

DRAFT

**Department of Defense (DoD)
Goal Security Architecture
(DGSA)**

**Center for Information System Security
Defense Information Systems Security
Program**

Version 1.0

1 August 1993

DRAFT

DRAFT

DGSA Preface-Version 1.0-1 August 1993

DRAFT

DRAFT

DGSA Preface-Version 1.0-1 August 1993

PREFACE

The Defense Information Systems Security Program is a joint undertaking of the Defense Information Systems Agency (DISA) and the National Security Agency (NSA). This document was prepared by the Architecture and Engineering Directorate of the DISA Center for Information System Security. The Architecture and Engineering Directorate is located at the NSA and comments on this document may be delivered to:

DIRECTOR, NATIONAL SECURITY AGENCY
Fort George G. Meade, MD 20755-6000
Attention: CISS/A&E/V37
Facsimile: 410-859-6813
Internet: rmcallister@dockmaster.ncsc.mil

DRAFT

TABLE OF CONTENTS

SECTION	PAGE
1.0 INTRODUCTION	1-1
1.1 PURPOSE	1-1
1.2 SCOPE	1-2
1.3 ARCHITECTURAL TYPES	1-2
1.3.1 Abstract Architecture	1-2
1.3.2 Generic Architecture	1-3
1.3.3 Logical Architecture	1-3
1.3.4 Specific Architecture	1-3
1.4 PROCESS	1-3
1.5 DOCUMENT ORGANIZATION	1-4
2.0 SECURITY REQUIREMENTS	2-1
2.1 DGSA SECURITY POLICY	2-3
2.2 DGSA SECURITY REQUIREMENTS	2-4
2.2.1 Multiple Information Security Policy Support	2-4
2.2.2 Open Systems Employment	2-4
2.2.3 Appropriate Security Protection	2-5
2.2.4 Common Security Management	2-5
2.3 DGSA DERIVED SECURITY REQUIREMENTS	2-6
2.3.1 Security Requirements Refinement	2-6
2.3.2 Interaction Between Mission-Related Operational Objectives and Security Requirements	2-8
3.0 DIS TARGET ARCHITECTURE PERSPECTIVES AND EVOLUTION	3-1
3.1 TAFIM GUIDANCE	3-3
3.1.1 DoD Technical Reference Model	3-3
3.1.2 TAFIM Information Management Integration Model	3-5
3.2 C4IFTW GUIDANCE	3-7
3.3 DIS TARGET ARCHITECTURE EVOLUTION	3-8
3.3.1 Voice-Video/Imagery-Data	3-8
3.3.2 Portable-Mobile-Fixed	3-9
3.3.3 Secure-Nonsecure	3-10
3.3.4 Workstations-Servers-Hosts	3-10
3.3.5 Programmable-Nonprogrammable	3-10
4.0 SECURITY VIEWS AND CONCEPTS	4-1
4.1 INFORMATION SYSTEM ARCHITECTURE SECURITY VIEWS	

4-1		
4.1.1	Abstract Information System Architecture Security View	4-1
4.1.2	LSE Generic Security View	4-2
4.1.3	TAFIM IM Integration Model Security View	4-5
4.2	SECURITY SERVICE ALLOCATIONS	4-6
4.2.1	CN Security Service Allocation	4-6
4.2.2	LSE Security Service Allocation	4-7
4.3	SECURITY CONCEPTS	4-10
4.3.1	Information Domains	4-10
4.3.2	Strict Isolation	4-12
4.3.3	Interdomain Information Sharing and Transfer	4-12
4.3.5	Absolute Protection	4-15
4.3.6	Uniform Accreditation	4-16
4.3.7	Security Management	4-17
5.0	END SYSTEMS AND RELAY SYSTEMS	5-1
5.1	END SYSTEM SECURITY ARCHITECTURE OVERVIEW	5-2
5.1.1	The LSE Protects the Hardware	5-2
5.1.2	The Hardware Protects the Software	5-2
5.1.3	The Software Protects Information	5-3
5.2	END SYSTEM SECURITY ARCHITECTURE DESCRIPTION	5-3
5.2.1	Separation Kernel	5-6
5.2.2	Security Contexts	5-8
5.2.3	Security-Critical Functions	5-11
5.2.4	Security-Relevant Functions	5-15
5.3	END SYSTEM SECURITY ARCHITECTURE TECHNOLOGIES	5-17
5.3.1	LSE	5-18
5.3.2	Hardware	5-18
5.3.3	Software	5-18
6.0	SECURITY MANAGEMENT	6-1
6.1	SECURITY MANAGEMENT RELATIONSHIPS TO DGSA CONCEPTS	6-1
6.2	ISO 7498-2 AND DGSA SECURITY MANAGEMENT CONCEPTS	6-4
6.2.1	Information Domains	6-4
6.2.2	Security Management Information Bases	6-4
6.2.3	Communication of Security Management Information	6-6
6.2.4	Distributed Security Management Administration	6-7
6.2.5	Security Management Application Protocols	6-7
6.2.6	End Security Management Functions	6-8

