Applying Security Practices to Justice Information Sharing

March 2004
Version 2.0

Global Justice Information Sharing Initiative
Security Working Group
www.it.ojp.gov/global

This document was prepared under the leadership, guidance, and funding of the Bureau of Justice Assistance (BJA), Office of Justice Programs, U.S. Department of Justice, in collaboration with the Global Justice Information Sharing Initiative. The opinions, findings, and conclusions or recommendations expressed in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Acknowledgements

Applying Security Practices to Justice Information Sharing was developed through a collaborative effort of the Security Working Group of the Global Justice Information Sharing Initiative (Global), Office of Justice Programs (OJP), United States Department of Justice (DOJ).

Global aids its member organizations and the people they serve through a series of important initiatives. These include the facilitation of Global Working Groups. The Global Security Working Group (GSWG) is one of four various Global Working Groups covering critical topics such as intelligence, privacy, and standards.

The focus of the GSWG is on the trusted and secure information exchange among justice agencies. Security of the entire information exchange enterprise is only as strong as the weakest link. The GSWG pursues security measures necessary for today's enhanced information sharing abilities.

This document is the product of Global and its membership of justice practitioners and industry professionals. Therefore, a special thank-you is expressed to the Global Security Working Group and its members for developing and contributing to this document.

Mr. Bob Brinson, Chief Information Officer, Information Resources, North Carolina Department of Corrections, Raleigh, North Carolina

Mr. Steve Correll, Executive Director, National Law Enforcement Telecommunication System, Phoenix, Arizona

Mr. Fred Cotton, Training Services Director, SEARCH, The National Consortium for Justice Information and Statistics, Sacramento, California

Randy Doucet, Esquire, Tribal Attorney, Coushatta Tribe of Louisiana, LeBlanc, Louisiana

Mr. Ken Gill, Technology Advisor, Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, Washington, DC

Mr. Philippe Guiot, Vice President, IT Services and Products, American Association of Motor Vehicle Administrators, Arlington, Virginia

Alan Harbitter, Ph.D., Chief Technology Officer, PEC Solutions, Inc., Fairfax, Virginia

Mr. Joseph Hindman, Police Technology Director, Scottsdale Police Department, Scottsdale, Arizona

Mr. Clay Jester, Director, Information Systems Group, Institute for Intergovernmental Research, Tallahassee, Florida

Mr. John Loverude, Chairman, Joint Task Force on Rap Sheet Standardization, Illinois State Police, Springfield, Illinois

Mr. George March, Director, Office of Information Technology, Regional Information Sharing Systems, Thorndale, Pennsylvania

Ms. Lora Mellies, Systems Security Officer, Division of Information Technology, Missouri Office of the State Courts Administrator, Jefferson City, Missouri

Mr. Charles Pruitt, Assistant Director, Arkansas Crime Information Center, Little Rock, Arkansas

Table of Contents

Acknowledgements ..... **i**

Foreword ..... **xiii**

Global Justice Information Sharing Initiative (Global) ..... **xv**

Global Mission and Guiding Principles xv
Global Structure: Membership, Leadership, and Working Groups xvi
Global Web Site—www.it.ojp.gov xviii

How to Use This Document ..... **xix**

Executives, Managers, and Policymakers xix
Justice, Courts, and Public Safety Practitioners; Information System Owners; and Security Information Officers xx

Chapter 1: Security Considerations **1-1**

Introduction 1-1
Security Architecture 1-3
Security Foundation 1-3
Related Resources 1-5

Chapter 2: Security Disciplines **2-1**

Introduction 2-1
Chapter Structure 2-2
Security Disciplines 2-3

Objective 1: Support **2-7**

1-1: Governance **2-9**

Description 2-9
Purpose 2-9
Principles 2-9
Best Practices 2-9
References 2-10

1-2: Physical Security **2-11**

Description 2-11
Purpose 2-11
Principles 2-11
Policies 2-11
Best Practices 2-12

Secure Desktop Workstations 2-17
Remote Workstations 2-17

References 2-18

1-3: Personnel Security Screening 2-19

Description 2-19
Purpose 2-19
Principles 2-19
Policies 2-20
Best Practices 2-20

Step One: Determine the Appropriate Screening Requirements 2-20
Step Two: Identify Required Checks 2-20
Step Three: Obtain Consent 2-21
Step Four: Process the Required Checks 2-21
Step Five: Evaluate the Results of Required Checks 2-22
Step Six: Grant or Deny Access 2-22
Step Seven: Brief the Screened Person 2-22

References 2-22

1-4: Separation of Duties 2-23

Description 2-23
Purpose 2-23
Principles 2-23
Policies 2-23
Best Practices 2-23
Reference 2-24

Objective 2: Prevention 2-25

2-1: Identification and Authentication 2-27

Description 2-27
Purpose 2-27

Principles 2-27
Policies 2-28
Best Practices 2-28

Something You Know: Passwords 2-29
Something You Have: Token Devices and Smart Cards 2-29
Something About Yourself: Biometrics 2-30
Authentication Servers and Single Logon 2-33

References 2-34

2-2: Authorization and Access Control 2-35

Description 2-35
Purpose 2-35
Principles 2-35
Policies 2-35
Best Practices 2-36

Mandatory Access Control (MAC) 2-36
Discretionary Access Control (DAC) 2-36
Role-Based Access Control (RBAC) 2-37
Lightweight Directory Access Protocol (LDAP) 2-37
Security Assertion Markup Language (SAML) 2-38

