Welcome to the CD-ROM Version of the

# Information Assurance Technical Framework

## Release 3.1 September 2002

## What is the IATF?

The Information Assurance Technical Framework (IATF) is an overview document on security needs and potential technology solutions for information systems and networks. The IATF—and its predecessor, the Network Security Framework document—is the result of a collaborative effort by various organizations in the U.S. Government and industry. The IATF is a living document; this Release 3.1 is its fourth major release. We will continue to evolve the IATF to keep up with technology advances and to ensure that the IATF remains consistent with the Department of Defense (DoD) Information Assurance (IA) architectures and the Defense-In-Depth strategy. This September 2002 CD-ROM presents Release 3.1 of the IATF. To be certain that you are viewing the latest release of the IATF, please visit the IATF Forum Web site at http://www.iatf.net.

## Contents of this CD-ROM

This CD-ROM contains an interactive version of the IATF Release 3.1 implemented with Adobe® Acrobat® Reader® Portable Document Format (PDF) files. Using the Table of Contents, the reader can easily navigate through the IATF by clicking on a specific item of interest. Within each chapter, the bookmark column on the left of the screen provides links to:

- The IATF Screen
- The Table of Contents of the IATF
- The preceding chapter or section
- The IATF sections of the current chapter
- The next chapter or section
- Appendix A: Acronyms
- Appendix B: Glossary
- Search Instructions Page
- Reference Page.

We recommend reading the **Foreword** and **Executive Summary** sections first, to better understand the layout of the IATF. Use the **Table of Contents** and the PDF bookmarks to navigate within the IATF document.

Within each chapter or section, readers may wish to employ the *Find* function of Adobe® Acrobat® Reader® to locate all references to a particular term. The *Find* function can be accessed on the menu bar under Edit - Find, or by pressing CTRL-F. Also, the reader may increase the size of the document on the screen if necessary with Adobe® Acrobat®

Reader® View options. The View options are located under the View menu on the menu bar. The Search Instructions Page, available from each chapter, gives detailed instructions on how to use the Search capability for terms throughout the IATF document, not just in the current chapter or section. The Reference Page provides links to references in the IATF document on the CD-ROM. Lastly, the **Acronyms**, **Glossary, References Page, Search Instructions Page, and other appendices** are equipped with RETURN bookmarks. If you come across an unfamiliar term, use the **Acronyms** or **Glossary** bookmark to jump to either of these appendices. Then, use the RETURN bookmark to get back to where you left off. However, if you attempt to move between two or more separate PDF documents and use the RETURN bookmark, Adobe will likely crash. In this case, the reader will find it helpful to navigate using a series of direct links.

In addition to the PDF copy of the IATF, this CD-ROM also contains Microsoft® Word 2000 and PowerPoint 2000 files of the IATF Release 3.1. The Word files are located in the IATF_WORD folder. The PowerPoint files are the source files used for the IATF Release 3.1 figures and a set of graphical elements used in creating the IATF Release 3.1 figures. The PowerPoint files are located in the IATF_POWERPOINT folder. The Word and PowerPoint files may be accessed from your CD-ROM drive through Windows Explorer or similar directory application. Please note these Word and PowerPoint files do not have the automated navigation feature of the PDF files. Also note the IATF Release3.1 files are best printed using a PostScript printer.

Lastly, this CD-ROM also contains an installation copy of Adobe® Acrobat® Reader®.

## Your Review and Comments *Please*

The IATF is an evolving document; it will be expanded and updated. For these changes to be most beneficial, ***your*** comments and suggestions are needed. Please provide any comments or suggestions to:

IATF Manager

National Security Agency
9800 Savage Road (SAB 3), Suite 6730
Fort Meade, Maryland 20755-6730

Telephone: (410) 854-7302
Fax: (410) 854-7508
E-mail: webmaster@iatf.net.

As the IATF document continues to evolve—and increase in size—we are examining alternative ways to present the information it contains. This CD-ROM version is a step in that direction. We ask that you please send us your comments, reactions, criticism, recommended changes, noted omissions, and *any suggestions* that will make this document—on paper or on screen—more useful to you.

**Issued by:** **National Security Agency**
**Information Assurance Solutions**
**Technical Directors**

**Disclaimer:**

This Information Assurance Technical Framework is the result of a collaborative effort by various organizations within the U.S. Government and industry. This document captures security needs and potential technology solutions for information systems and networks.

The information contained in this document is provided for information purposes only.

This is not a solicitation for procurement. Rather, this document is intended to facilitate the coordination of the information systems security needs of the U.S. Government and to offer security solution recommendations based on the collaborative efforts of the joint Industry/Government Information Assurance Technical Framework Forum.

