

Summary of Changes

As of September 2002

This section summarizes the changes that have been made to the framework document with each release, beginning with today's IATF Release 3.1 through the initial draft Network Security Framework (NSF) documents.

In general, with each release spelling errors are corrected and editing, formatting, and punctuation changes are made. Internet URLs and acronyms are reviewed and updated as required. Framework sections are selectively updated or new sections are added. Figures are reviewed and redrawn as needed.

Changes in IATF Release 3.1—September 2002

- Expanded on Chapter 2, Defense-in-Depth Overview, to include a new introduction highlighting the Information Assurance (IA) strategy, which focused on the following areas: adversaries, motivations, classes of attacks, and IA. The IA section of the introduction covers the importance of people, technology, and operations.
- Reorganized Chapter 3, to emphasize the three important System Engineering (SE) principles and to separate sections on each of the SE and Information Systems Security Engineering (ISSE) activities.
- Expanded on Chapter 3, Information Systems Security Engineering Process, by including a new appendix elaborating on the Discover Needs section of the chapter. The appendix provides a description of the process of determining or eliciting from customers their information protection needs, hence the appendix is titled Protection Needs Elicitation (PNE).
- Added new Section 5.4, Security for Voice Over Internet Protocol (IP).
- Revised Chapter 7, Defending the Computing Environment, with major updates to Section 7.1, Security for System Applications.

Changes in IATF Release 3.0—September 2000

- Expanded the document beyond the Department of Defense (DoD) by “nationalizing” its presentation and content.
- Revised Chapter 1, Introduction, and Chapter 2, Defense-in-Depth Objectives Overview, to directly focus on the Defense-in-Depth strategy's approach to IA.
- Expanded and renamed Chapter 3, Information Systems Security Engineering Process, to address SE, systems acquisition, risk management, certification and accreditation (C&A), and life-cycle support and to show how these methodologies relate to the ISSE activities.

UNCLASSIFIED

Summary of Changes
IATF Release 3.1—September 2002

- Reconfigured Chapter 4 to address the common technical issues of adversaries (and how adversaries act) and to provide a discussion of the primary security services. Adversaries, Threat (Motivations/Capabilities), and Attacks (IATF 2.0.1, Section 3.2.2) became elements of Chapter 4.
- Expanded and modified Chapter 6, Defend the Enclave Boundary/External Connections as follows:
 - Added Sections 6.4, Network Monitoring Within Enclave Boundaries and External Connections; 6.5, Network Scanners Within Enclave Boundaries; and 6.6, Malicious Code Protection.
 - Revised Sections 6.1, Firewall, and 6.3, Guards.
 - Moved Section 6.3, Multi-Level Security to Section 6.7.
- Added new Section 7.2, Host-Based Detect and Respond Capabilities Within Computing Environments.
- Updated Chapter 8, Supporting Infrastructure, to include both a comprehensive description of what constitutes the Key Management Infrastructure/Public Key Infrastructure (KMI/PKI) and a discussion of detect-and-respond for providing warnings, detecting and characterizing suspected cyber attacks, coordinating effective responses, and performing investigative analyses of attacks.
- Incorporated old Appendix E into Chapter 8, Supporting Infrastructure.
- Created Appendix E, Office of the Secretary of Defense (OSD) Information Assurance (IA) Policy Robustness Levels.

Changes in IATF Release 2.0.1—22 September 1999

Release 2.0.1 changes consisted mostly of formatting and graphical updates. These changes included—

- Redrawing the remaining graphics retained from Release 1.1 for greater clarity and consistency.
- Correcting some acronyms.
- Updating table formats and headings.
- Changing the page heading to “IATF Release 2.0.1—September 1999.”

Changes in IATF Release 2.0—31 August 1999

- Changed name to Information Assurance Technical Framework (IATF).
- Aligned the security solution frameworks with the four focus areas of the Defense-in-Depth strategy: Defend the Network and Infrastructure (Chapter 5), Defend the Enclave

Boundary/External Connections (Chapter 6), Defend the Computing Environment (Chapter 7), and Supporting Infrastructures (Chapter 8).

- Made System High Interconnections and Virtual Private Networks (VPN) (NSF-R1.1 Section 5.2) and Availability of Backbone Networks (NSF R1.1 Section 5.7) elements of the new Chapter 5, Defend the Network and Infrastructure.
- Made Protection for Network Access (NSF R1.1 Section 5.3), Remote Access (NSF R1.1 Section 5.4), and Multilevel Security (NSF R1.1 Section 5.5) elements of the new Chapter 6, Defend the Enclave Boundary/External Connections.
- Made Security for System Applications (NSF R1.1 Section 5.6) an element of the new Chapter 7, Defend the Computing Environment.
- Changed name of NSF R1.1 Chapter 6 Security Management Infrastructure (SMI) to Key Management Infrastructure/Public Key Infrastructure (KMI/PKI) and made it an element of the new Chapter 8, Supporting Infrastructures.
- Added a new section, Wireless Security Solutions, to Chapter 5, Defend the Network and Infrastructure.
- Added a new Chapter 9, Information Assurance for the Tactical Environment.
- Added the outline of a new section, Detect and Respond, to Chapter 8.
- Added two new appendixes: Executive Summaries (Appendix F) and Protection Profiles (Appendix G).
- Revised Chapter 1 to include an explanation of the relationship of the GNIE IA effort, the Defense-in-Depth strategy, and the IATF.
- Updated the Remote Access section.
- Added “UNCLASSIFIED” to the header and footer of every page.
- Redrew some of the graphics retained from Release 1.1 for greater clarity and consistency.

Changes in NSF Release 1.1—3 December 1998

- A (new or updated) Robustness section for Chapter 4.
- Complete revision of Sections 5.6, Security for System Applications, and 5.7, Availability of Backbone Networks.
- Inclusion of Appendix A, Abbreviations & Acronyms.
- A significantly expanded Chapter 4 focusing on security services, security robustness, and secure interoperability.

UNCLASSIFIED

Summary of Changes
IATF Release 3.1—September 2002

Changes in NSF Release 1.0—22 May 1998

- Added a new Chapter 3 focused on security methodology.
- Added a new Chapter 4 focused on security services, security robustness, and secure interoperability.
- Added two new sections within Chapter 5 focused on security for system applications and backbone availability.
- Added a new Chapter 6 focused on security management infrastructure.
- Added appendices providing a glossary and amplifying information on some of the security solutions framework.
 - Glossary (Appendix B).
 - Characterization of Customer Community (Appendix C).
 - System Security Administration (Appendix D).
 - Public Key Infrastructure (PKI) Formats (Appendix E).

The Initial Network Security Framework (NSF) Document

The first releases of the NSF (Releases 0.1 and 0.2) provided initial insight and guidance on a few categories of network security challenges. The third release (Release 1.0) provided an initial treatment of all of the primary topics that were suggested in the original outline and in the comments received.