References 2-38

2-3: Data Integrity 2-39

Description 2-39
Purpose 2-39
Best Practices 2-39

System Failures, Communications, and Program Threats 2-39
Unintentional Human Threats 2-39
Intentional Human Threats 2-40
External Human Threats 2-40
Internal Human Threats 2-41
Prevention and Recovery 2-41

References 2-42

2-4: Data Classification 2-43

Description 2-43
Purpose 2-43
Principles 2-43

Policies 2-44
Best Practices 2-44
References 2-47

2-5: Change Management 2-49

Description 2-49
Purpose 2-49
Principles 2-49
Policies 2-50

Access Control Policy 2-50
Documentation Policy 2-50
Change Request Procedure 2-50
Audit Plan 2-50

Best Practices 2-50
Samples of Best Practices 2-51
Reference 2-51

2-6: Public Access, Privacy, and Confidentiality 2-53

Description 2-53
Purpose 2-54
Principles 2-54
Policies 2-54
Best Practices 2-55

Public Access 2-55
Privacy Principles 2-55

References 2-58

2-7: Firewalls, VPNs, and Other Network Safeguards 2-59

Description 2-59
Purpose 2-59
Principles 2-59
Policies 2-59
Best Practices 2-60

Firewalls 2-60
Virtual Private Networks (VPNs) 2-61
Antivirus Software 2-62

References 2-63

Objective 3: Detection and Recovery 2-65

3-1: Intrusion Detection System (IDS) 2-67

Description 2-67
Purpose 2-67
Principles 2-68
Policies 2-68
Best Practices 2-68
References 2-69

3-2: Critical Incident Response 2-71

Description 2-71
Purpose 2-71
Principles 2-71
Policies 2-72
Best Practices 2-72

Central Response Team (CRT) 2-73
Organizational Responsibilities 2-73
Help Desk Responsibilities 2-73
Phases of Response 2-73
Levels of Incidents 2-75
Central Response Team (CRT) Roles and Responsibilities 2-76

Reference 2-77

3-3: Security Auditing 2-79

Description 2-79
Purpose 2-79
Principles 2-79
Best Practices 2-80

Project Preparation 2-80
Information Gathering 2-80
Reporting 2-80
Remediation 2-80

References 2-81

3-4: Disaster Recovery and Business Continuity 2-83

Description 2-83
Purpose 2-83
Principles 2-83

Policies 2-84
Best Practices 2-84

Disaster Recovery Team 2-84
Threat/Risk Assessment 2-84
Business Impact Analysis (BIA) 2-85
Mitigation of Risks 2-86
Hardware Redundancy 2-86
Software Redundancy 2-87
Plan Development 2-88
Testing the Plan 2-88
Plan Maintenance 2-88

References 2-88

Chapter 3: Models for Justice Information Sharing 3-1

Introduction 3-1
Chapter Structure 3-2
Guidelines for Applying Information Security Practices 3-2
Current Information Sharing Systems and Their Relationship to Each Model 3-2

Justice Information Sharing Models 3-5

The Joint Task Force (JTF) Model 3-7

Introduction 3-7
Security Guidelines for the Joint Task Force (JTF) Model 3-8
Joint Task Force Disciplines 3-11

Identification and Authentication 3-11
Authorization and Access Control 3-11
Security Auditing 3-11
Intrusion Detection Systems 3-11
Data Classification 3-12
Physical Security 3-12
Critical Incident Response 3-13
Disaster Recovery and Business Continuity 3-13
Public Access, Privacy, and Confidentiality 3-13

The Centralized Information Repository (CIR) Model 3-15

Introduction 3-15
Security Guidelines for the Centralized Information Repository (CIR) Model 3-17
Centralized Information Repository Disciplines 3-18

Physical Security 3-18
Identification and Authentication 3-19
Authorization and Access Control 3-19
Data Classification 3-19
Public Access, Privacy, and Confidentiality 3-20
Firewalls, VPNs, and Other Network Safeguards 3-20
Critical Incident Response 3-20
Disaster Recovery and Business Continuity 3-21

Operational Examples of the Centralized Information Repository (CIR) Model 3-21

FBI CJIS/NCIC Case Study 3-21

The Peer Group (PG) Model 3-31

Introduction 3-31
Security Guidelines for the Peer Group (PG) Model 3-32
Peer Group Security Disciplines 3-35

Personnel Security 3-35
Firewalls, VPNs, and Other Network Safeguards 3-35
Critical Incident Response 3-36
Physical Security 3-36
Identification and Authentication 3-37
Authorization and Access Control 3-37
Data Classification 3-38
Public Access, Privacy, and Confidentiality 3-38
Intrusion Detection 3-38
Security Auditing 3-39
Disaster Recovery and Business Continuity 3-39

Operational Examples of the Peer Group (PG) Model 3-39

Arizona COPLINK 3-39
Wisconsin Integrated Justice Information Sharing 3-40

The Justice Interconnection Services Network (JISN) Model 3-41

Introduction 3-41
Security Guidelines for the Justice Interconnection Services Network (JISN) Model 3-43
Justice Interconnection Services Network (JISN) Disciplines 3-44
Firewalls, VPNs, and Other Network Safeguards 3-44
Critical Incident Response 3-45
Physical Security 3-45

Identification and Authentication 3-45
Authorization and Access Control 3-45
Data Classification 3-46
Public Access, Privacy, and Confidentiality 3-46
Intrusion Detection 3-46
Security Auditing 3-46
Disaster Recovery and Business Continuity 3-47

