ARMY RESEARCH LABORATORY

Information Assurance Issues and Requirements for Distributed Electronic Records Archives

by Binh Q. Nguyen

ARL-TR-2963 **April 2003**

Approved for public release; distribution unlimited.

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position, unless so designated by other authorized documents.

Citation of manufacturers' or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

Army Research Laboratory
Adelphi, MD 20783-1197

ARL-TR-2963 **April 2003**

Information Assurance Issues and Requirements for Distributed Electronic Records Archives

Binh Q. Nguyen
Computational and Information Sciences Directorate, ARL

Approved for public release; distribution unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY *(Leave Blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	April 2003	Technical Report, March–September 2002

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Information Assurance Issues and Requirements for Distributed Electronic Records Archives	N/A
6. AUTHORS Binh Q. Nguyen	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Research Laboratory ATTN: (AMSRL-CI-CN) 2800 Powder Mill Road Adelphi, Maryland 20783-1197	8. PERFORMING ORGANIZATION REPORT NUMBER ARL-TR-2963
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) National Archives and Records Administration 8601 Adelphi Road College Park, MD 20740-6001	10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE
Approved for public release, distribution unlimited.	

13. ABSTRACT *(Maximum 200 words)*

This document reports the findings of a 6-month study focused on the initial information assurance (IA) requirements for safeguarding distributed electronic records archives (ERA) in network environments capable of providing speedy communications and swift transfer of electronic records and software tools among National Archives and Records Administration (NARA) administrators and researchers. The report also includes Internet addresses of IA-related organizations that can offer NARA further information about our national strategy for safeguarding cyberspace and technical details about IA strategies and technological products.

14. SUBJECT TERMS	15. NUMBER OF PAGES
information assurance, electronic records archives	38
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-1
298-102

Contents

List of Figures **iv**

Preface **v**

Summary **1**

1. Introduction **3**

1.1 Background 3

1.2 Scope 3

1.3 Method....4

2. Distributed ERA Research Network **4**

2.1 Threats 6

2.2 Concerns 7

2.3 Requirements 7

3. Information Assurance **8**

3.1 IA Definition 8

3.2 IA Strategy 9

3.3 IA Solution 10

3.4 IA Products 10

3.5 IA Product Acquisition 13

3.6 IA Research at ARL 14

3.7 IA Summary 14

4. Conclusions and Recommendations **15**

5. References **17**

Appendix. Other Information Assurance (IA)-Related Activities **21**

Glossary **25**

List of Acronyms **27**

List of Figures

Figure 1. Initial implementation of the distributed ERA research network.....5
Figure 2. Defense in Depth strategy (*7*).....9
Figure 3. IA model *(47)* 15

Preface

The U.S. Army Research Laboratory (ARL) prepared this technical document for the U.S. National Archives and Records Administration (NARA). As the corporate research arm of the U.S. Army Materiel Command, ARL provides innovative science, technology, and analyses to enable full-spectrum operations.[1] NARA is the recordkeeper of the United States of America; it is the steward of irreplaceable electronic records collections documenting our nation's experience, the actions of government, and the rights and entitlements of our citizens.

This document reports the findings of a 6-month study focused on the initial information assurance (IA) requirements for safeguarding distributed electronic records archives in network environments capable of providing speedy communications and swift transfer of electronic records and software tools among NARA administrators and researchers. The report also includes Internet addresses of IA-related organizations that can offer NARA with further information about our national strategy for safeguarding cyberspace and technical details about IA strategies and technological products.

[1] U.S. Army Research Laboratory Strategic Plan. http://www.arl.army.mil/main/Main/ARLSTRATPLAN.pdf (accessed Feb 2003).

INTENTIONALLY LEFT BLANK.

Summary

A synopsis of information assurance (IA) issues and requirements for implementation of distributed Electronic Records Archives (ERA) is presented in this report. Information assurance is a multidimensional concept that varies over time to accommodate changes in organizational requirements and technological innovations. Capabilities assignable to future ERA are appropriately considered as the means of fulfilling the National Archives and Records Administration's (NARA's) federal requirements for authentically preserving ERA. An effective IA program for securing and protecting future ERA in transmission, storage, and processing will have to provide five essential services: (1) availability, (2) integrity, (3) authentication, (4) confidentiality, and (5) nonrepudiation by leveraging innovative technology, employing trusted experts, and ensuring that all procedures comply with organizational policies.

Information assurance is a major complex challenge that demands great efforts and commitment for ensuring the success of "Building the Archives of the Future." This study is only the initial, important step to provide the safeguards for ERA. Additional actions are required to find IA solutions for the protection of ERA.

To meet the initial IA requirements for distributed ERA, the U.S. Army Research Laboratory (ARL) recommends that NARA implement a secure, high-speed network to several geographically dispersed locations. The network should be implemented in two phases: a pilot testbed first, then later a fully functional distributed ERA environment. Understanding of IA issues and requirements for a future system of distributed repositories may potentially serve the mission interest of both ARL and NARA with a research testbed in which infrastructure issues may empirically examined and evaluated. This testbed will serve as a showcase for NARA illustrating integrated approaches for the development of ERA solutions that incorporate extendable IA components at the inception to avoid subsequent security patches.

The testbed also should demonstrate the ability of NARA to perform at least four technical areas: (1) assessing specific risks and threats to ERA and the vulnerability and interrelationships of ERA systems; (2) designing a component-based security architectural model supporting future scalable ERA architectural plans, strategies, and implementation; (3) developing ERA performance metrics for technical progress measurements and performance goals for operational readiness and business continuity; and (4) analyzing distributed ERA implementation costs, benefits, challenges, and issues associated with IA research, development, implementation, education, and training.

ARL further recommends that NARA fund the development of IA solutions that leverage research activities at ARL and partner with ARL to take advantage of its technical prowess, prudent management, and extensive and reliable connections to outstanding national universities, industry partners, and the U.S. Department of Defense (DOD) laboratories. ARL facilities are conveniently located within local commuting distance from the Archives II, College Park, MD. The ARL facilities are connected to the DOD Information Infrastructure (DII) at various security levels and to the Defense Research and Engineering Network (DREN).

INTENTIONALLY LEFT BLANK.

1. Introduction

1.1 Background

The ERA program is building the archives of the future. NARA envisions that "ERA will authentically preserve and provide access to any kind of electronic record, free from dependency on any specific hardware or software, enabling NARA to carry out its mission into the future." Electronic records are posing an enormous challenge for NARA in terms of diversity, complexity, and exponential growth in volume.[*,†]

NARA is now sponsoring several research efforts finding innovative techniques and methods for the preservation of authentic ERA. Among them is a project entitled "Presidential Electronic Records Pilot System (PERPOS)" (*3*), which is being performed at the Georgia Tech Research Institute (GTRI) in Atlanta, GA.

A major goal of NARA is to enable researchers, developers, and administrators to conveniently share information and newly developed software tools across the country using modern communications, networking, and information technologies. Communications via electronic means will enable NARA to monitor research progress and to manage ERA projects more expeditiously. Additionally, ERA researchers, developers, and administrators can collaborate, connect, coordinate, and communicate more easily through the transfer of critically needed electronic records and tools among participating entities. ERA and its processing software tools need protection; therefore, before any concrete steps toward realizing the goal of a fully connected team can be taken, NARA partnered with ARL for analyzing its requirements, identifying their associated issues, and recommending strategies that are potentially responsive to the identified requirements.

