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

CHAPTER 6

This page intentionally left blank.

LIST OF APPENDICES

This page intentionally left blank.

LIST OF FIGURES

Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Chapter 8

Chapter 9

LIST OF TABLES

Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Chapter 8