Operational Examples of the Justice Interconnection Services Network (JISN) Model 3-47

National Law Enforcement Telecommunication System (NLETS) 3-47
Regional Information Sharing Systems (RISS) 3-50
AAMVAnet Case Study 3-54

Appendix A: Glossary of Security Acronyms and Terminology A-1

Appendix B: Bibliography B-1

Tables

Table 2-1: Information Security Disciplines 2-3
Table 2-2: Sample Access Control List 2-36
Table 2-3: Confidentiality Classification 2-45
Table 2-4: Integrity Classification 2-46
Table 2-5: Availability Classification 2-47
Table 2-6: Security Incident Levels and Responses 2-75
Table 3-1: Operational Examples of the Justice Information Sharing Models 3-3
Table 3-2: Sample Roles and Privileges 3-38

Figures

Figure 1-1: Security Intrusion Incidents 1-2
Figure 1-2: A Model for Security Architecture 1-5

Figure 2-1: Site-to-Site VPN 2-61
Figure 2-2: Antivirus Software Pattern Searching 2-63
Figure 3-1: The Joint Task Force Model 3-7
Figure 3-2: Security Practices to Support Information Flow Into the Joint Task Force Model 3-9
Figure 3-3: The Central Information Repository Model 3-15
Figure 3-4: Security Practices to Support Information Flow Into the Central Information Repository Model 3-17
Figure 3-5: Federal Bureau of Investigation CJIS System of Systems 3-24
Figure 3-6: The Peer Group Model 3-31
Figure 3-7: Security Practices to Support a Query and Update in the Peer Group Model 3-34
Figure 3-8: Security Practices to Support Notifications in the Peer Group Model 3-34
Figure 3-9: The Justice Interconnection Services Network Model 3-41
Figure 3-10: Security Practices to Support Brokered Information Flow Into the Justice Interconnection Services Network Model 3-43

Foreword

Modern justice agencies rely heavily upon their information technology resources to perform critical tasks and to provide emergency services to the public. Increasingly, justice agencies share information across wide area networks and the Internet. The sensitivity of this information and its related systems infrastructure make it a particularly vulnerable target. The core components of these information technology resources are so critical that disabling any single resource could potentially incapacitate the mutually dependent and interconnected systems. Disruption or intentional corruption of the information justice systems can have a dramatic impact upon our organizations and the society we serve. It must be recognized that justice information technology systems are a vital part of the nation's critical infrastructure, and as such, information technology infrastructure requires comprehensive security architecture. Protecting this critical resource is not just a matter of operational good sense; it is increasingly a matter of national security and public safety.

Security should be a core foundation of any information system and is best implemented during the design of any given system. Security can and should be successfully applied to existing systems as well. Security cannot be ignored.

The purpose of this document is to educate justice executives and managers on good, basic, foundational security practices that they can deploy within their enterprise and between multiple enterprises.

> ***"Information security within the justice discipline has never been more important than it is today: not only in how it can protect the data or systems, but how it can enhance secure information exchange between trusted partners."***
>
> ***Steve E. Correll***
> ***National Law Enforcement Telecommunication System***

The long-term goal is to enable an environment of electronic trust among law enforcement and justice organizations. Electronic trust will be engendered if each organization can be assured that all parties with access to shared information follow certain minimum practices to safeguard that information. An environment of electronic trust is a minimum requirement for us to begin to fulfill the national priority of sharing information and improving the safety of the country.

Global Justice Information Sharing Initiative (Global)

Global Mission and Guiding Principles

The Global mission is to improve the administration of justice and protect the nation's public by promoting practices and technologies for the secure sharing of justice-related information.

The guiding principles of Global are to:

- Bring together representatives from the entire justice community and related entities—including private industry—to overcome the barriers to justice information sharing across agencies, disciplines, and levels of government.
- Promote the development and implementation of standards that facilitate seamless exchange of information among justice and related systems.
- Provide information that supports sound business decisions for the planning, design, and procurement of cost-effective, interoperable information systems.
- Promote constitutional values and individual rights by ensuring the accuracy and security of justice information and the implementation of appropriate privacy safeguards.
- Recommend concepts that leverage existing infrastructure, capabilities, and functionality.

Global operates under the auspices of the Office of Justice Programs (OJP), U.S. Department of Justice (DOJ), and advises the federal government—specifically through the Assistant Attorney General, OJP, and the U.S. Attorney General—in facilitating standards-based electronic information exchange throughout the justice and public safety communities. The broad scope of the effort is fundamental, because public and practitioner safety is best secured when all players—from patrol officers to prosecutors and from court officials to corrections personnel—have access to timely and accurate information.

Global operates in accordance with Federal Advisory Committee Act (FACA) provisions and convenes twice a year in Washington, DC. Meetings are announced in the *Federal Register,* and the public are welcome as observers.

Global Structure: Membership, Leadership, and Working Groups

The Global Advisory Committee (GAC) is comprised of key personnel from local, state, tribal, federal, and international justice and public safety entities and includes agency executives and policymakers; automation planners and managers; information practitioners; and, most importantly, end users. This last group distinguishes the GAC as a committee whose members remain actively dedicated to information sharing, precisely because they continue to be producers, consumers, and administrators of crucial justice-related data.