# Please review and provide comments.

The Information Assurance Technical Framework is an evolving document. It will be expanded and updated. For these changes to be most beneficial, ***your*** comments and suggestions are needed. Please provide any comments or suggestions you care to make to:

IATF Manager

National Security Agency
9800 Savage Road (SAB 3), Suite 6730
Fort Meade, Maryland 20755-6730

Telephone: (410) 854-7302
Fax: (410) 854-7508
E-mail: webmaster@iatf.net

# Foreword

The Information Assurance Technical Framework (IATF) document, Release 3.1, provides technical guidance for protecting the information infrastructures of the United States (U.S.) Government and industry. The information infrastructure processes, stores, and transmits information critical to the mission and business operations of an organization. This information is protected through information assurance (IA) that addresses all the security requirements of today's information infrastructure. IA relies on ***people***, ***operations***, and ***technology*** to accomplish the mission/business and to manage the information infrastructure. Attaining robust IA means implementing policies, procedures, techniques, and mechanisms at all layers of the organization's information infrastructure.

The IATF defines the information system security engineering (ISSE) process for developing a secure system. This process defines the principles, the activities, and the relationship to other processes. Applying these principles results in layers of protection known collectively as the Defense-in-Depth Strategy. The four major technology focus areas of the Defense-in-Depth Strategy are to Defend the Network and Infrastructure, Defend the Enclave Boundary, Defend the Computing Environment, and Defend Supporting Infrastructures.

The Defense-in-Depth Strategy has been broadly adopted. For example, within the U.S. Department of Defense (DoD), the Global Information Grid (GIG) IA Policy and Implementation Guidance was built around the strategy. This departmental-level policy document cites the IATF as a source of information on technical solutions and guidance for the DoD IA implementation.

The following content in the IATF has been updated in Release 3.1:

- Chapter 2, Defense-in-Depth, incorporates the major elements of the Defense-in-Depth Strategy.
- Chapter 3, Information Systems Security Engineering Process, refines the description of the Information Systems Security Engineer (ISSE) process.
- Chapter 7, Defend the Computing Environment, Section 7.1, Security for System Applications has been updated.
- A new appendix, Protection Needs Elicitation (PNE), has been added to detail the first and most important activity in the ISSE process.

The IATF is a living document; the next release already is being planned. Many people provided comments and recommendations on IATF Release 3.0; their comments helped define Release 3.1. Your suggestions, recommendations, and needs will define the next release—***if we hear from you***.

We want and need your feedback.

We ask that you send us your comments, reactions, criticism, recommended changes, noted omissions, and any suggestions that will make this document more useful to you. Please send your suggestions to webmaster@iatf.net. We also encourage you to visit the IATF Forum Web site (http://www.iatf.net) often. There you will be able to see the next release of the IATF unfolding, to review new and draft sections, to access contributor's resources, and, again, to give us your feedback. The objective of the IATF is to be a useful document *for you.* Please let us know how we did.

Recently, we have drafted Cooperative Research and Development Agreements (CRADA) for contributors who may prepare articles, papers, or other submissions for inclusion in the IATF. The CRADA is located on the contributor's page of the IATF Forum Web site.

On behalf of all the contributors of the Information Assurance Technical Framework—Release 3.1 and its predecessors—our thanks to the many people who reviewed and commented on the documents. Thanks also go to the many speakers and panelists of the IATF Forum sessions and the past Network Security Framework Forum sessions for sharing their valuable insights on the security architectures, standards, and solutions that industry and government are bringing to bear on the complex challenge of information assurance.

Cynthia Frederick
IATF Technical Director

# TABLE OF CONTENTS

**FOREWORD** ..... iii

**LIST OF APPENDICES** ..... xiii

**LIST OF FIGURES** ..... xv

**LIST OF TABLES** ..... xix

**EXECUTIVE SUMMARY** ..... ES-1

**SUMMARY OF CHANGES** ..... 1

CHAPTER 1
**INTRODUCTION** ..... 1-1
- 1.1 Objectives ..... 1-1
- 1.2 Intended Audiences ..... 1-2
- 1.3 Context ..... 1-2
  - 1.3.1 Information Infrastructures Defined ..... 1-2
  - 1.3.2 Categorizing Information and Information Infrastructures ..... 1-3
  - 1.3.3 Boundaries and Information Infrastructures ..... 1-5
  - 1.3.4 Information Assurance Framework Areas ..... 1-6
  - 1.3.5 Nature of Cyber Threats ..... 1-11
- 1.4 Defense-in-Depth ..... 1-14
  - 1.4.1 Defense-in-Depth and the IATF ..... 1-15
- 1.5 IATF Organization ..... 1-15