1.2 Scope

This report contains preliminary results of an ARL-conducted study focused on identifying, assessing, evaluating IA issues and requirements, and recommending strategies and technologies potentially responsive to supporting the PERPOS researchers, NARA archivists, and records administrators at several locations. The intended audience of this report includes NARA management and archivists, ERA researchers and partners, and ARL management and technical personnel. The intended purposes of this document are as follows:

- Identify major IA requirements for implementing distributed ERA.
- Explain multiple aspects of IA requirements.
- Familiarize NARA with important national IA activities, acquisition policy, and standards.
- Recommend IA solutions potentially responsive to the requirements of ERA.

[*] The scope and the vision of the ERA program can be obtained from the public Website of NARA (*1*).

[†] Further details about the challenges facing NARA and the ERA research efforts of NARA to overcome them can be found in an eloquently elucidated article entitled "Building the Archives of the Future" by Kenneth Thibodeau, the ERA program director (*2*).

- Elicit feedback and guidance from NARA for future research activities meeting requirements of IA for ERA activities.

The organization of this report follows the order of its intended purposes. The report also provides Internet addresses of IA-related sources of information for further details. The next section describes (1) a networked computing model of distributed ERA research capable of providing information sharing among geographically and organizationally different entities, (2) threats to ERA, and (3) requirements for safeguarding ERA. Section 3 discusses IA-related activities, processes, and technologies including IA definitions, strategy, solutions, technology products, and ARL research. Section 4 provides a summary of substantiated findings together with their implication to ERA and a list of recommendations for implementation and future research opportunities. Other IA-related activities and their Internet addresses are included in the Appendix.

1.3 Method

The principal investigator (PI) of this study and author of this report gathered information from available documentation, publications, and Internet Web pages of various government agencies and authoritative organizations responsible for different aspects of IA. In addition, the PI also attended many technical meetings and discussions with ERA-cognizant personnel to determine NARA-specific requirements. This research was guided by several incisive managerial and technical leaders: Mr. Robert Chadduck of NARA, the Director of Research of the ERA program; Dr. William Underwood of GTRI, the principal investigator of the PERPOS project; and R. Glenn Racine and Dr. John (Jay) Gowens of ARL, the ARL program managers and leaders of this study.

Fundamental knowledge of IA, acquisition policies and regulations, requirements and certifications, common criteria, protection profiles, standards, and the "Defense-in-Depth" strategy (see section 3.2) was obtained from their cognizant organizations: the Information Assurance Technical Framework (IATF), the Information Assurance Technology Analysis Center (IATAC), and the Computer Security Division (CSD) of the National Institute of Standards and Technology (NIST).

The knowledge of IA basic research programs was gained from studying published scholarly papers and from attending IA workshops—especially the ones sponsored and conducted by the Army Research Office (ARO) and the Computational and Information Sciences Directorate (CISD) of ARL. The purpose of the research programs was to find IA solutions that are more efficacious for the protection of national critical information infrastructure systems and of the digitized tactical communications and information networks of the U.S. Army highly mobile tactical forces (*4, 5*).

2. Distributed ERA Research Network

A model of a future distributed ERA research and development network is envisioned as a secure, high-performance network connecting geographically dispersed repositories and organizations. Present research is directed to establish appropriately secure telecommunication

capabilities enabling information sharing among ERA research administrators, partners, and collaborators who are located in different states. Other institutions, ERA creators, and ERA end users may also be securely connected in the future. Figure 1 depicts an instance of a communication scenario.

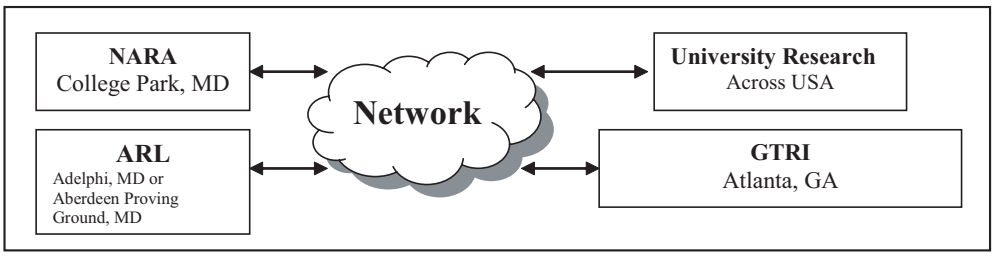

Figure 1. Initial implementation of the distributed ERA research network.

All digital communication messages traveling among the sites in Figure 1 will traverse a network, presently unspecified at the start of this study. The network will be a Wide Area Network (WAN), which may be a public network, a private network, or a virtual private network. According to Comer (*6*), a network is said to be public if it is owned and operated by a service provider similar to a telephone service; whereas, a network is said to be private if use of network is restricted to the corporate or individual owner. A private network can be privately owned or leased, and it can be isolated from any other networks and computers; thereby, it is considered a secured environment. A private network can be costly whether it is privately owned or leased, and it places the burden of ownership on its owner. On the other hand, a public network such as the Internet is shared, and thus it is relatively less expensive. All subscribers connected to the same public network can communicate with one another using computers; in so doing, every computer is physically connected. Therefore, a public network is considered an unsecured environment.

Each site presumably has its own internal network called "enterprise network" connecting its employees and departments. Each internal network consists of several subnets, each serving a particular purpose. For example, part of the enterprise network of GTRI (GTRI Net) could be a dedicated subnet for ERA research only (ERA Net), and it is tied to all other subnets of the GTRI Net. If the GTRI Net is connected to the enterprise network of the Georgia Institute of Technology (GATech Net), then every computer attached to the ERA Net is physically linked to every computer attached to the GATech Net. When the GATech Net is connected to the Internet, which provides connections to other organization's networks, then every computer connected to the GATech Net is physically connected to that organization; i.e., all computers having access to the Internet are physically connected to each other.

Egress and ingress traffic departing from and destined for the ERA subnet depend on the organizational and external networks for transportation services. Once the traffic is in the external network, it passes through the network cloud, as shown in Figure 1, to its destination. The external network cloud can be a public network, such as the Internet, providing digital data transport services for communicating parties.

2.1 Threats

Electronic records collections preserved, managed, and accessed in future ERAs will be subject to attacks everywhere in a distributed ERA network. An attack is the act of an actualized threat. Threat is potential; attack is real. The IATF (*7*) classifies five different classes of attacks: (1) passive, (2) active, (3) close-in, (4) inside, and (5) distribution.

Passive attacks generally consist of traffic analysis and eavesdropping that violate the confidentiality of ERA and ERA activities including authentication information. The potential attackers will attempt to discover the content of ERA or to identify specific communicating parties responsible for ERA activities based on the location of the ERA and on the corresponding addresses tagged in the ERA messages when they are transported across a network. Confidential information can be inferred from known corresponding addresses. Passive attacks are difficult to detect; however, a new cryptographic technology called "quantum cryptography" could be used in future ERA systems to safeguard ERA once it has been fully developed, proven, and affordable. This cryptographic technology is claimed to be mathematically unbreakable and capable of detecting eavesdropping activities (*8, 9*).

Active attacks are attempts to circumvent or break protection features, introduce malicious code, or steal or modify information. Typical active attacks include modifying data in transit, replaying, session hijacking, masquerading as authorized user/server, exploiting system-application and operating-system software, exploiting host or network trust, exploiting data execution, inserting and exploiting malicious code, exploiting protocol and infrastructure bugs, and denial of service (*7*). These deliberate attempts to impede future ERA operations will include attacks that change the content or the structure of ERA, disclose or disseminate ERA to unauthorized parties, copy ERA for unauthorized releases to unintended recipients, delay or block the movement of ERA, or deny ERA services to legitimate users.

