

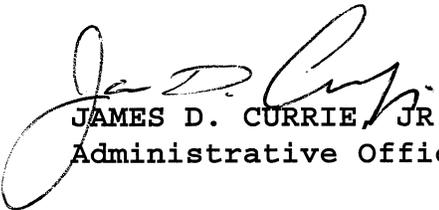
DEPARTMENT OF THE ARMY
UNITED STATES ARMY INTELLIGENCE AND
SECURITY COMMAND
Fort Belvoir, Virginia 22060-5246
24 March 2000

***INSCOM Regulation
25-70**

Information Management
ACQUISITION AND MANAGEMENT OF INFORMATION RESOURCES

FOR THE COMMANDER:

LARRY L. MILLER
Colonel, GS
Chief of Staff


JAMES D. CURRIE, JR.
Administrative Officer

History. This regulation revises the United States Army Intelligence and Security Command (INSCOM) Regulation 25-70.

Applicability. This regulation applies to Headquarters (HQ), INSCOM and subordinate commands who have or plan to acquire Information Management (IM)/Information Technology (IT) resources to include office automation, Information Management Processing Equipment (IMPE), communications equipment, or software. Resources supporting visual information, standard Army systems, Advanced Concept Technical Demonstrations (ACTD), Advanced Technical Demonstrations (ATD) or the Combat Development Futures Technical Lab are excluded from this regulation. Attachment of devices to networks require prior approval.

Proponent and exception authority. The proponent for this regulation is the Assistant Chief of Staff, G6 (ACofS, G6). The ACofS, G6 has the authority to approve exceptions that are consistent with controlling law and regulations.

*This regulation supersedes INSCOM Regulation 25-70, 30 January 1995.

INSCOM Regulation 25-70 • 24 March 2000

Supplementation. Supplementation of this regulation is prohibited without prior approval from HQ, INSCOM, ATTN: ACofS, G6 (IAIM-POR).

Suggested Improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to INSCOM, ATTN: IAIM-POR.

Distribution. Distribution is intended for command levels A, B, and C.

Contents (Listed by paragraph and page number)

Chapter 1
Introduction

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
Procedures

Process • 2-1, page 4
Hardware/Software Management • 2-2, page 4
System Accreditation • 2-3, page 4
IA Form 3044-R-E • 4-1, page 6

Appendix A. References

Glossary

Chapter 1

Introduction

1-1. Purpose

This regulation sets policy, responsibilities and procedures for the acquisition and management of information management/information technology in accordance with (IAW) AR 25-1.

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. The Assistant Chief of Staff, G6 (ACofS, G6) will-

(1) Exercise direct staff supervision of INSCOM automation and communication programs and systems.

(2) Advise and assist INSCOM staff elements and subordinate commands in technical and managerial aspects of determining automation and communication requirements.

(3) Ensure budget submissions are submitted by Major Subordinate Commands (MSCs) through the INSCOM Investment Strategy (I2S) process.

(4) Determine redistribution priorities of identified excess IMPE assets within INSCOM.

(5) Validate proposed technical solutions.

(6) Provide a Point of Contact (POC) who will ensure staff coordination of requirements.

(7) Publish a list of INSCOM standard software products.

(8) Exercise staff supervision over the INSCOM Software Management Program.

(9) Exercise staff supervision over all software development within INSCOM.

(10) Publish a list of INSCOM standard hardware products.

(11) Exercise staff supervision over the INSCOM Hardware Management Program.

b. The Assistant Chief of Staff, G3 (ACofS, G3) will validate all automation, communications and software requirements.

c. The Assistant Chief of Staff, G4 (ACofS, G4)-Supply and Services Division will-

(1) Identify and publish user automated and manual requirements for capturing and reporting IMPE assets to the Defense Information Technology Management System (DITMS).

(2) Develop and publish general excess equipment reporting procedures for all INSCOM equipment users IAW INSCOM Regulation 700-7.

(3) Conduct lateral staff coordination with IAIM-POR for commodity management control and internal redistribution of identified excess IMPE assets within INSCOM.

(4) Provide Major Army Command MACOM level logistics automation planning and programming for INSCOM in accordance with established Army goals and objectives using standard Army systems.