CHAPTER 2
**DEFENSE IN DEPTH** ..... 2-1
- 2.1 Introduction and Context Diagrams ..... 2-1
  - 2.1.1 Examples of User Environments ..... 2-1
- 2.2 Adversaries, Motivations, and Classes of Attack ..... 2-4
- 2.3 People, Technology, Operations ..... 2-7
  - 2.3.1 People ..... 2-7
  - 2.3.2 Technology ..... 2-8
  - 2.3.3 Operations ..... 2-9
- 2.4 Defense in Depth Objectives Overview ..... 2-9
- 2.5 Additional Resources ..... 2-14

CHAPTER 3
**THE INFORMATION SYSTEMS SECURITY ENGINEERING PROCESS** ..... 3-1
3.1 Introduction ..... 3-1
3.2 Principles ..... 3-4
3.3 Process ..... 3-5
3.3.1 Discover Information Protection Needs ..... 3-5
3.3.2 Define System Security Requirements ..... 3-8
3.3.3 Design System Security Architecture ..... 3-10
3.3.4 Develop Detailed Security Design ..... 3-11
3.3.5 Implement System Security ..... 3-12
3.3.6 Assess Information Protection Effectiveness ..... 3-15
3.4 ISSE Relationship to Sample SE Processes ..... 3-16
3.5 Relationship of ISSE to DITSCAP ..... 3-17
3.6 Summary ..... 3-22

CHAPTER 4
**TECHNICAL SECURITY COUNTERMEASURES** ..... 4-1
4.1 Introduction ..... 4-1
4.2 Adversaries, Motivations, and Categories of Attacks ..... 4-2
4.2.1 Potential Adversaries ..... 4-2
4.2.2 Classes of Attack ..... 4-4
4.3 Primary Security Services ..... 4-10
4.3.1 Access Control ..... 4-10
4.3.2 Confidentiality ..... 4-18
4.3.3 Integrity ..... 4-21
4.3.4 Availability ..... 4-22
4.3.5 Nonrepudiation ..... 4-23
4.4 Important Security Technologies ..... 4-24
4.5 Robustness Strategy ..... 4-30
4.5.1 Overview of the General Process ..... 4-31
4.5.2 Determining the Degree of Robustness ..... 4-32
4.5.3 Strength of Mechanism ..... 4-34
4.5.4 Level of Assurance ..... 4-45
4.5.5 Examples of Process Application ..... 4-46
4.5.6 Robustness Strategy Evolution ..... 4-52
4.5.7 Real-World Applications ..... 4-53
4.6 Interoperability Framework ..... 4-53
4.6.1 Major Elements of Interoperability ..... 4-54
4.6.2 Challenges for Interoperability ..... 4-55
4.6.3 Interoperability Strategy ..... 4-55

4.7 Key Management Infrastructure/ Public Key Infrastructure Considerations ..... 4-57
4.7.1 KMI/PKI Overview ..... 4-57
4.7.2 KMI/PKI Operational Services ..... 4-58
4.7.3 KMI/PKI Processes ..... 4-58

CHAPTER 5
**DEFEND THE NETWORK AND INFRASTRUCTURE** ..... 5-1
5.1 Availability of Backbone Networks ..... 5.1-1
5.1.1 Target Environment ..... 5.1-1
5.1.2 Consolidated Requirements ..... 5.1-5
5.1.3 Potential Attacks and Potential Countermeasures ..... 5.1-8
5.1.4 Technology Assessment ..... 5.1-13
5.1.5 Framework Guidance ..... 5.1-17
5.2 Wireless Networks Security Framework ..... 5.2-1
5.2.1 Cellular Telephone ..... 5.2-4
5.2.2 Low Earth Orbiting/Medium Earth Orbiting Satellite Telephone Networks ..... 5.2-16
5.2.3 Wireless Local Area Network ..... 5.2-22
5.2.4 Paging (One-Way and Two-Way) ..... 5.2-31
5.2.5 Wireless Local Loop/Wireless Public Branch Exchange Cordless Telephones ..... 5.2-39
5.3 System-High Interconnections and Virtual Private Networks ..... 5.3-1
5.3.1 Target Environment ..... 5.3-2
5.3.2 Consolidated Requirements ..... 5.3-5
5.3.3 Potential Attacks ..... 5.3-7
5.3.4 Potential Countermeasures ..... 5.3-9
5.3.5 Technology Assessment ..... 5.3-10
5.3.6 Cases ..... 5.3-22
5.3.7 Framework Guidance ..... 5.3-23
5.4 Security for Voice Over Internet Protocol (VoIP) ..... 5.4-1
5.4.1 Target Environment ..... 5.4-3
5.4.2 Requirements ..... 5.4-4
5.4.3 Potential Attacks ..... 5.4-5
5.4.4 Potential Countermeasures ..... 5.4-7
5.4.5 Technology Assessment ..... 5.4-8
5.4.6 Cases ..... 5.4-23
5.4.7 Framework Guidance ..... 5.4-25
5.4.8 Technology Gaps ..... 5.4-26
5.4.9 Summary of Important Concepts ..... 5.4-27
5.5 Multiple Security Layers ..... 5.5-1