Close-in attack is where an unauthorized individual is in physical close proximity to networks, systems, or facilities for modifying, gathering, or denying access to information. Close proximity is achieved through surreptitious entry, open access, or both (e.g., modification of data/information gathering, system tampering, and physical destruction) (*7*).

Inside attacks can be malicious or nonmalicious. Malicious insiders have the intent to eavesdrop, steal or damage information, use information in a fraudulent manner, or deny access to other authorized users. Nonmalicious attacks typically result from carelessness, lack of knowledge, or intentionally circumventing security for nonmalicious reasons such as to "get the job done." Examples of malicious inside attacks are modification of data or security mechanism, establishment of unauthorized network connections, covert channels, and physical damage/destruction; nonmalicious attacks include modification of data and physical damage/destruction (*7*).

Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks can introduce malicious code into a product such as a back door to gain unauthorized access to information or a system function at a later date (e.g., modification of software/hardware at manufacturer's facility or during distribution) (*7*).

Once a computer has been compromised, it can no longer ensure the confidentiality and the integrity of the ERA or that of itself, or it can be used as storage for illegal materials or as a launching pad for attacking other systems without the knowledge of its owner or users.

Downloading and running an executable file containing malicious code that is solicited or exhorted in an e-mail message sent to an innocent user or displayed in a Web page can cause unpredictable consequential damages to future ERA.

The threats are real, and they are a national concern. The President's Critical Infrastructure Protection Board (PCIPB) is preparing a national strategy for securing a national information infrastructure, and the board probably will have completed it by the end of 2003. The draft document entitled "The National Strategy for Secure Cyberspace" contains "a case for action" and national policies and guiding principles (*10*).

2.2 Concerns

Some of the initial concerns regarding the implementation of a future distributed ERA include the following questions:

- How can NARA be sure that sensitive ERA will be accessible and/or intelligible only to the authorized, intended recipients? This is an issue of confidentiality that future ERA must consider.
- How can remote ERA users be assured that they will be communicating with a legitimate ERA portal to transmit (upload) authentic records and that the authentic records will remain authentic at the portal for preservation and sharing purposes? These are issues of authentication and integrity that future ERA must consider.
- How can remote ERA researchers or users be reasonably assured that they will be communicating with a legitimate ERA portal to retrieve (download) authentic ERA and that the retrieved ERA will be the same as the archived records? These are issues of authentication and integrity that future ERA must consider.
- How can an ERA system know that a requester of ERA or services will be an authorized user having appropriate security clearance and NARA-granted rights and privilege? This is an issue of access-level authorization, including access within government that future ERA must consider.
- How can an ERA system confirm the claimed identity of an ERA user requesting electronic records and services? This is an issue of user-to-host authentication that future ERA must consider.
- How can an action performed on an ERA be checked for consistency with assigned requirements and tracked for accountability and historical purposes? These are issues of access-level authorization and non-repudiation that future ERA must consider.
- How can resources supporting ERA activities be made available only to authorized users with appropriate clearance-based, NARA-granted rights and privileges at any time in any place for as long as they are needed? These are issues of access-level authorization, service quality, and availability that future ERA must consider.

2.3 Requirements

NARA is the steward and public trust of irreplaceable electronic records documenting our nation's experience, the actions of government, and the rights and entitlements of our citizens.

Identified requirements for authenticity, integrity, and preservation are assigned under federal law to these collections. As considered in this report, capabilities assignable to a future ERA are appropriately considered as the means to fulfilling these requirements.

- *The genuineness of communicating entities and legitimate users will be certain*. This is about trust—a term that is difficult to define, quantitatively or unambiguously. Distributed ERA activities over a telecommunication network cannot simply rely on intuition. All participants of a communication scenario will have to mutually require a way to authenticate one another—confirming and validating the other side's presented evidence of truth; therefore, a distributed ERA environment will have to offer mutual authentication services through a secure logon system.
- ERA information will be disclosed or released only to the authorized, intended recipients; the confidentiality of ERA will be maintained. Unauthorized disclosure or release of ERA will negatively impact NARA and its mission; therefore, a distributed ERA environment will have to offer confidentiality services either through the type of network used or encryption or both.
- ERA information and system resources will be expeditiously available only for their intended ERA activities whenever and as long as they are needed. A distributed ERA environment will have to ensure the availability of expeditious and efficient services to legitimate users.
- The wholeness of ERA will be well protected—preserving the structural and informational integrity and authenticity of ERA. A distributed ERA environment will have to protect the integrity and authenticity of ERA through network protection services. An ERA system will be capable of detecting every change to the state of ERA, from the high-level attributes down to the bit level.
- Assertions in ERA-related activities will be irrefutable—enabling accountability, traceability, and nonrepudiation. All future ERA-related activities will be recorded for historical and auditing services that can provide credible evidence of ERA activities performed by an initiator; therefore, a distributed ERA environment will have to offer nonrepudiation services.

3. Information Assurance

3.1 IA Definition

The Committee on National Security System (CNSS), chaired by the DOD, formally defines information assurance as *"information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities."* Within the context of ERA, information operations are defensive actions taken to protect ERA. The CNSS sets national security policy and provides a forum for discussing policy issues; it reports directly to the PCIPB.

Information assurance addresses the concerns of users, owners, and trustees of ERA. The purpose of an IA program is to mitigate potential risks and damages; to detect, deter, and defeat potential attacks; to disrupt malicious attempts; to restore damaged ERA; and to raise awareness of risks to ERA, computing systems, and organizational and personal reputation.

3.2 IA Strategy

The DOD has developed a strategy called "Defense in Depth" based on a multilayered approach that depends on people, technology, and operations (policies and procedures) to defend four major areas: (1) network infrastructure, (2) enclave boundary, (3) computing environment, and (4) supporting infrastructure, as depicted in Figure 2.

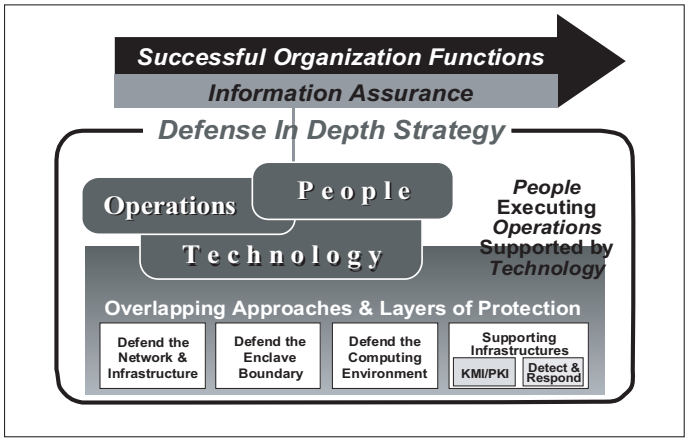

Figure 2. Defense in Depth strategy (*7*).

Defending the network and infrastructure refers to the protection of ERA from eavesdropping and modification/substitution attacks or from denial-of-service attacks or both. Thus, the confidentiality and integrity of ERA are preserved, and the availability of the network is (reasonably) assured.

Defending the enclave boundary refers to the protection of a networked ERA system at its points of entry and exit to detect intrusion and to drop or to track unauthorized egress and ingress traffic; thereby, the availability and the integrity of the system are preserved.

Defending the computing environment refers to the control of access to individual computers or a shared computing resource within an organization to deter inside attacks and to protect the system from malicious software and hardware, thereby preserving its availability and integrity.

The supporting infrastructure has two main elements: a cryptographic infrastructure and an intrusion infrastructure. The former is the enabling technology that renders IA services, and the latter provides prevention, detection, reporting, and responding services.