Committee membership reflects the fundamental GAC tenet that the entire justice, public safety, and courts community must be involved in information exchange. Representatives from the following entities serve as members:

- Administrative Office of the U.S. Courts
- American Association of Motor Vehicle Administrators
- American Correctional Association
- American Probation and Parole Association
- Conference of State Court Administrators
- Criminal Justice Information Services Advisory Policy Board
- Executive Office for the United States Attorneys
- Federal Bureau of Investigation – Criminal Justice Information Services Division
- International Association of Chiefs of Police
- International Association of Chiefs of Police – Division of State and Provincial Police
- International Association of Chiefs of Police – Indian Country Law Enforcement Section
- INTERPOL–USNCB
- Major Cities Chiefs Association
- National Association for Court Management
- National Association of Attorneys General
- National Association of State Chief Information Officers
- National Center for State Courts
- National Conference of State Legislatures
- National Congress of American Indians
- National Council of Juvenile and Family Court Judges
- National Criminal Justice Association
- National District Attorneys Association
- National Governors Association
- National Law Enforcement Telecommunication System
- National Legal Aid & Defender Association
- National Sheriffs' Association
- SEARCH, The National Consortium for Justice Information and Statistics

- U.S. Department of Homeland Security
- U.S. Department of Justice – Justice Management Division
- U.S. Department of the Treasury
- U.S. Drug Enforcement Administration

GAC working groups, comprised of committee members and other subject-matter experts expand the GAC's knowledge and experience. These groups are formed around timely issues impacting justice information sharing and meet as often as necessary. The following working groups are engaged in targeted activities on behalf of the GAC:

- **Global Security Working Group**—The Global Security Working Group was formed in recognition of the fact that the security of the entire justice information exchange enterprise is only as strong as the weakest link. Of particular importance is the determination of effective security guidelines for legacy systems, as well as the new and enhanced networks and systems to which they are joined. The goal of this working group is to inform the justice and justice-related communities about acceptable integrated justice system security measures, encouraging them to adopt security guidelines that have been reviewed to ensure trusted partnerships and data integrity.

- **Global Privacy and Information Quality Working Group**—The Global Privacy and Information Quality Working Group was formed because of the growing need to address information privacy as impacted by advancing technological capabilities. Goals of this working group include assisting governments in ensuring that personal information will not be inappropriately disseminated or misused; ensuring that there are safeguards against the collection and use of inaccurate information—particularly when the information is disseminated in open environments such as Internet-based systems; and improving the reliability of criminal records in an integrated electronic system.

- **Global Intelligence Working Group**—The Global Intelligence Working Group was formed to examine and integrate into the GAC dialogue the particular challenges to intelligence sharing. This working group has developed a *National Criminal Intelligence Sharing Plan*—a formal intelligence sharing initiative that will securely link local, state, tribal, and federal law enforcement agencies, facilitating the exchange of critical intelligence information. This Plan contains model policies and standards and describes a nationwide network that will link all levels of law enforcement personnel, including officers on the street, intelligence analysts, unit commanders, and police executives. In October 2003, U.S. Attorney General John Ashcroft approved the Plan.

- **Global Infrastructure/Standards Working Group**—The Global Infrastructure/Standards Working Group was formed because successful broadscale data exchange is greatly facilitated by (if not dependent on) the development and adoption of standards that enable transparent integration of disparate systems. The goal of this working group is to define a framework that will assist government entities in establishing an operational environment

that will enable them to share justice information within the guiding principles of the GAC. The framework will be designed to identify those critical components, programmatic and technical, necessary to develop and maintain a sound infrastructure.

Global Web Site—www.it.ojp.gov

The Web site provides information about Global and other important information technology initiatives. The Web site is in response to the need for additional information sharing resources throughout justice and public safety communities. This valuable online tool offers resources that support information sharing at all levels of government.

How to Use This Document

Executives, Managers, and Policymakers

Executives and managers should use this document as a resource to secure critical justice information systems and as a resource of ideas and best practices to consider in building their agency's information infrastructure. Security should also be considered before sharing information with other agencies in order to develop compatible security policies. For example, agencies such as the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) and the National Law Enforcement Telecommunication System (NLETS) have minimal standards required before they allow access to their information systems. This document is not designed to replace or reduce those minimal standards but rather to enhance them where applicable.

This document contains background information, overviews of best practices, and guidelines for secure information sharing. Fifteen disciplines have been identified—governance; physical security; personnel security screening; separation of duties; identification and authentication; authorization and access control; data integrity; data classification; change management; public access, privacy, and confidentiality; firewalls, virtual private networks (VPNs), and other network safeguards; intrusion detection systems; critical incident response; security auditing; and disaster recovery and business continuity—that span the important elements of an information security architecture.

> ***"There is a strong need for information security in justice applications."***
>
> ***Fred Cotton***
> ***SEARCH, The National Consortium for Justice Information and Statistics***
> ***Training Services Director***

This document is not intended to suggest a standard security approach, nor is it intended to provide an in-depth security solution for any particular system. It is also not intended to provide detailed technical reference for system administrators.

Many of these suggested practices are low-cost in that they require users to be educated about security practices and suggest awareness and evaluation of the security threat. Other practices require capital investment and continued maintenance to ensure their effectiveness. However, doing nothing can have unacceptable associated costs.