CHAPTER 6

**DEFEND THE ENCLAVE BOUNDARY/EXTERNAL CONNECTIONS** ..... 6-1

6.1 Firewalls ..... 6.1-1
6.1.1 Target Environment ..... 6.1-1
6.1.2 Firewall Requirements ..... 6.1-2
6.1.3 Potential Attacks ..... 6.1-4
6.1.4 Potential Countermeasures ..... 6.1-6
6.1.5 Firewall Technology Assessment ..... 6.1-10
6.1.6 Cases ..... 6.1-19
6.1.7 Enclave Boundary Protection Framework Guidance ..... 6.1-29

6.2 Remote Access ..... 6.2-1
6.2.1 Target Environment ..... 6.2-1
6.2.2 Consolidated Requirements ..... 6.2-2
6.2.3 Potential Attacks ..... 6.2-4
6.2.4 Potential Countermeasures ..... 6.2-5
6.2.5 Technology Assessment ..... 6.2-6
6.2.6 Cases ..... 6.2-12
6.2.7 Framework Guidance ..... 6.2-13

6.3 Guards ..... 6.3-1
6.3.1 Target Environment ..... 6.3-1
6.3.2 Requirements ..... 6.3-3
6.3.3 Potential Attacks ..... 6.3-5
6.3.4 Potential Countermeasures ..... 6.3-7
6.3.5 Guard Technology Assessment ..... 6.3-10
6.3.6 Selection Criteria ..... 6.3-19
6.3.7 Framework Guidance ..... 6.3-21
6.3.8 Technology Gaps ..... 6.3-25

6.4 Network Monitoring Within Enclave Boundaries and External Connections ..... 6.4-1
6.4.1 Network Intrusion Detection ..... 6.4-2
6.4.2 Malicious Code (or Virus) Detectors ..... 6.4-12
6.4.3 Discussion of Typical Bundling of Capabilities ..... 6.4-16
6.4.4 Beyond Technology Solutions ..... 6.4-17
6.4.5 For More Information ..... 6.4-18

6.5 Network Scanners Within Enclave Boundaries ..... 6.5-1
6.5.1 Network Vulnerability Scanners ..... 6.5-1
6.5.2 War Dialers ..... 6.5-6
6.5.3 Considerations for Deployment ..... 6.5-10
6.5.4 Considerations for Operation ..... 6.5-11
6.5.5 Discussion of Typical Bundling of Capabilities ..... 6.5-11
6.5.6 Beyond Technology Solutions ..... 6.5-12
6.5.7 For More Information ..... 6.5-12

6.6 Malicious Code Protection ..... 6.6-1
6.6.1 Target Environment ..... 6.6-2

6.6.2 Malicious Code Protection Requirements ..... 6.6-3
6.6.3 Potential Attack Mechanisms ..... 6.6-4
6.6.4 Potential Countermeasures ..... 6.6-6
6.6.5 Technology Assessment ..... 6.6-11
6.6.6 Selection Criteria ..... 6.6-22
6.6.7 Cases ..... 6.6-23
6.6.8 Framework Guidance ..... 6.6-25
6.7 Multilevel Security ..... 6.7-1
6.7.1 High-to-Low ..... 6.7-1
6.7.2 MLS Workstation ..... 6.7-23
6.7.3 MLS Servers ..... 6.7-23
6.7.4 MLS Network Components ..... 6.7-23

CHAPTER 7
**DEFEND THE COMPUTING ENVIRONMENT** ..... 7-1
7.1 Security for System Applications ..... 7.1-1
7.1.1 Target Environment ..... 7.1-1
7.1.2 Consolidated Requirements ..... 7.1-5
7.1.3 Potential Attacks ..... 7.1-6
7.1.4 Potential Countermeasures ..... 7.1-8
7.1.5 Technology Assessment ..... 7.1-11
7.1.6 Cases ..... 7.1-21
7.1.7 Framework Guidance ..... 7.1-23
7.2 Detect and Respond Capabilities Within Host-Based Computing Environments ..... 7.2-1
7.2.1 Host Monitors—Intrusion Detection ..... 7.2-2
7.2.2 Host Monitors—Malicious Code or Virus Detectors ..... 7.2-13
7.2.3 Host Vulnerability Scanners ..... 7.2-17
7.2.4 File Integrity Checkers ..... 7.2-23
7.2.5 Typical Bundling of Capabilities Within Products ..... 7.2-27
7.2.6 Beyond Technology Solutions ..... 7.2-27
7.2.7 For More Information ..... 7.2-29