Details about the Defense in Depth strategy can be found in a document entitled "IATF Document 3.1" (reflecting the latest version as of September 2002) located at the IATF's Website, an IA repository sponsored by the National Security Agency (NSA) (*7*). The document

is one of the most important publications of the IATF. It covers every aspect of IA including an elaborate description of the Defense in Depth strategy. The strategy is summarized in a Critical Review and Technology Assessment (CA/TA) Report by the IATAC (*11*).

3.3 IA Solution

An IA solution developed for a future distributed ERA environment during this study emphasizes the technological aspect of the Defense in Depth strategy. It is based on IA technological products potentially responsive to immediate requirements for securing telecommunications and information infrastructure.

A secure environment for future distributed ERA will have to offer the following five basic services: (1) availability, (2) integrity, (3) authentication, (4) confidentiality, and (5) nonrepudiation. Availability services maximize operational readiness and efficiency of ERA services. Integrity services provide a means for verifying the wholeness and the authenticity of ERA against unauthorized changes. Authentication services offer a way for identifying and verifying a claimed identity of an individual or an entity. Confidentiality services enable information to be intelligible only to the intended recipients using cryptographic technologies. Confidentiality sometimes refers to privacy, which often connotes anonymity. Anonymity is an undesirable service for future distributed ERA because it will conflict with nonrepudiation services. Nonrepudiation services are rendered by employing cryptographic technologies to create trustworthy evidence that can be used to prevent an individual or an entity from a denial of having performed a particular action related to ERA. Details about IA products will be described in the subsequent sections of this report.

Current IA technologies are potentially responsive to many exigent requirements for securing distributed ERA although their performance is less than desirable due to constantly changing threats and rapid innovation of information technology, which often superannuates previously effective solutions. Desirability is a nebulous term that is always subjectively defined; therefore, IA technology implementation should include a set of metrics against which the performance, usability, and interoperability of IA products can be objectively evaluated.

3.4 IA Products

This section describes commercially available IA technological products commonly used to defend network infrastructure, enclave boundary, computing environment, and supporting infrastructure. The IATAC is the authoritative organization that can provide comprehensive assessment of IA technologies.

- *Firewall.* A firewall is usually deployed at the first line of defense, at the egress and ingress points of a computing enclave, to drop unwanted or unauthorized incoming and outgoing traffic by inspecting the corresponding addresses embedded in each packet. Firewalls can create a log of activities for subsequent auditing, traffic-analysis purposes. It should also be deployed at the user's computer to further filter out the unwanted traffic. Detailed information and product availability can be obtained from an IATAC document entitled "Firewalls" (*12–15*).
- *Intrusion Detection System (IDS).* An IDS can be categorized as network- or host-based or hybrid IDS. A network-based IDS inspects the contents of incoming packets that were allowed to enter by a firewall for signs of an attack. High-speed incoming packets can

inundate an IDS, which will have to let some packets escape its inspection. A host-based IDS analyzes system log files to determine whether an attack has occurred. A hybrid IDS does both, scanning incoming traffics and analyzing system log files, which are often very large.

Intrusion detection systems are also classified as signature- or anomaly-based detection IDS. Signature-based IDS can detect only known attacks whose signatures were identical to that of previous attacks; therefore, the signatures need to be updated regularly. An anomaly-based IDS is designed to detect new types of attacks whose behavior is considered abnormal. Deciding whether a computing activity is normal or abnormal is a very challenging task. Some of the utilized algorithms include fuzzy logic, neural network, data mining, and other statistical methods. Common issues include false alarm rate, detection accuracy, detection of novel attacks, and lack of a common baseline for evaluating and comparing the efficacy of commercial and experimental IDS products (*16*).

- *File Integrity Checker*. A file integrity checker is designed to detect changes to digital files while they are in storage and to notify the system administrator of any discrepancy, e.g., to detect an instance of a Website defacement attack. The file integrity checker is also classified as specialized IDS (*17*). One of the first file integrity checkers that remains popular is Tripwire* (*18*).
- *Virus Scanner*. A virus scanner is deployed at the last line of defense, the user's computer, to defend against malicious code capable of damaging a computer system. Popular virus scanners include McAfee VirusScan from Network Associates (*19*), Norton Antivirus from Symantec Corporation (*20*), and Trend Micro security products (*21*). One issue regarding these tools is that the database containing the known attack signatures is growing very rapidly and requires frequent updates. The IATAC has published an excellent comprehensive state-of-the-art (SOAR) report entitled "Malicious Code" which can be obtained directly from the IATAC or from the Defense Technical Information Center (*22*).
- *Vulnerability Analysis Tools*. According to an IA Tools Report by IATAC, these tools belong to one or more of the five classes: (1) simple vulnerability identification and analysis, (2) comprehensive vulnerability identification and analysis, (3) war dialers, (4) password crackers, and (5) risk analysis tools (*23*). The vulnerability identification and analysis tools are designed to known vulnerabilities of a specific operating system or an application residing in the user's computer. They also inspect system configurations and settings for possible vulnerabilities. As new vulnerabilities are discovered practically every day, the assessment mechanisms of this tool need regular updates to remain effective.
- *Network Port Scanning Tool*. This tool is a vulnerability assessment tool that automates the detection of network-computing services being offered at a particular computer by systematically scanning all the possible opening ports of a computer. For example, a publicly available network systems vulnerability audit tool called "Nessus" could be used for defending the future distributed ERA environments in the near term (*24*). Each port is associated with a number. Some ports are reserved for standard network services, and each is preassigned with a unique number. A preassigned port is known as a well-known port. For example, port 80 is designated to provide World Wide Web services, and port 25 is for

*Tripwire is a registered trademark of Tripwire Inc.

Internet mail. A list of well-known ports and network-computing services is specified in the Request for Comments (RFC) 1700 (*25*). The main use of a port scanner for defending ERA computing systems in the future will be to detect unauthorized network-computing services running in ERA-hosted systems.

- *Virtual Private Network (VPN)*. A VPN refers to a communications and computing technique that provides confidentiality services to remote users in a shared public network, e.g., the Internet. The functionality of a VPN is equivalent to that of privately owned or leased lines with lower costs (*26*).

- *Data Encryption Standard (DES), Triple DES (3DES)*. The DES is designed to preserve the confidentiality of digital data. It is a more than 20-year-old Federal Information Processing Standard (FIPS) for encrypting digital data using a secret 56-bit key. Triple DES uses three different keys in successive encryption of the data to further strengthen its effectiveness. Recipients of a DES-encrypted message must have the same key to decrypt it, or they must try one of 2^{56} possible keys. DES will be gradually replaced by the Advanced Encryption Standard although the two standards can coexist.

- *Advanced Encryption Standard (AES)*. The AES is designed to preserve the confidentiality of digital data. It is the latest FIPS for encrypting digital data using a secret key, whose sizes can be 128, 192, or 256 bits. AES is more secure than 3DES and faster than DES. Recipients of an AES-encrypted message must have the same key to decrypt it; otherwise, they would need practically an infinite amount of time and computing resources to derive the correct key, one of 2^{128} possible keys.

- *Public Key Infrastructure (PKI)*. The PKI is a secure method that relies on a trusted third party to provide the following IA services: (1) confidentiality, (2) authentication, (3) integrity, and (4) nonrepudiation. The PKI has the following main components: (1) asymmetric cryptographic method, (2) certification authority (CA), (3) digital certificates, and (4) digital signatures. The asymmetric cryptographic method is known as public/private key; the private key is kept secret, and the public key is published. Messages encrypted with the public key are decrypted only with the private key, and vice versa.

  The CA issues digital certificates containing validated, verified information of the requesters, who will use the certificates to represent themselves for subsequent identification and authentication purposes before they can obtain any services.