Justice, Courts, and Public Safety Practitioners; Information System Owners; and Security Information Officers

A security architecture should be developed by justice, courts, and public safety practitioners; information system owners; and security information officers that addresses the three fundamental service areas—Confidentiality, Integrity, and Availability (see Chapter 1, "Security Considerations," for more information)—and includes automated, procedural, and physical security safeguards. In addition to these service areas, there are three overarching security discipline objectives: Support, Prevention, and Detection and Recovery. Managers should also consider these in layered security architecture to provide security protection across the multiple security disciplines and to establish security services that satisfy justice information technology requirements (see Security Architecture found in Chapter 1, "Security Considerations," for more information). At minimum, practitioners should review their overall security architecture to ensure that the fifteen security disciplines have the appropriate security practices applied.

Chapter 1: Security Considerations

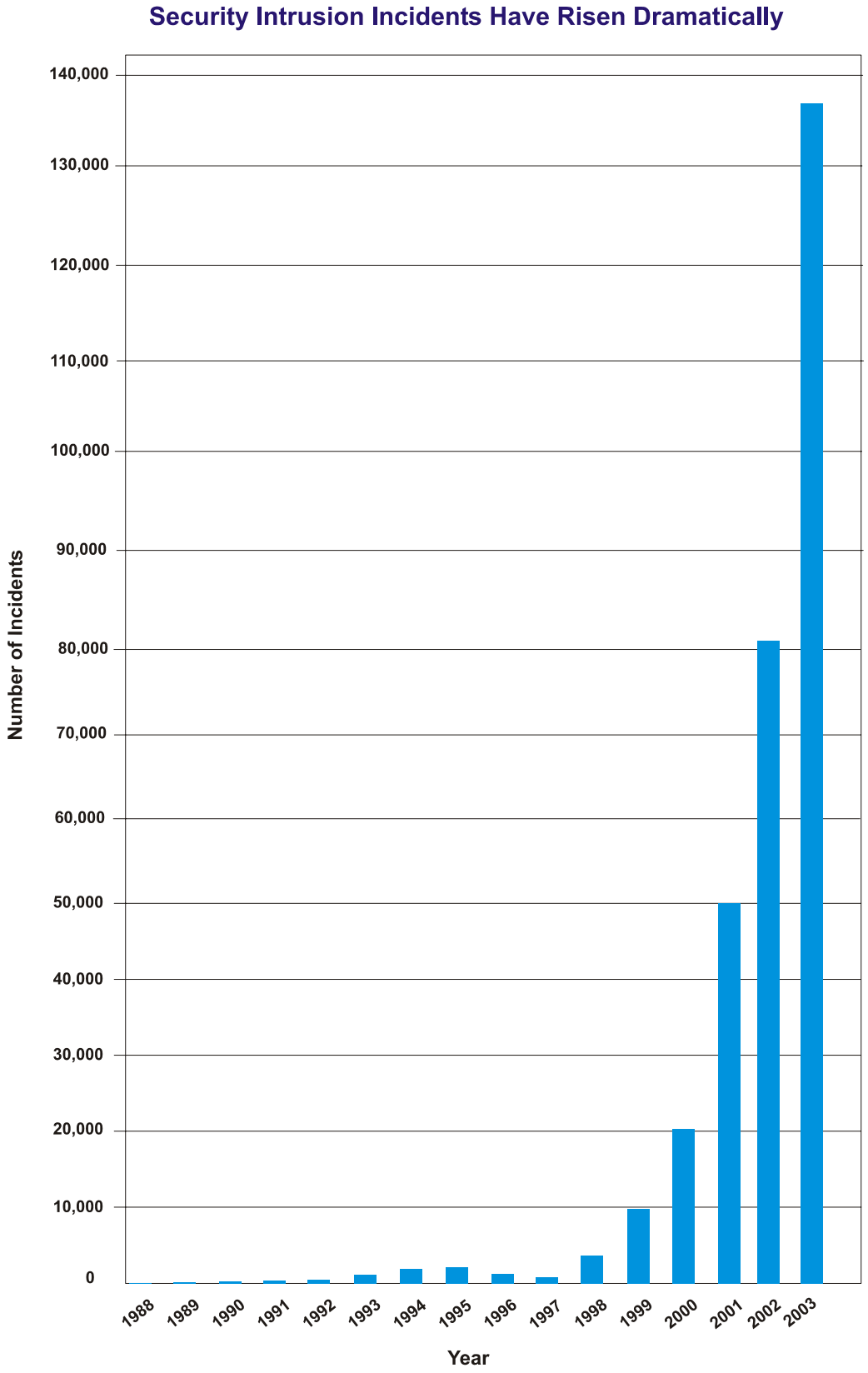
Introduction

Recent world events have expanded the borders in which justice systems must operate—beyond municipality, county, or state—to the national and global levels. Operating effectively in this environment increases the need to securely share information among diverse organizations. This priority has been expressed at the highest levels of government and was well articulated by U.S. Attorney General John Ashcroft in an April 11, 2002, press release.

> **"Information is the best friend of prevention. The September 11 attacks demonstrate that the war on terrorism must be fought and won at all levels of government. To meet this continuing threat, law enforcement officials at all levels—federal, state, and local—must work together, coordinating information and leveraging resources in the joint effort to prevent and disrupt terrorist activity."**
>
> **— U.S. Attorney General John Ashcroft**

As a further consideration, there is an ever-increasing threat to the security of valuable law enforcement and justice information resources from cyberattacks. The incidences of detected intrusions have increased over the last decade, and cyberterrorism has become a real risk. Figure 1-1: Security Intrusion Incidents is representative of statistics, collected by the Carnegie Mellon University Computer Emergency Response Team Coordination Center (CERT®/CC), providing an illustration of this threat (<http://www.cert.org/stats/#incidents>). The number of intrusions reported to the Center has increased exponentially over the last five years.