CHAPTER 8
**SUPPORTING INFRASTRUCTURE** ..... 8-1
8.1 Key Management Infrastructure/ Public Key Infrastructure ..... 8.1-1
8.1.1 KMI/PKI Introduction ..... 8.1-1
8.1.2 Certificate Management ..... 8.1-11
8.1.3 Symmetric Key Management ..... 8.1-35
8.1.4 Infrastructure Directory Services ..... 8.1-39
8.1.5 Infrastructure Management ..... 8.1-48
8.1.6 KMI/PKI Assurance ..... 8.1-70
8.1.7 KMI/PKI Solutions ..... 8.1-71

8.1.8 Future Trends of Public Key Infrastructure ..... 8.1-102
8.2 Detect and Respond as a Supporting Element ..... 8.2-1
8.2.1 What This Focus Area Addresses ..... 8.2-1
8.2.2 Enterprise Architecture Considerations ..... 8.2-2
8.2.3 General Considerations for a Detect and Respond Solution ..... 8.2-5
8.2.4 Detect and Respond Functions ..... 8.2-8
8.2.5 Relevant Detect and Respond Technologies ..... 8.2-19
8.2.6 For More Information ..... 8.2-38

CHAPTER 9
**INFORMATION ASSURANCE FOR THE TACTICAL ENVIRONMENT** ..... 9-1
9.1 Target Environment ..... 9-2
9.2 Wiping Classified Data From Tactical Equipment ..... 9-8
9.2.1 Mission Need ..... 9-8
9.2.2 Consolidated Requirements ..... 9-10
9.2.3 Technology Assessment ..... 9-10
9.2.4 Framework Guidance ..... 9-11
9.3 Stored Data Protection in a Hostile Environment ..... 9-11
9.3.1 Mission Need ..... 9-12
9.3.2 Consolidated Requirements ..... 9-13
9.3.3 Technology Assessment ..... 9-13
9.3.4 Framework Guidance ..... 9-14
9.4 Key Management in a Tactical Environment ..... 9-14
9.4.1 Mission Need ..... 9-14
9.4.2 Consolidated Requirements ..... 9-16
9.4.3 Technology Assessment ..... 9-16
9.4.4 Framework Guidance ..... 9-18
9.5 Network Mobility/Dynamic Networks ..... 9-18
9.5.1 Mission Need ..... 9-19
9.5.2 Consolidated Requirements ..... 9-20
9.5.3 Technology Assessment ..... 9-21
9.5.4 Framework Guidance ..... 9-23
9.6 Access to Individual Classified Accounts by Multiple Users ..... 9-24
9.6.1 Mission Need ..... 9-25
9.6.2 Consolidated Requirements ..... 9-25
9.6.3 Technology Assessment ..... 9-26
9.6.4 Framework Guidance ..... 9-27
9.7 Secure Net Broadcast and Multicast ..... 9-28
9.7.1 Mission Need ..... 9-28
9.7.2 Consolidated Requirements ..... 9-28
9.7.3 Technology Assessment ..... 9-29
9.7.4 Framework Guidance ..... 9-31

9.8 IA Solutions in Low Bandwidth Communications ..... 9-31
9.8.1 Mission Need ..... 9-31
9.8.2 Consolidated Requirements ..... 9-32
9.8.3 Technology Assessment ..... 9-32
9.8.4 Framework Guidance ..... 9-34
9.9 Split-Base Operations ..... 9-34
9.9.1 Mission Need ..... 9-37
9.9.2 Consolidated Requirements ..... 9-37
9.9.3 Technology Assessment ..... 9-38
9.9.4 Framework Guidance ..... 9-39
9.10 Multi-Level Security ..... 9-39
9.10.1 Mission Need ..... 9-40
9.10.2 Consolidated Requirements ..... 9-40
9.10.3 Technology Assessment ..... 9-41
9.10.4 Framework Guidance ..... 9-42
9.11 Additional Technologies ..... 9-42