  Digital signatures are tied into the contents of the message that is to be signed. A digital signature is created using a combination of two cryptographic techniques: a one-way hash function and public-key encryption. The message is first computed by the hash function to produce a digest. Producing an identical digest from two different messages is practically impossible; therefore, the integrity of the message is protected. The digest is then encrypted with the signer's private key to produce a digital signature. The recipient of the signed message will then use the signer's public key to decrypt the signature then use the same hashing algorithm to compute the digest. If everything is successful, then the recipient has a reasonable assurance that the integrity and the authenticity of the message have been attained. A signed digital certificate is an identification credential that is signed

by the CA, whom both parties trust. Ford and Baum (*27*), Hellman (*28*), IATF (*7*), Menezes et al. (*29*), and Schneier (*30*) provide technical details of the PKI technology.

The Federal Public Key Infrastructure Steering Committee (FPKISC) provides a wealth of information about PKI applications in Federal Government agencies and departments (*31*).

The DOD Public Key Infrastructure Program Management Office provides information about the applications of PKI within the DOD (*32*).

- *Hypertext Transfer Protocol Over Secure Socket Layer (HTTPS)*. The HTTPS is a set of communications and public key cryptographic techniques that provide Web-server authentication and data confidentiality services over the World Wide Web. The identity embedded in the signed digital certificate of the Web server is validated by the signer of the certificate. The signer of the certificate is the trusted CA whom both parties trust. Once the authenticity of the Web server is confirmed, the Web browser generates a 128-bit secret key, encrypts it with the public key of the Web server, and then sends it to the Web server. This key is unique in each session, and hence it is called a session key. A secure connection is established when the server and the client mutually agree to use this session key to encrypt all transmitting messages traveling between two sites during the session. The session key is discarded after the session is terminated. HTTPS exists to enable electronic commerce transactions over the World Wide Web. An ERA portal can use the same technology for secure ERA activities. Easy-to-read white papers describing this technology can be obtained from VeriSign, Inc., a leading provider of secure e-commerce services (*33*). For further detailed treatment of secure e-commerce including legal topics, see the book by Ford and Baum (*27*).
- *Secure Shell (SSH)* The SSH enables secure computing services over the network such as remote login, remote system administration, and file transfer. A detailed technical description of SSH can be found at the Website of its inventor and vendor (*34*).

3.5 IA Product Acquisition

Acquisition of IA products and IA-enabled products follows the National Information Assurance Acquisition Policy, National Security Telecommunications and Information Systems Security Policy (NSTISSP) Number 11 (*35*), a critical policy component of the national IA strategy. An IA product is a security product designed specifically to provide IA services (confidentiality, integrity, authenticity, authentication, and nonrepudiation); whereas, an IA-enabled product is an information technology-functional product that can provide additional IA services. The policy requires that U.S. Government departments and agencies within the Executive Branch acquire only validated commercial-off-the-shelf (COTS) products whose claimed performance has been corroborated by a standardized evaluation process (*36*).

The Common Criteria Evaluation and Validation Scheme (CCEVS) (*37*) is a standardized evaluation process used by the National Information Assurance Partnership (NIAP), a joint initiative created by NIST and NSA. A purpose of this initiative is to evaluate COTS IA products against the Common Criteria for Information Technology Security Evaluation, an International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15408 Standard, which is often known by its shorter name, “Common Criteria” (CC) (*38*).

Other documents related to IA product acquisition include the Protection Profiles and Security Targets. A protection profile is a user-prepared document that specifies the functional requirements of an IA product. Several Protection Profiles are available at the IATF (*39*) and the NIAP (*40*) Websites. A security target is a vendor-prepared document that specifies claimed functionality provided by an IA producer. It must be submitted to NIAP before a product can go through an evaluation and validation process.

The outcome of the validation process simply states whether an IA product or an IA-enabled product performs as it is claimed. The validation process neither ranks its relative performance nor states its suitability for a particular application. Selecting the right product and training the analyst will be a near-term challenge for building a distributed ERA. Validated IA and IA-enabled products can be found at the NIAP Website (*41*).

3.6 IA Research at ARL

ARL conducts IA research at various locations in at least two different programs: network intrusion detection and critical infrastructure protection. Some information about ARL-sponsored activities is published by the U.S. Army High Performance Computing Research Center (HPCRC) located at the University of Minnesota. An ARL-sponsored project designed to detect intrusion in high-speed network is being conducted at the University of California at Santa Barbara (UCSB). The results of this research effort could be adapted for uses in future distributed ERA environments (*42, 43*).

The ARO sponsors basic IDS research in its "Modeling and Simulation Environment for Critical Infrastructure Protection (CIP)" program, a Multidisciplinary University Research Initiative (MURI) program. This ARO program includes modeling IDS, network systems vulnerability audits, case-based reasoning for CIP, and human factors in information security. Some of the technologies developed under ARL research programs can be transferred to NARA for further evaluation by experimentation in its future distributed ERA (*44*).

ARL also partners with private sectors, university, and other government laboratories through its Collaborative Technology Alliance (CTA) Program. Under this program is the Communication and Networks Alliance whose research objectives include tactical information protection that focuses on developing security technologies suitable for resource-constrained mobile, wireless networks operating in harsh environments (*45*).

3.7 IA Summary

The aspects of IA are multidimensional and vary over time. As information technologies are developed in the future, new threats will emerge, thus entailing the development of new countermeasure techniques. Maconachy et al. (*46*) have developed a three-dimensional IA model encompassing all the possible aspects of IA. Figure 3 depicts the multidimensional IA model, which is included in this report to serve as a summary of discussed IA topics and as a reference model for future research and implementation efforts.

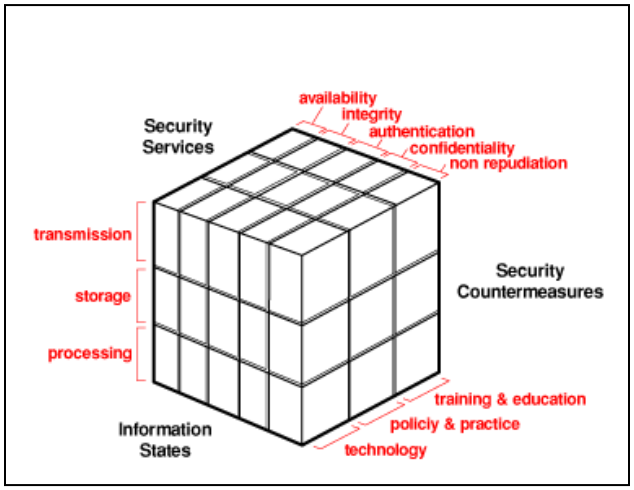

Figure 3. IA model (*47*).

An effective IA program for the protection of ERA in transmission, in storage, and in processing must provide five essential services: (1) availability, (2) integrity, (3) authentication, (4) confidentiality, and (5) nonrepudiation by leveraging innovative technology, employing trusted experts, and ensuring that all procedures comply with organizational policies.

4. Conclusions and Recommendations

This study focused on initial IA requirements for distributed ERA. By sponsoring this effort, NARA has executed its due diligence in its efforts to perform its duty of care over irreplaceable electronic records documenting our nation's experience, the actions of government, and the rights and entitlements of our citizens. NARA is also doing its part to respond to the President's call for a "National Strategy to Secure Cyberspace to ensure that America has a clear roadmap to protect a part of its infrastructure so essential to our way of life" (*10*).