Figure 1-1: Security Intrusion Incidents



These changes in our environment increase the importance of information security in law enforcement and justice applications. System owners, managers, and users must be more aware of the technology and practices critical to safeguarding information. Security experts uniformly agree that there is no such thing as a 100 percent-secure information system. While there are many tools and practices that can dramatically reduce security risks, the technology is not at a point where anyone can guarantee that information resources will be safe from all possible threats. For this reason, system owners and managers must balance the level of risk, the value of the information, and the amount of investment in security safeguards. Striking this balance requires a firm background in the capabilities of security technology and an understanding of best practices.

Security Architecture

In order to achieve the goals of secure information sharing, organizations must think comprehensively about security or otherwise end up merely moving around the weak link in the security chain ineffectively protecting their information resources. In other words, if security is addressed by focusing on only one or two aspects of the enterprise, very strong protection is achieved only in those areas, and weaknesses are found in others. Those that seek to compromise the security of the enterprise will concentrate their efforts on these weaker areas.

Security Foundation

One way to address the complete universe of information security is to think in terms of three fundamental service areas: Confidentiality, Integrity, and Availability, as represented by the mnemonic "CIA."

- **Confidentiality**—Confidentiality concerns the mechanisms that support information access policies and is designed to ensure that information is not exposed to unauthorized parties.

- **Integrity**—Integrity reflects the accuracy or reliability of information products and requires processes and technology that prevent unauthorized modifications.

- **Availability**—Availability is required to provide confidence that information systems will be accessible when needed—especially important in justice systems where the safety of civil servants or citizens may be at stake.

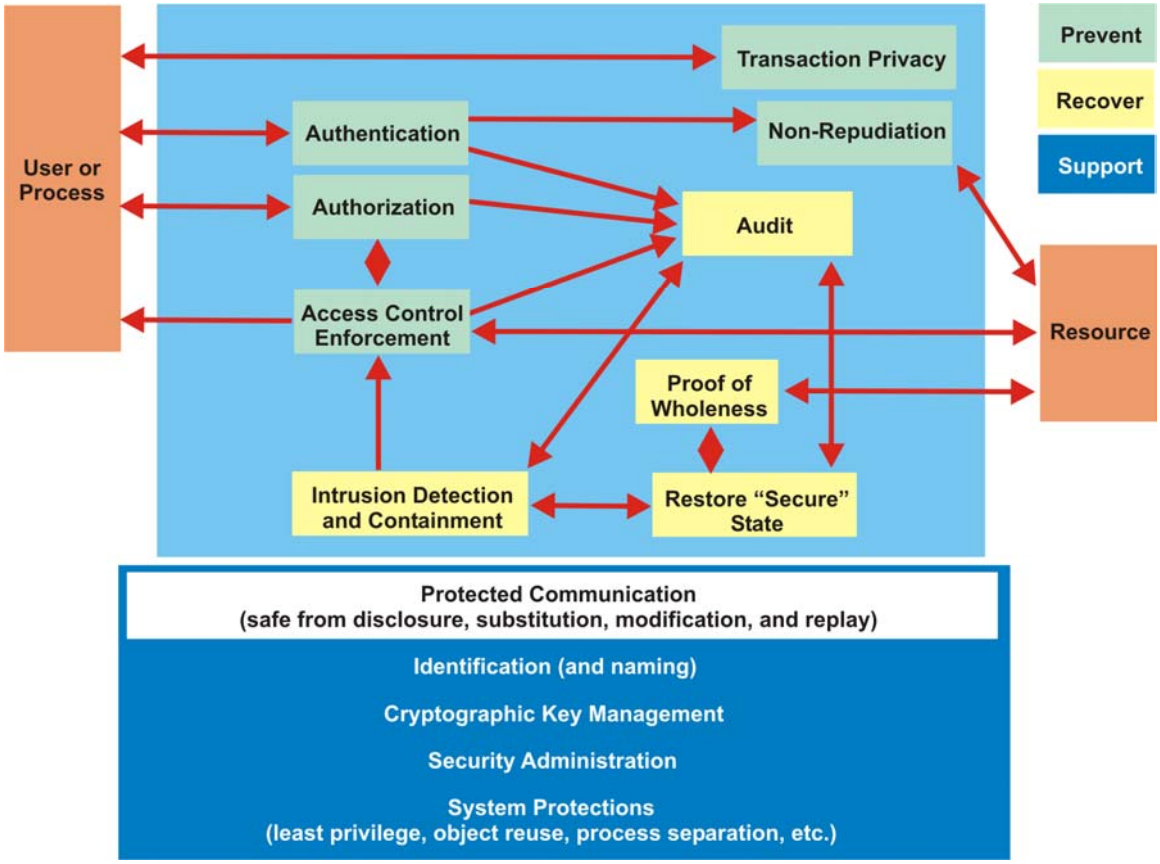
Information system owners and managers should develop a security architecture that addresses "CIA" and includes automated, procedural, and physical security safeguards.

Information system owners and managers should mandate information security architecture. The goal of information security is to protect information from a wide range of accidental or malicious threats. The objective is to:

- Enable the sharing of trusted information.
- Provide continuity in justice agencies.
- Minimize organizational damage by protecting data and systems against destruction, modification, and disclosure.
- Maximize opportunities for information sharing.

