR

special access required

SIPRNET

Secret Internet Protocol Router Network

TB

technical bulletin

UDCI

unauthorized disclosure of classified information

Section II**Terms**

This section contains no entries.

Section III**Special Abbreviations and Terms**

This section contains no entries.

UNCLASSIFIED

PIN 202898-000