(5) Publish INSCOM equipment redistribution instructions and provide MACOM approval authority for lateral transfer of identified excess between MSCs and to outside activities/agencies as the losing MACOM IAW AR 710-2 and INSCOM Regulation 700-7.

d. The Assistant Chief of Staff, System Integration (SI) and Chief Information Officer will-

(1) Serve as the principal staff advisor to the Commanding General for IM/IT and automated information systems (AISs) development activities. The ACofS, SI is designated as the INSCOM CIO.

(2) Provide management oversight for IM/IT investments.

(3) Promote efficiency and productivity in all activities through budget program management and acquisition decisions related to information technologies in conjunction with the ACofS, G6.

(4) Align IM/IT investment strategy with INSCOM strategic vision, goals, and objectives.

(5) Identify, validate, coordinate, and integrate INSCOM IM/IT enterprise-wide requirements.

(6) Ensure requirements are consistent with emerging Information Technologies/Command, Control, Communications, Computers and Intelligence (IT/C4I) technologies and comply with policies relating to C4I systems.

(7) Document requirements in a unit Systems Architecture and/or Site Transition Plan.

(8) Coordinate on all IM/IT activities prior to allocation of funds.

e. Heads of Staff Elements will-

(1) Gain ACofS, G6 approval on all requirements for the acquisition of automation, communications equipment, and software. G6 will coordinate with CIO prior to approval.

(2) Report newly acquired equipment for accountability IAW current Property Book and Hand Receipt Holder procedures.

(3) Serve as functional proponent for automation initiatives within the organization's mission area.

(4) Identify and report excess IMPE assets to INSCOM G6 IAW INSCOM Regulation 700-7.

(5) Ensure security accreditation package is staffed through the ACofS, G6 (HQ Information System Security Manager (ISSM)) in coordination with the ACofS, G2.

(6) Comply with the INSCOM Software Management Policy Program.

(7) Comply with the INSCOM Hardware Management Program.

f. INSCOM subordinate commanders will-

(1) Gain ACofS, G6 approval on all requirements for the acquisition of automation equipment, communications equipment, and software. G6 will coordinate with CIO prior to approval.

(2) Coordinate all requirements through the local organizational chain of command prior to submission to IAIM-POR.

(3) Report newly acquired equipment for accountability IAW current Property Book and Hand Receipt Holder procedures.

(4) Identify and report excess IMPE assets to ACofS, G6 IAW INSCOM Regulation 700-7.

(5) Ensure security accreditation package is staffed through the unit ISSM in coordination with the ACofS, G2.

(6) Comply with the INSCOM Software Management Policy Program.

(7) Comply with the INSCOM Hardware Management Program.

Chapter 2 Procedures

2-1. Process

The process for submitting an automation, networks or communications requirement is described in figure 2-1.

2-2. Hardware/software management

All hardware and software management will be IAW with INSCOM Regulation 700-7 and the INSCOM Software and Hardware Management Program. All National Security Agency (NSA) mission excess software will be directed by INSCOM to NSA for disposition.

2-3. System Accreditation

Information/system configurations must comply with the provisions of AR 380-19, AR 380-28, AR 380-381, Department of Defense Intelligence Information System (DODIIS)/Cryptologic Sensitive Compartmented Information (SCI) Information System Security (ISS) Standards. Accreditation of the Information Systems is accomplished through unit ISSM in coordination with HQ, INSCOM, ACofS, G2. Accreditation is required prior to implementation of the system. ACofS, G6 will assist upon request.

2-4. IA Form 3044-R-E (Automation/Communications/Network Requirements Request Form)

a. IA Form 3044-R-E will be used to document automation, communications, networks, and software requirements. IA Form 3044-R-E will be locally reproduced on 8 ½ by 11-inch paper. A copy for reproduction purposes is located at the back of this regulation.

b. Instructions.

(1) Item I. Identifying Information. Self-explanatory.

(2) Item II. Funding Information.

(a) INSCOM I2S Priority Number (or reference Commanders Needs Letter). The priority that the staff head or major subordinate commander assigns to this requirement.