Figure 1-2: A Model for Security Architecture is extracted from *Underlying Technical Models for Information Security* (Stoneburner, 2001). This figure characterizes the services required to implement comprehensive security architecture. It is expressed in a format similar to that used for general information system enterprise architectures. The security services identified in this figure are addressed in this document. Refer to Chapter 2, "Security Disciplines," for more information on the topics addressed in this figure.

Figure 1-2: A Model for Security Architecture



Related Resources

Other related resources that help support the objective of secure information sharing and, more generally, the improvement of the assurance level of information systems in this country are as follows:

- **National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC)** (<http://csrc.nist.gov/>)—The CSRC is the Web site of NIST's Computer Security Division, whose mission is to improve information systems' security by raising awareness of information technology (IT) risks, vulnerabilities, and protection requirements; researching, studying, and advising agencies of IT vulnerabilities; developing standards, metrics, tests, and validation programs; and developing guidance to increase secure IT planning, implementation, management, and operation. The site provides a wealth of background and guidance documents, including information on NIST's Automated Security Self-Evaluation Tool (ASSET).

- **CERT®/CC** (<http://www.cert.org>)—The CERT® Coordination Center is a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development organization operated by Carnegie Mellon University. The CERT®/CC focus is protecting information systems against potential problems, reacting to current problems, and predicting future problems. Their work products include handling computer security incidents and vulnerabilities, publishing security alerts, researching long-term changes in networked systems, and developing information and training.

- **Integrated Justice Information Systems (IJIS) Industry Working Group (IWG)** (<http://www.ijis.org>)—The IJIS IWG is an organization of service and product vendors that serve the local, state, and federal agencies in the area of law enforcement and criminal justice. The charter for the IJIS IWG, sanctioned by the OJP, DOJ, is to contribute to the implementation of integrated justice information systems throughout the country by applying the knowledge and experience of the IT industry. The IJIS IWG Web site contains briefing materials and documents that provide background information on security technologies and practices.

- **Center for Internet Security (CIS)** (<http://www.cisecurity.org/>)—CIS's mission is to help organizations effectively manage the risks related to information security. CIS provides methods and tools to improve, measure, monitor, and compare the security status of Internet-connected systems and appliances.

Chapter 2: Security Disciplines

Introduction

This chapter discusses the following security disciplines for each of these objectives: Support, Prevention, and Detection and Recovery. Each security discipline is defined in Table 2-1: Information Security Disciplines.

Objective 1: Support

These services are generic and underlie most information technology capabilities.

- ❑ Governance
- ❑ Physical Security
- ❑ Personnel Security Screening
- ❑ Separation of Duties

Objective 2: Prevention

- ❑ Identification and Authentication
- ❑ Authorization and Access Control
- ❑ Data Integrity
- ❑ Data Classification
- ❑ Change Management
- ❑ Public Access, Privacy, and Confidentiality
- ❑ Firewalls, VPNs, and Other Network Safeguards

Objective 3: Detection and Recovery

- ❑ Intrusion Detection Systems
- ❑ Critical Incident Response
- ❑ Security Auditing
- ❑ Disaster Recovery and Business Continuity

Chapter Structure

In general, each security discipline section is constructed as follows:

- **Description and Purpose**—provides a summary of the discipline and the role it plays in securing information.
- **Principles**—identifies the qualities that should be in place in an organization that responsibly and securely manages justice information.
- **Policies**—contains guidance and, when applicable, references to sample policies in order to assist organizations in establishing good internal policies for securing information.
- **Best Practices**—includes tutorials and also overviews the best ways to apply the tools, technologies, and processes within each discipline.
- **References**—provides resources to assist justice organizations in designing their security practices in meeting well-established industry standards.

Table 2-1: Information Security Disciplines

Information Security Disciplines	Definition and Relevance
Governance	Identifies the practices applied to establish, manage, and enforce information security policy.
Physical Security	Protects against compromises in security that may arise from facility and environmental vulnerabilities.
Personnel Security Screening	Includes the processes applied to determine if personnel warrant the level of trust required to access sensitive justice information and systems.
Separation of Duties	Requires the segregation of administrative, development, security, and user functions to provide security checks and balances.
Identification and Authentication	Ensures those wishing to gain access to information resources are who they represent themselves to be. Typical methods include passwords, smart cards, and biometrics.
Authorization and Access Control	Determines what permissions and access authorization an information system user holds.
Data Integrity	Safeguards information content and protects against inadvertent or intentional information modification or loss.
Data Classification	Provides guidelines to label information by its level of sensitivity and appropriate treatment.
Change Management	Recommends procedures so that system configurations are controlled and understood, reducing the risk of security compromise.
Public Access, Privacy, and Confidentiality	Outlines tools and procedures to protect the privacy of individuals and information in light of the increased accessibility offered by networked information systems.
Firewalls, VPNs, and Other Network Safeguards	Identifies the tools employed to establish a barrier between private and public information in a justice organization.
Intrusion Detection Systems	Monitors computing and communications facilities for evidence of inappropriate access or use.
Critical Incident Response	Determines whether or not an incident has occurred and develops methods of control to handle and minimize disruption of service.
Security Auditing	Examines and verifies that organizational practices meet security policies and applicable regulations.
Disaster Recovery and Business Continuity	Establishes and documents the procedures to follow in the event of a disaster so that operations that depend on the accuracy and availability of information can continue and be restored.