CHAPTER 10
**A VIEW OF AGGREGATED SOLUTION** ..... 10-1

**This page intentionally left blank.**

# LIST OF APPENDICES

APPENDIX A — **ACRONYMS** ..... A-1

APPENDIX B — **GLOSSARY** ..... B-1

APPENDIX C — **CHARACTERIZATION OF CUSTOMER COMMUNITY NETWORKS** C-1

APPENDIX D — **SYSTEM SECURITY ADMINISTRATION** ..... D-1

APPENDIX E — **OFFICE OF THE SECRETARY OF DEFENSE INFORMATION ASSURANCE POLICY ROBUSTNESS LEVELS** ..... E-1

APPENDIX F — **EXECUTIVE SUMMARIES** ..... F-1

APPENDIX G — **PROTECTION PROFILES** ..... G-1

APPENDIX H — **PROTECTION NEEDS ELICITATION** ..... H-1

APPENDIX I — **MISSION-ORIENTED RISK ANALYSIS** ..... I-1

APPENDIX J — **ISSE RELATIONSHIP TO SAMPLE SE PROCESSES** ..... J-1

**This page intentionally left blank.**

# LIST OF FIGURES

## Chapter 1

Figure 1-1. Availability and Protection to Information ..... 1-4
Figure 1-2. Information Infrastructure Elements ..... 1-5
Figure 1-3. IA Technology Framework Access ..... 1-6
Figure 1-4. Local Computing Environment Area ..... 1-7
Figure 1-5. Enclave Boundaries Framework Area ..... 1-8
Figure 1-6. Network and Infrastructure Framework Structure ..... 1-10
Figure 1-7. Classes of Attacks on the Information Infrastructure ..... 1-13
Figure 1-8. Principal Aspects of the Defense-in-Depth ..... 1-14
Figure 1-9. Composition of the IATF ..... 1-16

## Chapter 2

Figure 2-1. Federal Computing Environment—DOE ..... 2-2
Figure 2-2. Federal Computing Environment—DoD ..... 2-4
Figure 2-3. Classes of Attacks on the Information Infrastructure ..... 2-6
Figure 2-4. Defense in Depth Strategy ..... 2-7
Figure 2-5. Defense in Depth Strategy—People ..... 2-8
Figure 2-6. Defense in Depth Strategy—Technology ..... 2-8
Figure 2-7. Defense in Depth Strategy—Operations ..... 2-9
Figure 2-8. Defense in Depth Focus Areas ..... 2-11

## Chapter 3

Figure 3-1. Generic Systems Engineering Process ..... 3-2
Figure 3-2. Discover Needs ..... 3-7
Figure 3-3. Allocation of Needs into a Solution Set ..... 3-8
Figure 3-4a. Define System Requirements ..... 3-10
Figure 3-4b. Design System Architecture ..... 3-10
Figure 3-5. DoD 5000.2-R Systems Engineering Process ..... 3-17
Figure 3-6. IEEE Std 1220-1998 Systems Engineering Process ..... 3-18
Figure 3-7. Relationship of SE/ISSE and C&A ..... 3-19

## Chapter 4

Figure 4-1. Categories of Attacks Against Networked Systems ..... 4-5

## Chapter 5

Figure 5-1. Defend the Network and Infrastructure ..... 5-2
Figure 5.1-1. Backbone Availability Model ..... 5.1-3

Figure 5.2-1. Wireless Extension of the Wired Infrastructure ..... 5.2-4
Figure 5.2-2. Cellular Telephone Environment ..... 5.2-6
Figure 5.2-3. Mobile Satellite Subscriber Environment ..... 5.2-17
Figure 5.2-4. WLAN Environment ..... 5.2-23
Figure 5.2-5. Pager Environment ..... 5.2-33
Figure 5.2-6. Wireless Telephony Environments ..... 5.2-41
Figure 5.3-1. Target Environment Communications Infrastructure ..... 5.3-2
Figure 5.3-2. Local Virtual Private Network Architectures ..... 5.3-5
Figure 5.3-3. IP Layering Encryption Methods ..... 5.3-16
Figure 5.3-4. Reverse Tunneling Placement of Cryptographic Mechanisms ..... 5.3-19
Figure 5.4-1. SIP Network ..... 5.4-10
Figure 5.4-2. Relationship Between Media Gateway Control Protocol and H.323 or SIP ..... 5.4-15
Figure 5.4-3. Voice over ATM ..... 5.4-16
Figure 5.4-4. Voice over Frame Relay ..... 5.4-17
Figure 5.4-5. Integrating a VoIP Capability onto and Existing Network ..... 5.4-24

## Chapter 6

Figure 6-1. Defend the Enclave Boundary ..... 6-2
Figure 6.1-1. Enclave Boundary Environment ..... 6.1-2
Figure 6.1-2. Application Gateway ..... 6.1-14
Figure 6.1-3. Dual-Homed Firewall Architecture ..... 6.1-15
Figure 6.1-4. Screened Host Firewall Architecture ..... 6.1-16
Figure 6.1-5. Screened Subnet Firewall Architecture ..... 6.1-17
Figure 6.1-6. Case 1—Private to Public Network Communication ..... 6.1-19
Figure 6.1-7. Case 2—Remotely Accessing a Private Network ..... 6.1-22
Figure 6.1-8. Case 3—Private Network Connectivity via a Lower-Level Network ..... 6.1-24
Figure 6.1-9. Case 4—Collaborative LAN's with Public Network Connections ..... 6.1-26
Figure 6.2-1. Typical Remote Access Environment ..... 6.2-2
Figure 6.2-2. Attacks Against the Remote Access Scenario ..... 6.2-4
Figure 6.2-3. Security Technologies in the Remote Access Scenario ..... 6.2-7
Figure 6.2-4. Protocol Layers In Remote Access Scenario ..... 6.2-9
Figure 6.2-5. Remote Access Cases ..... 6.2-13
Figure 6.3-1. Guard Environment ..... 6.3-2
Figure 6.3-2. Dual Network Approach ..... 6.3-11
Figure 6.3-3. Cascading Protection ..... 6.3-19
Figure 6.3-4. File Transfers ..... 6.3-22
Figure 6.3-5. Secret to Unclassified Releasability ..... 6.3-23
Figure 6.3-6. Human Reviewer-Man in the Middle ..... 6.3-24