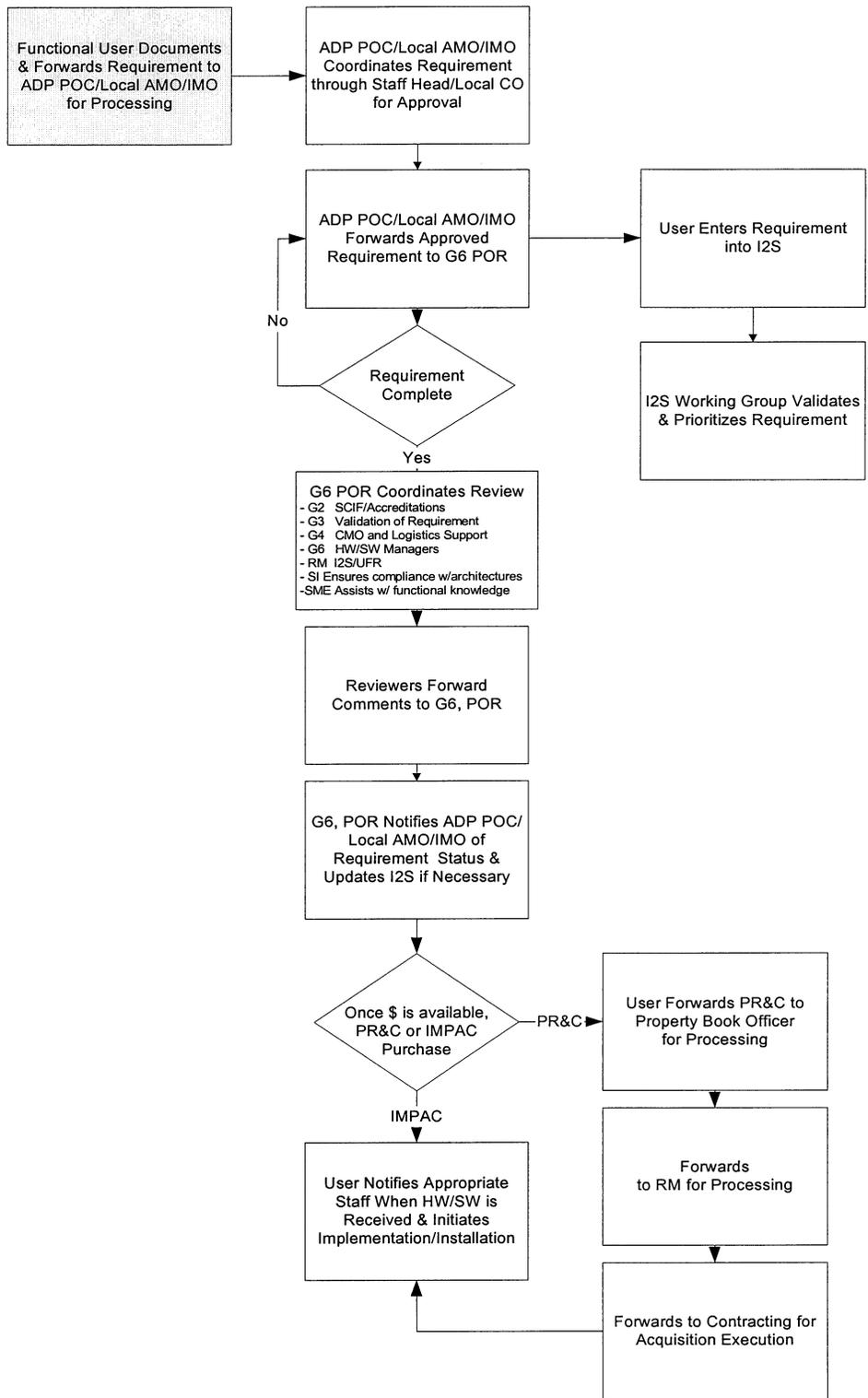


Figure 2-1. Process for Submitting an Automation/Networks/Communications Requirement

(b) Source of Funds. (e.g., year-end, General Defense Intelligence Program, Consolidated Cryptologic Program, or Budget Activity Funds).

(c) Type of Funds (OMA, OPA, etc.).

(3) Item III. Requirements Description.

(a) Requirement. Self-explanatory.

(b) Description (e.g., item specifications). List generic hardware/software/communications/networks, maintenance and sustainment requirements. In addition, list the recommended operational date.