Information assurance is a major complex challenge that demands great efforts and commitment for ensuring the success of "Building the Archives of the Future." This study is only the initial, important step to provide the safeguards for ERA. Additional actions are required to find IA solutions for the protection of ERA. The solutions must be efficacious over a long period, and therefore, they must be adaptable and amenable—adaptable to inevitable technological innovations and amenable to foreseeable organizational security policy changes in the future.

To meet the initial requirements of IA for distributed ERA, ARL recommends that NARA implement a secure, high-speed network to each of the geographically dispersed locations. The network should be implemented in two phases: a pilot testbed first, then later a fully functional distributed ERA environment. Understanding of IA issues and requirements for a future system of distributed repositories may potentially serve the mission interest of both ARL and NARA with a research testbed in which infrastructure issues may empirically examined and evaluated. This testbed will serve as a showcase for the ERA program of NARA. It would show an

integrated approach by incorporating information-assurance requirements in the beginning of a software development process to avoid subsequent security patches. The testbed also should demonstrate the ability of NARA to perform at least the following four technical areas:

- Assessing potential specific risks and threats to ERA and the vulnerability and interrelationships of ERA computing systems—including, but not limited to, its current infrastructure and architectural concepts, experimental and validated COTS IA products, assessing their performance, interoperability, and suitability for ERA activities.
- Studying, designing, and developing component-based security architectural models capable of supporting future scalable, evolvable distributed ERA architectural plans, strategies, and implementation.
- Developing an ERA performance metrics for technical progress measurements, and ERA performance goals for operational readiness and business continuity of a distributed ERA system supporting the efforts of authentically preserving ERA.
- Analyzing distributed ERA implementation costs and benefits as well as the challenges and issues associated with ERA IA research, development, and implementation.

ARL further recommends that NARA partner with ARL and fund the development of IA solutions that leverage research activities at ARL and its technical prowess, prudent management, and extensive and reliable connections to intellectual capital resources at outstanding national universities, industry partners, DOD laboratories, and the Defense Advanced Research Projects Agency. ARL facilities are conveniently located within local commuting distance from the Archives II, College Park, MD. The ARL facilities also have connections to the DII at various security levels and to the DREN.

5. References

1. National Archives and Records Administration. Electronic Records Archives. http://www.archives.gov/electronic_records_archives/about_era.html/ (accessed Jan 2003).
2. Thibodeau, K. Building the Archives of the Future: Advances in Preserving Electronic Records at the National Archives and Records Administration. *D-Lib Magazine* [online] **2001**, *7*; http://www.dlib.org/dlib/february01/thibodeau/02thibodeau.html (accessed Jan 2003).
3. Presidential Electronic Records Pilot System Home Page. http://perpos.gtri.gatech.edu (accessed Jan 2003).
4. U.S. Army Research Laboratory Home Page. http://www.arl.army.mil (accessed Dec 2002).
5. The Army Research Office Home Page. http://www.aro.army.mil (accessed Jan 2003).
6. Comer, D. E. *Computer Networks and Internets with Internet Applications,* 3rd ed., Prentice Hall, Inc.: New Jersey, 2001; http://netbook.cs.purdue.edu (accessed Jan 2003).
7. *Information Assurance Technical Framework Release 3.1.* Information Assurance Solutions Technical Directors, National Security Agency, Fort Meade, MD, September 2002; http://www.iatf.net/framework_docs/version-3_1/index.cfm (accessed Jan 2003).
8. Mullins, J. Making Unbreakable Code. *IEEE Spectrum Online*, May 2002; http://www.spectrum.ieee.org/WEBONLY/publicfeature/may02/code.html (accessed Feb 2003).
9. Johnson, R. C. Quantum Technology Isn't Just Sci-Fi Anymore, *Information Week*, November 7, 2002; http://www.informationweek.com/story/IWK20021107S0003 (accessed Feb 2003).
10. President's Critical Infrastructure Protection Board (PCIPB). *A National Strategy to Secure Cyberspace*, 18 September 2002; http://www.whitehouse.gov/pcipb/ (accessed Jan 2003).
11. Rothenheber, E.; Seibert S. *Defense in Depth*, Critical Review and Technology Assessment (CA/TA) Report, Information Assurance Technology Analysis Center (IATAC), Falls Church, VA, March 28, 2000; contributing editor R. Lamb.
12. Information Assurance Technical Analysis Center (IATAC). *Firewalls*, Information Assurance Tools Report, Information Assurance Technical Analysis Center (IATAC), Falls Church, VA, September 28, 2001.
13. Cheswick, W. R.; Bellovin, S. M. *Firewalls and Internet Security: Repelling the Wily Hacker*, 8th printing; Addison-Wesley: Reading, MA, 1998.

14. Wack, J.; Carnahan, J. *Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls*; NIST Special Publication 800-10, U.S. Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, November 2001; http://csrc.nist.gov/publications/nistpubs/800-10/800-10.pdf (accessed Jan 2003).

15. Wack, J.; Cutler, K.; Pole, J. *Guidelines on Firewalls and Firewall Policy*; NIST Special Publication 800-41, U.S. Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, November 2001; http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf (accessed Jan 2003).

16. Bace, R.; Bell, P. *Intrusion Detection Systems*, NIST Special Publication 800-31, U.S. Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, November 2001; http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf (accessed Jan 2003).

17. Information Assurance Technical Analysis Center. *Intrusion Detection*, Information Assurance Tools Report, Information Assurance Technical Analysis Center (IATAC), Falls Church, VA, June 15, 2001.

18. *Tripwire*; Tripwire Inc.: Portland, OR, 2002; http://tripwire.com (accessed Jan 2003).

19. McAfee Security Anti-Virus Products. http://mcafee.com/myapps/antivirus.asp (accessed Jan 2003).

20. Symantec Home Page. http://www.symantec.com (accessed Jan 2003).

21. Trend Micro Home Page. http://www.trendmicro.com/ (accessed Jan 2003).

22. Burkhar, G.; Perera, A.; Ritchey, R.; Rodriguez, E.; Steele, G.; Usher, A. *Malicious Code*, State of-the-Art Report (SOAR), Information Assurance Technology Analysis Center (IATAC), Falls Church, VA, May 14, 2002; contributing editors R. Lamb and C. McNemar.

23. Information Assurance Technical Analysis Center. *Vulnerability Analysis*, Information Assurance Tools Report, Information Assurance Technical Analysis Center (IATAC), Falls Church, VA, March 15, 2002.

24. Nessus; developed by Renaud Deraison, deraison@cvs.nessus.org; http://nessus.org (accessed Jan 2003).

25. Reynolds, J.; Postel, J. *Assigned Numbers*; The Internet Engineering Task Force (IETF), University of Southern California/Information Sciences Institute, Marina del Rey, CA, October 1994; http://www.ietf.org/rfc/rfc1700.txt (accessed Jan 2003).

26. Tyson, J. *How Virtual Private Networks Work*. http://www.howstuffworks.com/vpn.htm (accessed Jan 2003).

27. Ford, W.; Baum, M. *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption*, 2nd ed., Prentice Hall, Inc.: NJ, 2002; http://vig.prenhall.com/catalog/academic/product/1,4096,0130272760,00.html (accessed Dec 2002).

28. Hellman, M. E. An Overview of Public Key Cryptography. *IEEE Communications Magazine*, 50th Anniversary Issue, May 2002, pp 42–49.

29. Menezes, A. J.; Oorschot, P.C.; Vanstone S. A. *Handbook of Cryptography*, 5th printing; CRC Press: Boca Raton, FL, August 2001; http://www.cacr.math.uwaterloo.ca/hac (accessed Jan 2002).

30. Schneier, B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed.; John Wiley & Sons, Inc.: New York, 1996; http://www.wiley.com/cda/product/0,,0471128457,00.html (accessed Jan 2003).