Figure 6.3-7. Releasability Human Verification ..... 6.3-24
Figure 6.4-1. Breakdown of Network Monitor Technologies ..... 6.4-1
Figure 6.4-2. Network IDS Deployment Options ..... 6.4-11
Figure 6.5-1. Back-Door Attacks Through Telephone Networks ..... 6.5-7
Figure 6.6-1. Malicious Code Relationship ..... 6.6-1
Figure 6.6-2. Sources of Malicious Code Infections ..... 6.6-2
Figure 6.6-3. Virus Execution ..... 6.6-12
Figure 6.6-4. Logic Bomb Execution ..... 6.6-15
Figure 6.6-5. Virus Filter ..... 6.6-18
Figure 6.6-6. DOS File Infection ..... 6.6-20
Figure 6.6-7. Intelligent Scanning Architecture (ISA) ..... 6.6-22
Figure 6.6-8. Macro Virus Infection ..... 6.6-23
Figure 6.6-9. Polymorphic Virus Infection ..... 6.6-24
Figure 6.6-10. Trojan Horse Infection ..... 6.6-25
Figure 6.7-1. High-to-Low Concepts ..... 6.7-1
Figure 6.7-2. Recommended Topology ..... 6.7-21

## Chapter 7

Figure 7-1. Local Computing Environments ..... 7-1
Figure 7.1-1. Custom N-Tier Applications ..... 7.1-17
Figure 7.2-1. Breakdown of Host Sensor Technologies ..... 7.2-1

## Chapter 8

Figure 8-1. Supporting Infrastructures: KMI/PKI ..... 8-2
Figure 8-2. Supporting Infrastructures: Detect and Respond ..... 8-4
Figure 8.1-1. Interactions of the KMI/PKI Applications Operational Services ..... 8.1-7
Figure 8.1-2. Using PKIs in Secure Enclaves ..... 8.1-12
Figure 8.1-3. Hierarchical, Trust List, and Mesh Approaches to PKI Interoperation ..... 8.1-13
Figure 8.1-4. Bilateral Cross-Certification, Bridge CA, and Online Status Approaches to PKI Interoperation ..... 8.1-14
Figure 8.1-5. Browser Certification: Key Generation and Certificate Request ..... 8.1-22
Figure 8.1-6. Browser Certification: CA Processing Request ..... 8.1-23
Figure 8.1-7. S/MIME Client Certification Process ..... 8.1-25
Figure 8.1-8. Browser Certification: Installing Certificate in Browser ..... 8.1-27
Figure 8.1-9. Critical Elements of Symmetric Key Management Activities ..... 8.1-35
Figure 8.1-10. Directory Model ..... 8.1-40
Figure 8.1-11. Directory Use Access ..... 8.1-41
Figure 8.1-12. Key Management Infrastructure Directory Information Tree ..... 8.1-43
Figure 8.1-13. Access Control Decision Function Required for Access Control ..... 8.1-45

Figure 8.1-14. DoD Class 3 PKI Architecture ..... 8.1-57
Figure 8.1-15. FORTEZZA CMI Components ..... 8.1-75
Figure 8.1-16. Operational Activities Supported by the KMI ..... 8.1-78
Figure 8.1-17. DoD KMI System Context ..... 8.1-84
Figure 8.1-18. Nodal View of the Target KMI ..... 8.1-85
Figure 8.1-19. Breakdown of Client Nodes ..... 8.1-85
Figure 8.1-20. Federal PKI Architecture ..... 8.1-95
Figure 8.2-1. Perspectives of Layers in a Detect and Respond Infrastructure Hierarchy ... 8.2-6
Figure 8.2-2. Basic Hierarchy for Detect and Respond Infrastructure ..... 8.2-7
Figure 8.2-3. Basic View of Detect and Respond Phases ..... 8.2-9
Figure 8.2-4. Realistic View of Detect and Respond Phases ..... 8.2-10
Figure 8.2-5. Possible Allocations of Detect and Respond Functions ..... 8.2-11
Figure 8.2-6. Functions to Support Warning ..... 8.2-12
Figure 8.2-7. Functions to Support Local Incident Detection ..... 8.2-13
Figure 8.2-8. Functions to Support Incident Characterization ..... 8.2-14
Figure 8.2-9. Functions to Support Incident Response ..... 8.2-15
Figure 8.2-10. Functions to Support Attack Determination ..... 8.2-16
Figure 8.2-11. Functions to Support Attack Characterization ..... 8.2-17
Figure 8.2-12. Functions to Support Response Coordination ..... 8.2-18
Figure 8.2-13. Functions to Support Attack Investigation ..... 8.2-19
Figure 8.2-14. Detect and Respond Technologies ..... 8.2-21
Figure 8.2-15. Sensor Technologies Grouping ..... 8.2-22
Figure 8.2-16. Possible Sensor Deployment Locations ..... 8.2-25
Figure 8.2-17. Detect and Respond Technology Reference Model ..... 8.2-37