6.2.7	Security Service Management	6-9
6.2.8	Security Mechanism Management	6-13
6.3	SECURITY MANAGEMENT TOOLS	6-18
6.3.1	Security Policy Rule Specification	6-18
6.3.2	Security Mechanisms Catalog	6-18
6.3.3	Maintenance Applications for Security Administrators	6-19
6.4	AREAS FOR SECURITY MANAGEMENT STANDARDIZATION	6-20
7.0	TRANSFER SYSTEM	7-1
7.1	DISTRIBUTED SECURITY CONTEXTS	7-2
7.1.1	Distributed Security Contexts for Interactive Communications	7-2
7.1.2	Staged Delivery Distributed Security Contexts	7-6
7.1.3	Other Aspects of Distributed Security Contexts	7-7
7.2	TRANSFER SYSTEM SUPPORT	7-8
7.2.1	Security Management Application Process	7-8
7.2.2	Security Management Information Base	7-9
7.2.3	Security Protocols	7-10
7.2.4	Cryptographic Support	7-11
7.2.5	Distributed Management Systems	7-12
7.3	DGSA TRANSFER SYSTEM ISSUES	7-13
7.3.1	Traffic Flow Security in Open System Communication Environments	7-14
7.3.2	Limitations on Distributed Processing	7-14
8.0	SECURITY DOCTRINE	8-1
8.1	SECURITY SERVICES	8-1
8.2	DOCTRINAL SECURITY MECHANISMS TO PROVIDE SECURITY SERVICES	8-2
8.2.1	Mechanisms for Identification and Authentication	8-2
8.2.2	Mechanisms for Access Control	8-2
8.2.3	Mechanisms for Confidentiality	8-3
8.2.4	Mechanisms for Integrity	8-4
8.2.5	Mechanisms for Non-Repudiation	8-4
8.2.6	Mechanisms for Availability	8-4
8.3	COTS PRODUCT CONSIDERATIONS	8-5
8.4	SECURITY MANAGEMENT	8-5
9.0	EXAMPLE LOGICAL ARCHITECTURE DEVELOPMENT PROCESS	9-1
9.1	MISSION DESCRIPTIONS	9-2

DRAFT

DGSA Table of Contents-Version 1.0-1 August 1993

9.1.1	Intelligence Mission Area Function Description	9-2
9.1.2	Tactical Mission Area Function Description	9-5
9.1.3	Drug Interdiction Mission Area Function Description	9-6
9.2	MISSION AREA INFORMATION DOMAINS	9-8
9.3	INFORMATION DOMAIN SECURITY POLICIES	9-12
9.3.1	Intelligence Mission Function Information Domains	9-14
9.3.2	Tactical Mission Function Information Domains	9-17
9.3.3	Drug Interdiction Mission Function Information Domains	9-21
9.4	LOCAL SUBSCRIBER ENVIRONMENTS	9-25
9.4.1	Intelligence Site LSE Architecture (LSE-A)	9-28
9.4.2	Tactical Site LSE Architecture (LSE-B)	9-31
9.4.3	DEA Site LSE Architecture (LSE-C)	9-34
9.4.4	DOJ Site LSE Architecture (LSE-D)	9-35
9.4.5	Drug Interdiction User Site LSE Architecture (LSE-E)	9-35
9.5	SYSTEM SECURITY POLICIES	9-36
9.5.1	Intelligence Site System Security Policy (LSE-A)	9-36
9.5.2	Tactical Site System Security Policy (LSE-B)	9-36
9.5.3	DEA Site System Security Policy (LSE-C)	9-37
9.5.4	DOJ Site System Security Policy (LSE-D)	9-37
9.5.5	Drug Interdiction User Site System Security Policy (LSE-E)	9-37
9.6	SYSTEM SECURITY ARCHITECTURES	9-39
9.6.1	Intelligence Site System Security Architecture (LSE-A)	9-39
9.6.2	Tactical Site System Security Architecture (LSE-B)	9-46
9.6.3	DEA Site System Security Architecture (LSE-C)	9-47
9.6.4	DOJ Site System Security Architecture (LSE-D)	9-47
9.6.5	Drug Interdiction System Security Architecture (LSE-E)	9-47
9.7	INTERDEPENDENCY ANALYSIS	9-47
9.7.1	Interoperability Analysis	9-48
9.7.2	Security Service and Mechanism Interdependencies	9-53
9.7.3	Vulnerabilities, Residual Risk, And Recommended Countermeasures	9-57