(c) Quantity. Self-explanatory.

(d) Local Area Network Requirements (LAN). If this request involves a LAN, describe its purpose and what impact it will have on existing local area networks.

(e) Installation Resources Required. Indicate if government or contract personnel are required for installation.

(f) Documentation Required. List any user manuals, operations manuals, maintenance manuals, or on-line help, etc. required.

(g) Training. Identify required training and the target audiences

(h) Maintenance. Define the level of involvement to maintain this hardware/software/communications and the level of clearance required.

(i) Justification. At a minimum, identify what functional requirements will be met, whether the system is new, upgraded and/or networked, who will benefit, the level of classified information to be processed, whether the requested acquisition is consistent with the INSCOM Information Technology Architecture, whether the initiative has been entered into I2S and the impact if it is not operational by requested date.

(j) Source of Acquisition. Requestor may recommend any known sources that may fulfill the functional requirements.

(k) Site Preparation. Provide the following information unless it already has been submitted with engineering change proposal. Ensure sufficient space for proposed equipment, uninterrupted power supply if required, the power supply equipment and electrical voltage required, the temperature and humidity levels required, whether there is a requirement for facility modification (e.g., dedicated power lines, disk drives, air conditioners, raised floors, conduit, etc.)

(l) Security Requirements. Provide the approval authority for all systems processing classified information. Provide name, address, and phone number of ISSM/Computer Security Officer.

(m) Repair parts/Basic Supplies. Self-explanatory.

(n) Property Book Officer's Name and Address. Self-explanatory.

(4) Anticipated Costs. Self-explanatory.

Appendix A
References

Section I
Required Publications

AR 25-1
The Army Information Management

AR 380-19
Information Systems

(C) AR 380-28
Department of the Army Special Security System (U)

AR 380-381
Security, Special Access Programs (SAPs) (U)

AR 710-2
Inventory Management Supply Policy Below the Wholesale Level

(FOUO) Joint DODIIS/Cryptologic SCI Information System
Security Standards

INSCOM Regulation 700-7
Supply and Services

INSCOM Supplement 2 to AR 380-28
Department of the Army Special Security System

Section II
Related Publications

AR 71-9
Materiel Requirements

AR 335-15
Management Information Control System

**INSCOM Supplement 1 to
AR 335-15**
Management Information Control System

AR 380-5
Department of Army Information Security Program

**INSCOM Supplement 2 to
AR 380-5**
Department of Army Information Security Program

(C) AR 380-19-1
Control of Compromising Emanations (U)

DA Pam 25-91
Visual Information Procedures

DA Pam 710-2-1
Using Unit Supply System Manual

DCID 6/3
Protecting Sensitive Compartmented Information Within
Information Systems

DOD 5200-40
Information Technology Security Certification and Accreditation
Process (DITSCAP)

(FOUO) NSA Circular 25-5
Systems Acquisition Management

NSA Circular 60-5
Excess and Non-Excess SIGINT Materiel and Cryptologic Mission
IMPE Utilization Program

NSA Circular 80-7
Integrated Logistics Support Management

NTISSI 4009
National Information Systems Security Glossary

Section III
Prescribed Forms

IA Form 3044-R-E

Automation/Communications/Network Requirements Request Form,

Section IV

Referenced Forms

This section contains no entries.