## Chapter 9

Figure 9-1. Tactical Communications Environment ..... 9-3
Figure 9-2. Tactical Communications Information Flow ..... 9-4
Figure 9-3. Interconnecting Cell Sites Using a UAV ..... 9-30
Figure 9-4. Near-Term Architecture ..... 9-36
Figure 9-5. Objective WIN Security Architecture ..... 9-36
Figure 9-6. Battlefield Video Teleconference ..... 9-44

# LIST OF TABLES

## Chapter 1

Table 1-1. Classes of Attack ..... 1-11

## Chapter 2

Table 2-1. Classes of Attack ..... 2-5
Table 2-2. Examples of Layered Defenses ..... 2-13

## Chapter 3

Table 3-1. Corresponding SE and ISSE Activities ..... 3-3
Table 3-2. Assess Information Protection Effectiveness Tasks by ISSE Activity ..... 3-15

## Chapter 4

Table 4-1. Potential Adversaries ..... 4-3
Table 4-2. Examples of Passive Attacks ..... 4-6
Table 4-3. Examples of Active Attacks ..... 4-6
Table 4-4. Examples of Close-In Attacks ..... 4-8
Table 4-5. Examples of Insider Attacks ..... 4-9
Table 4-6. Examples of Distribution Attacks ..... 4-10
Table 4-7. Degree of Robustness ..... 4-32
Table 4-8. Security Management Mechanisms ..... 4-36
Table 4-9. Confidentiality Mechanisms ..... 4-37
Table 4-10. Integrity Mechanisms ..... 4-38
Table 4-11. Availability Mechanisms ..... 4-40
Table 4-12. I&A Mechanisms ..... 4-41
Table 4-13. Access Control Mechanisms ..... 4-42
Table 4-14. Accountability Mechanisms ..... 4-43
Table 4-15. Nonrepudiation Mechanisms ..... 4-44
Table 4-16. Example Assessment Using Degree of Robustness Table ..... 4-48
Table 4-17. Application of Confidentiality Mechanisms Table for Example One ..... 4-49
Table 4-18. Use of Security Management Mechanisms Table ..... 4-50
Table 4-19. Example Assessment Using Degree of Robustness Table ..... 4-51

## Chapter 5

Table 5.3-1. Digital Service Standards ..... 5.3-3
Table 5.3-2. Characteristics of Layer 2 Protected Networks ..... 5.3-11
Table 5.3-3. Characteristics of Layer-3-Protected Networks ..... 5.3-14

## Chapter 6

Table 6.2-1a. Summary Guidance for Remote Access Direct Dial-up Access to Secret Enclave ..... 6.2-14
Table 6.2-1b. Summary Guidance for Remote Access Direct Dial-up Access to Secret Enclave ..... 6.2-15
Table 6.2-1c. Summary Guidance for Remote Access Direct Dial-Up Access to Secret Enclave ..... 6.2-16
Table 6.2-1d. Summary Guidance for Remote Access Direct Dial-up Access to Secret Enclave ..... 6.2-17
Table 6.4-1. Network-Based IDS Considerations ..... 6.4-5
Table 6.6-1. Comparison of Macro Viruses ..... 6.6-13

## Chapter 7

Table 7.1-1. Pros and Cons of GSS-API ..... 7.1-15
Table 7.1-2. Pros and Cons of CDSA ..... 7.1-15
Table 7.1-3. Pros and Cons of Cryptoki (PKCS #11) ..... 7.1-15
Table 7.2-1. Host-Based IDS Considerations ..... 7.2-6
Table 7.2-2. File Integrity Checker Considerations ..... 7.2-24

## Chapter 8

Table 8.1-1. KMI/PKI Services Support to Subscriber Categories ..... 8.1-1
Table 8.1-2. Security Applications Supported By Cryptographic Type ..... 8.1-3
Table 8.1-3. KMI/PKI Processes ..... 8.1-5
Table 8.1-4. Attacks and Countermeasures ..... 8.1-10
Table 8.1-5. Business Requirement and Security Technology Comparison ..... 8.1-96