31. Federal Public Key Infrastructure Steering Committee Home Page. http://www.cio.gov/fpkisc (accessed Jan 2003).

32. Public Key Infrastructure Program Management Office Home Page. http://www.c3i.osd.mil/org/sio/ia/pki/index.html (accessed Jan 2003).

33. VeriSign Free Guides and Trials. http://www.verisign.com/freeguides/index.html (accessed Jan 2003).

34. SSH Communications Security Products. http://ssh.com/products/ssh/index.html (accessed Jan 2003).

35. *National Information Assurance Acquisition Policy*; NSTISSP No. 11; National Security Telecommunications and Information Systems Security Committee, National Security Agency, Ft. Meade, MD, January 2000.

36. Fact Sheet, NSTISSP No. 11, National Information Assurance Acquisition Policy; http://www.nstissc.gov/Assets/pdf/nstissp_11.pdf (accessed Jan 2003).

37. The Common Criteria Evaluation and Validation Scheme. http://niap.nist/gov/cc-scheme/index.html (accessed Jan 2003).

38. Common Criteria…The Standard for Information Security. http://www.commoncriteria.org/ (accessed Jan 2003).

39. Information Assurance Technical Framework Forum Home Page. http://www.iatf.net (accessed Jan 2003).

40. National Information Assurance Partnership Home Page. http://www.niap.nist.gov (accessed Jan 2003).

41. Validated Products List. http://niap.nist.gov/cc-sheme/ValidatedProducts.html (accessed Jan 2003).

42. Workshop on Network Instrusion Detection. http://www.arc.umn.edu/conferences/IDS/workshop_description.html (accessed Jan 2003).

43. High Speed Intrusion Detection. http://www.cs.ucsb.edu/~rsg/HighSpeedID/index.html (accessed Jan 2003).

44. CIP Modeling and Simulation Environment for Critical Infrastructure Protection. https://quickplace.berbee.com/cip (accessed Feb 2003).

45. Collaborative Technology Alliances, Communication and Network Alliance Overview. http://www.arl.army.mil/alliances/cnnoview.htm (accessed Jan 2003).

46. Maconachy, W. V.; Schou, C. D.; Ragsdale D.; Welch D. In *A Model for Information Assurance: An Integrated Approach*, Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, June 5–6, 2001; http://www.itoc.usma.edu/ragsdale/pubs/modelPaper.pdf (accessed Jan 2003).

47. Loeb, L. *Information Assurance Powwow, Part 2: Delving Deeper into IA at the West Point Conference*, IBM DeveloperWorks, August 2001; ftp://www6.software.ibm.com/software/developer/library/s-confnotes2.pdf (accessed Jan 2003).

Appendix. Other Information Assurance (IA)-Related Activities

Below is a list of IA Websites:

The Advanced Technology Office (ATO) of the Defense Advanced Research Projects Agency (DARPA) is conducting at least three IA research programs: (1) the Information Assurance Operational Experimentation (IA OPX) program, (2) the Composable High Assurance Trusted Systems (CHATS) program, and (3) the Cyber Panel Program.

The main goals of the IA OPX program are "to accelerate fielding of advanced IA technologies and to increase feedback from operators to research community." <http://www.darpa.mil/ato/programs/opx.htm>.

The CHATS program "focus[es] on the development of the tools and technology that enable the core systems and network services to protect themselves from the introduction and execution of malicious code and other attack techniques and methods." <http://www.darpa.mil/ato/programs/chats.htm>.

The Cyber Panel program seeks to provide "capabilities to help defend mission-critical information systems by monitoring them for signs of cyber attack, and allowing operators to manage the operation of system security and survivability features to avert or counterdeveloping attack situations." <http://www.darpa.mil/ato/programs/cyberpanel.htm>.

The Purdue Center for Education and Research in Information Assurance and Security (CERIAS). The center performs multidiscipline research and education in areas of information security. <http://www.cerias.purdue.edu/>.

The Carnegie Mellon University Computer Emergency Response Team (CERT) Coordination Center (CERT/CC). Located at the Software Engineering Institute of Carnegie Mellon University, the center provides information about Internet security. It handles computer security incidents and vulnerabilities, publishes security alerts, researches long-term changes in networked systems, and develops information and training to help improve computer security." <http://www.cert.org/>.

Presidential Decision Directive 63 (PDD-63). Issued in May 22, 1998, the directive is the Clinton Administration's policy on Critical Infrastructure Protection (CIP). The directive defines critical infrastructures as "those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private." The directive states that each department and agency of the Federal Government is responsible for protecting its own critical infrastructures; especially its cyber-based infrastructure and that the Chief Information Officer (CIO) of each department and agency is responsible for IA. <http://www.ciao.gov/resource/paper598.html>.

The Critical Infrastructure Assurance Office (CIAO). The office "was created in response to a Presidential Decision Directive (PDD-63) in May 1998 to coordinate the Federal Government's initiatives on critical infrastructure assurance. The CIAO's primary areas of focus are to raise

issues that cut across industry sectors and ensure a cohesive approach to achieving continuity in delivering critical infrastructure services. CIAO's major initiatives are to coordinate and implement the national strategy, assess the U.S. Government's own risk exposure and dependencies on critical infrastructure, raise awareness and educate public understanding and participation in critical infrastructure protection efforts, [and] coordinate legislative and public affairs to integrate infrastructure assurance objectives into the public and private sectors." <http://www.ciao.gov/publicaffairs/about.html>.

The Federal Bureau of Investigation (FBI) National Infrastructure Protection Center (NIPC). The Presidential Decision Directive 63 authorizes the FBI to expand itself to a full-scale national infrastructure protection center. "Established in February 1998, the NIPC's mission is to serve as the U.S. Government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures. These infrastructures, which include telecommunications, energy, banking and finance, water systems, government operations, and emergency services, are the foundation upon which our industrialized society is based." <http://www.nipc.gov/about/about.htm>.

The Partnership for Critical Infrastructure Security (PCIS). "The mission of the Partnership is to coordinate cross-sector initiatives and complement public-private efforts to promote the assurance of reliable provisions of critical infrastructure services in the face of emerging risks to economic and national security." <http://www.pcis.org/>.

President's Critical Infrastructure Protection Board (PCIPB). "President Bush directed the development of a National Strategy to Secure Cyberspace to ensure that America has a clear roadmap to protect a part of its infrastructure so essential to our way of life." <http://www.whitehouse.gov/pcipb/>.

Executive Order 13231—Critical Infrastructure Protection in the Information Age, October 16, 2001. <http://www.ciao.gov/resource/eo13231.html>.

National Infrastructure Advisory Committee (NIAC). "Established by Executive Order 13231, NIAC will make recommendations regarding the security of the cyber and information systems of the United States' national security and economic critical infrastructures. The Committee will also examine ways that partnerships between the public and private sectors can be enhanced to improve cyber security." <http://www.whitehouse.gov/news/releases/2002/09/20020918-12.html>.

Committee on National Security Systems (CNSS). "Under Executive Order (E.O.) 13231 of October 16, 2001, Critical Infrastructure Protection in the Information Age, the President has redesignated the National Security Telecommunications and Information Systems Security Committee (NSTISSC) as the Committee on National Security Systems (CNSS). The Department of Defense continues to chair the committee under the authorities established by NSD-42. As a standing committee of the President's Critical Infrastructure Protection Board, the CNSS reports fully and regularly on its activities to the Board. <http://www.nstissc.gov/>.