Glossary

Section I Abbreviations

ACofS, G2

Assistant Chief of Staff, G2

ACofS, G3

Assistant Chief of Staff, G3

ACofS, G4

Assistant Chief of Staff, G4

ACofS, G6

Assistant Chief of Staff, G6

ACTD

Advanced Concept Technical Demonstrations

AEA

Army Enterprise Architecture

AIS

Automated Information System

AMO

Automation Management Officer

ATD

Advanced Technical Demonstrations

ATTN

Attention

BPR

Business Processing Reengineering

C4I

Command, Control, Communications, Computers, and Intelligence

CIO
Chief Information Officer

DDITMS
Defense Information Technology Management System

DODIIS
Department of Defense Intelligence Information
System

HQ
Headquarters

IAW
in accordance with

IMPE
Information Management Processing Equipment

INSCOM
United States Army Intelligence and Security Command

ISS
Information Systems Security

ISSM
Information Systems Security Manager

ISSO
Information System Security Officer

IT
Information Technology

JTA-A
Joint Technical Architecture-Army

MACOM
Major Army Command

MSC
Major Subordinate Command

NSA

National Security Agency

POC

Point of Contact

SCI

Sensitive Compartmented Information

Section II**Terms****Accreditation**

The official management authorization to operate automated information systems (AISs)/LANs in a particular security mode; with a prescribed set of administrative, environmental, and technical security guards; against a defined threat and with stated vulnerabilities and countermeasures; in a given operational environment; under a stated operational concept; with stated interconnections to other AISs and LANs; and at an acceptable level of risk for which the accrediting authority has formally assumed responsibility. The accrediting authority formally accepts and officially declares that a specified AIS or LAN will adequately protect National Security information against compromise, destruction, or unauthorized alteration through the continuous employment of safeguards including administrative, procedural, physical, personnel, communications security, emanations security, and controls. The accreditation statement affixes security responsibility with the accrediting authority and shows that due care has been taken for security.

Automated Information System

An assembly of computer hardware, software and/or firmware configured to collect, create, communicate, compute, disseminate, store, and/or control data or information.

Classification

A derivative or original classification decision that information requires protection against unauthorized disclosure in the interest of national security. Such material is annotated with appropriate classification markings that delineate the level of protection required and the

declassification date, and may contain additional warning notices and provide dissemination instructions or restrictions.

Hardware

The electric, electronic, and mechanical equipment used for processing data.

Information Management

Activities required to coordinate, plan, organize, integrate, evaluate, and control information resources effectively.

Information Systems Security Officer

An organizational level individual responsible for the security of a particular information system (IS) and to the Information Systems Security Manager (ISSM). Each organizational level unit assigns one Information System Security Officer (ISSO) per system. An ISSO may have the responsibility for more than one system.

Information Technology

Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement control, display, switching, interchange, transmission, or reception of data or information. Use is defined as direct use by a Federal agency, including Army, or by a contractor under contract with a Federal agency when the contract requires the use of such equipment, or requires use of the equipment to a significant extent to perform the contracted service or furnish the contracted product. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Information technology does not include equipment acquired by a Federal contractor which is incidental to a Federal contract.

Local Area Network

An interconnected group of system components that are physically located within a small geographic area, such as a building or campus.

Network

A network is composed of a communications medium and all components attached to that medium whose responsibility is the transfer of information, such as packet switches,

telecommunications controllers, key distribution centers, technical control devices, and other components used by the network.

Section III
Special Abbreviations and Terms

ACoS, SI
Assistant Chief of Staff, System Integration

I2S
INSCOM Investment Strategy

**AUTOMATION/COMMUNICATIONS/NETWORK
REQUIREMENTS REQUEST**

For use of this form see INSCOM Reg 25-70, the proponent is ACofS G6

I. IDENTIFYING INFORMATION

Requesting Organization	Project Name (if applicable)
-------------------------	------------------------------

Point of Contact

Office Symbol	Email Address:
---------------	----------------

Commercial Phone	Defense Switch Network Number (DSN)	Secure
------------------	--	--------

II. FUNDING INFORMATION

INSCOM Investment Strategy (I2S) Priority Number
(or reference Commanders Needs Letter)

Source of Funds	Type of Funds
-----------------	---------------

III. REQUIREMENTS DESCRIPTION

Requirement: New <input type="checkbox"/> Upgrade <input type="checkbox"/>	Hardware <input type="checkbox"/> Software <input type="checkbox"/> Comms <input type="checkbox"/>
	Standard <input type="checkbox"/> Nonstandard <input type="checkbox"/>

Description

Quantity

Local Area Network Requirements

Installation Resources Required

Documentation Required

Training

Maintenance

Justification

Known Sources of Acquisition

Site Preparation

Security Requirements (highest level of classification processed)

Government/Contract Assistance Requested

Repair parts/Basic Supplies

Property Book Officer's Name & Address

IV. Anticipated Costs

Unit Cost	\$	Training	\$
Equipment Installation	\$	Maintenance	\$
Cable Installation	\$	Life Cycle Replacement	\$
Documentation	\$	Repair Parts/Supplies	\$
Site Preparation	\$	Other	\$
Anticipated Total Cost:	\$		