APPENDIX A A-1

APPENDIX B B-1

REFERENCES REF-1

DRAFT

DRAFT

DGSA Table of Contents-Version 1.0-1 August 1993

LIST OF ACRONYMS

ACR-1

DRAFT

LIST OF FIGURES**FIGURE
PAGE**

2-1. Security Policy and Requirements	2-2
2-2. Mission-Specific Security Architecture Development	2-3
3-1. Building Blocks of the DIS	3-2
3-2. DoD Technical Reference Model	3-4
3-3. TAFIM IM Integration Model	3-6
3-4. DIS Target Architecture	3-9
4-1. Abstract Security Perspective	4-1
4-2. Security View of LSEs	4-2
4-3. Example Variations of Network Elements	4-3
4-4. Example LSEs and Network Elements	4-4
4-5. TAFIM IM Integration Model and DGSA End System Mapping	4-6
4-6. Secure-to-Nonsecure LSE Communications	4-7
4-7. Secure LSE Communications	4-8
4-8. Security Service Allocation Summary	4-10
5-1. End System Security Architecture Abstract View	5-5
5-2. Security Context Software Abstract Relationships	5-16
7-1. Component Relationships for Creating a Security Association	7-6
9-1. Example Mission Functions and Their Relationships	9-3
9-2. Example Mission Area Information Domain Relationships	9-13
9-3. LSE Locations, Mission Applications, and Communications	9-27
9-4. Intelligence Site LSE Functional Architecture (LSE-A)	9-29
9-5. Intelligence Site Transfer System Architecture (LSE-A)	9-30
9-6. Intelligence Site Security Protocols (LSE-A)	9-31
9-7. Tactical Site Functional Architecture (LSE-B)	9-32
9-8. Tactical Site Transfer System Architecture (LSE-B)	9-33
9-9. DEA Site Functional Architecture (LSE-C)	9-34
9-10. DEA Site Transfer System Architecture (LSE-C)	9-35
9-11. Drug Interdiction Site Functional Architecture (LSE-E)	9-36
9-12. LSE-A End System Information Domain Allocations	9-43

LIST OF TABLES

TABLE	PAGE
2-1. Summary of Security Requirements Refinements	2-9
7-1. DGSA Security Protocols and Security Services	7-11
9-1. Hierarchical Policy/Mission Relationships	9-4
9-2. Intelligence Mission Area Positions and Responsibilities	9-5
9-3. Tactical Mission Area Positions and Responsibilities	9-6
9-4. Drug Interdiction Mission Area Positions and Responsibilities	9-8
9-5. Summary of Mission Area Information Domains	9-11
9-6. Intelligence Information Domain Security Policy	9-18
9-7. Intelligence Security Management Information Domain Security Policy	9-19
9-8. Tactical Information Domain Security Policy	9-20
9-9. DEA-Only Information Domain Security Policy	9-22
9-10. DOJ-Only Information Domain Security Policy	9-23
9-11. Drug Interdiction Information Domain Security Policy	9-23
9-12. DEA/DI Security Management Information Domain Security Policy	9-25
9-13. Domain Allocations by LSE	9-28
9-14. Intelligence Site System Security Policy (LSE-A)	9-38
9-15. DEA Site System Security Policy (LSE-C)	9-39
9-16. DOJ Site System Security Policy (LSE-D)	9-40
9-17. Drug Interdiction User Site System Security Policy (LSE-E)	9-41
9-18. LSE-A End System Security Architecture Elements	9-44
9-19. Intradomain Communications Interoperability Summary	9-51
9-20. Interservice Relation to System Requirements	9-53
9-21. Hypothetical Mechanism Strength Scale	9-55
9-22. Weighted Mechanisms by Domain and LSE	9-56
9-23. Weighted Mechanism Totals, by Category and LSE-Information Domain	9-57