National Security Telecommunications and Information Systems Security Committee (NSTISSC) No. 4011. The instruction provides a minimum training standard for information systems security (INFOSEC) professionals, 20 June 1994. <http://www.nstissc.gov/Assets/pdf/4011.pdf.>

The Information Resources Management College (IRMC) of the National Defense University (NDU) offers a training program compliant with the Standard for Information Systems Security Professionals NSTISSI No. 4011. <http://www.ndu.edu/irmc/nstissi.html>.

National Security Telecommunications and Information Systems Security Committee (NSTISSC) Policy No. 11. The policy requires that U.S. Department of Defense (DOD) agencies handling national security data acquire certified IA and IA-enabled products. <http://www.nstissc.gov/Assets/pdf/nstissp_11.pdf>.

The Information Assurance Technology Analysis Center (IATAC). Operated by the DOD, the IATAC publishes highly useful and practical information for defending a networked computing system. IA documents can be ordered or downloaded from <http://iac.dtic.mil/iatac/products/products.htm>.

Information Assurance Support Environment (IASE). Operated by the DOD, the IASE offers free IA training to Government and DOD. Its most famous products are CD-ROM- and Web-based IA training courses. Further information about the training materials can be obtained from its Website: <http://iase.disa.mil/index2.html>.

National Security Agency (NSA)-Validated Information Assurance (IA) Products. "Products which have not only been validated against Common Criteria Security Targets under the Common Criteria International Mutual Recognition Arrangement (MRA) and listed on the NIAP Validated Products List, but which also have been determined to be compliant with Protection Profiles (PP) or Security Targets (ST) certified by NSA as appropriate for use in "national security" systems consistent with the environments specified in the PP or ST." <http://www.radium.ncsc.mil/tpep/epl/cc_st.html>.

Information Assurance Technical Framework (IATF). The framework is "an NSA-sponsored outreach activity created to foster dialog among U.S. Government agencies, U.S. industry, and U.S. academia seeking to provide their customers solutions for IA problems." <http://www.iatf.net/>.

The Defense-Wide Information Assurance Program. "The Office of the Secretary of Defense (OSD) mechanism to plan, monitor, coordinate, and integrate IA activities." <http://www.c3i.osd.mil/org/sio/ia/diap/faq.html>.

Interagency Operations Security (OPSEC) Support Staff (IOSS). "The primary mission of the Interagency OPSEC Support Staff is to act as a consultant to other U.S. government departments and agencies, providing technical guidance and assistance that will result in self-sufficient OPSEC programs throughout government and the protection of U.S. operations" <http://www.ioss.gov/>.

The Navy Information Systems Security (INFOSEC). This Website is a good place for finding out information about cryptographic equipment, acquisition procedure, and price list: <https://infosec.navy.mil/PRODUCTS/CRYPTO/>.

The SysAdmin, Audit, Network, Security (SANS) Institute. The SANS Institute provides practical advice and training for system administrators and other information system professionals. More details about the institute can be obtained from its Web site <http://www.sans.org/aboutsans.php>.

International Information Systems Security Certification Consortium, Inc (ISC2). The ISC2 provides the Certified Information Systems Security Professional (CISSP) and Systems Security Certified Practitioner (SSCP) certification examinations <http://www.isc2.org/>.

National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC). "The mission of the center is to improve information systems security by developing cryptographic standards and applications, testing security products, performing security research, developing security management and guidance, and providing support for information technology security awareness and education" <http://csrc.nist.gov/>.

Glossary

Information assurance (IA) terminologies used in this report have specific meanings as defined by the National Security Telecommunications and Information Systems Security Committee (NSTISSC).[1] Some of these terms are described below:

Access: Opportunity to make use of an information system (IS) resource.

Access Level: Hierarchical portion of the security level used to identify the sensitivity of IS data and the clearance or authorization of users. Access level, in conjunction with the nonhierarchical categories, forms the sensitivity label of an object.

Accountability: Process tracing IS to a responsible source.

Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Authorization: Access privileges granted to a user, program, or process.

Attack: Type of incident involving the intentional act of attempting to bypass one or more security controls of an IS.

Availability: Timely, reliable access to data and information services for authorized users.

Back door: Hidden software or hardware mechanism used to circumvent security controls. Synonymous with trap door.

Communication Security (COMSEC): Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission, security, emission security, and physical security of COMSEC material.

Confidentiality: Assurance that information is not disclosed to unauthorized persons, processes, or devices.

Countermeasure: Action, device, procedure, technique, or other measure that reduces the vulnerability of an IS.

Information System (IS): The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information.

Information System Security (INFOSEC and/or ISS): Protection of IS against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

[1] *National Information Systems Security (INFOSEC) Glossary*; NSTISSI No. 4009; National Security Agency, Ft. Meade, MD, September 2000; http://www.nstissc.gov/Assets/pdf/4009.pdf (accessed Jan 2003).

Integrity: Quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

Nonrepudiation: Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

Operations Security (OPSEC): Process denying information to potential adversaries about capabilities and/or intentions by identifying, controlling, and protecting unclassified generic activitites.

Sensitive Information: Information, loss, misuse, or unauthorized access to or modification of, which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act),[2] but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (Systems that are not national security systems, but contain sensitive information, are to be protected in accordance with the requirements of the Computer Security Act of 1987.[3])

Threat: Any circumstance or event with the potential to adversely impact an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

Traffic Analysis: Study of communications patterns.

---

[2] Public information; Agency rules, opinions, orders, records, and proceedings. *U.S. Code*, Section 552a, Title 5.

[3] The Computer Security Act of 1987. Public Law 100-235, (H.R. 145), 1987.

List of Acronyms

AES	Advanced Encryption Standard <http://cs-www.ncsl.nist.gov/publications/fips/fips197/fips-197.pdf>
ARL	U.S. Army Research Laboratory <http://www.arl.army.mil>
ARO	U.S. Army Research Office <http://www.aro.army.mil/>
CA	Certification Authority
CA/TA	Critical Review and Technology Assessment
CC	Common Criteria <http://www.commoncriteria.org>
CNSS	The Committee on National Security System, previously known as NSTISSI <http://www.nstissc.gov/>
DARPA	Defense Advanced Research Projects Agency <http://www.darpa.mil>
DES	Data Encryption Standard <http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>
DII	DOD Information Infrastructure
DOD	U.S. Department of Defense <http://www.dod.mil>
DREN	Defense Research and Engineering Network
ERA	Electronic Records Archives <http://www.archives.gov/electronic_records_archives>
FBI	Federal Bureau of Investigation <http://www.fbi.gov/>
FIPS	Federal Information Processing Standard
GTRI	Georgia Tech Research Institute <http://www.gtri.gatech.edu/>
IA	Information Assurance
IASE	Information Assurance Support Environment <https://iase.disa.mil/>
IATF	Information Assurance Technical Framework <http://www.iatf.net>

IATAC	The Information Assurance Technology Analysis Center <http://iac.dtic.mil/iatac>
IDS	Intrusion Detection System <http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf>.
IOSS	Interagency OPSEC Support Staff <http://www.ioss.gov/>
NARA	National Archives and Records Administration <http://www.archives.gov>
NIPC	The FBI National Infrastructure Protection Center <http://www.nipc.gov/about/about.htm>
NIST	The National Institute of Standards and Technology <http://www.nist.gov>
NSA	The National Security Agency <http://www.nsa.gov>
NSTISSI	National Security Telecommunications and Information Systems Security Instruction <http://www.nstissc.gov/>
OPSEC	Operations security
PCIPB	The President's Critical Information Protection Board <http://www.whitehouse.gov/pcipb/>
PERPOS	Presidential Electronic Records Pilot System <http://perpos.gtri.gatech.edu/>
PKI	Public Key Infrastructure