Objective 1: Support

Security Disciplines:

1-1. Governance 2-9

1-2. Physical Security 2-11

1-3. Personnel Security Screening..... 2-19

1-4. Separation of Duties..... 2-23

Objective 2: Prevention

Security Disciplines:

2-1. Identification and Authentication 2-27

2-2. Authorization and Access Control..... 2-35

2-3. Data Integrity 2-39

2-4. Data Classification..... 2-43

2-5. Change Management 2-49

2-6. Public Access, Privacy, and Confidentiality 2-53

2-7. Firewalls, VPNs, and Other Network Safeguards 2-59

Objective 3: Detection and Recovery

Security Disciplines:

3-1. Intrusion Detection Systems (IDS)..... 2-67

3-2. Critical Incident Response 2-71

3-3. Security Auditing..... 2-79

3-4. Disaster Recovery and Business Continuity 2-83

Security Disciplines for Objective 1: Support

1-1. Governance 2-9
1-2. Physical Security 2-11
1-3. Personnel Security Screening 2-19
1-4. Separation of Duties 2-23

1-1. Governance

Description

For an individual justice organization, governance is the source of security policy, establishing the activities required to assess risk, set direction, and monitor the application of security tools with the objective of creating a secure operating environment. In an environment in which justice information is shared, governance is more complex and must represent the security interests and policies of multiple organizations.

Purpose

Security management encompasses a number of functions, as outlined in this document. Governance recognizes that these functions need oversight and control at a high level to assure that each is addressed appropriately. Only in this way can the benefits of a comprehensive security program be gained. Further, information sharing and joint operations are becoming increasingly important for justice and public safety organizations. That implies the need for governance structures that cross individual agencies. Consequently, governance issues deserve prominent consideration.

Principles

- Governance involves both technologists, operational management, and strategic business management.
- At the governance level, risk assessment deals with risk to the operation, its continued viability, and the critical data it maintains.
- IT management staff has the responsibility to manage security to the best standard for a given level of risk; the governance group establishes that level of risk and is accountable for setting that level appropriately.
- Governance structures for information sharing should be representative of the stakeholders.
- Governance strives for repeatable results with continual improvement.

Best Practices

- Include strategic business management, senior operational management, and senior IT management on the governance board.
- Strive for a full discussion of risk so that all participants understand what the risks are. Classify risks according to level, set a strategic plan to attack the highest priority risks, and know which risk each new security initiative is targeting. For example, see NIST Special Publication 800-63,

Recommendations for Electronic Authentication, at <http://fasp.nist.gov/publications/drafts.html#draft-sp80063>.

- Understand what laws, regulations, and rules apply to the organization and to the information being used.
- Insist that the business purpose for each new security initiative is clear.
- Understand the total cost of ownership of each new security initiative, and make efforts to relate that cost to a return on that investment.
- Report periodically (at least annually) on progress made during the past period and the objectives set for the next period.

References

- Institute of Internal Auditors, Information Security Governance: What Directors Need to Know, <http://www.theiia.org/esac/index.cfm?fuseaction=or&page=rciap2&doc_id=2945>.
- Information Systems Audit and Control Association, *Information Security Governance: Guidance for Boards of Directors and Executive Management*, <http://www.isaca.org/Template.cfm?Section=Governance&template=/ECommerce/ProductDisplay.cfm&ProductID=110>.
- IT Infrastructure Library (ITIL): Provides IT governance models.
- Control Objectives for Information and Related Technology (COBIT).

1-2. Physical Security

Description

Computer systems and networks are vulnerable to physical attack; therefore, procedures should be implemented to ensure that systems and networks are physically secure. Physical access to a system or network provides the opportunity for an intruder to damage, steal, or corrupt computer equipment, software, and information. When computer systems are networked with other departments or agencies for the purpose of sharing information, it is critical that each party to the network take appropriate measures to ensure that their system will not be physically breached, thereby compromising the entire network. Physical security procedures may be the least expensive to implement but can also be the most costly if not implemented. The most expensive and sophisticated computer protection software can be overcome once an intruder obtains physical access to the network.

Purpose

This chapter identifies potential physical threats to facilities, hardware, software, and sensitive information. This chapter also recommends best practices to secure computer systems from physical intrusion.

Principles

- Identify potential physical threats to departmental computer systems and networks.
- Establish policies and procedures to thwart potential physical threats.
- Conduct audits to monitor employee compliance with department policies and procedures.

Policies

An organization should consider including the following physical security policies in the organization's overall security policy:

- Identify unauthorized hardware attached to the department computer system—make routine checks of system hardware for unauthorized hardware.
- Limit installation of hardware and software owned by employees on department desktop workstations.

- Identify, tag, and inventory all computer system hardware.
  - Conduct regular inspections and inventories of system hardware.
  - Conduct unscheduled inspections and inventories of system hardware.
- Implement policies that instruct employees/users on how to react to intruders and how to respond to incidents where an intrusion has been detected.

Best Practices

Physical security practices should address threats due to theft, vandalism, and malicious internal or external staff.

- **Theft**—Theft of hardware, software, or data can be expensive due to the necessity to restore lost data and the cost of replacing equipment and software. Theft also causes a loss of confidence in the department that may have compromised the network.

- **Vandalism**—Vandalism in most cases is not directed at compromising a system or network so much as it is the senseless destruction of property. Both external and internal perpetrators may pose a vandalism threat. Low morale in an organization may be the underlying reason for vandalism caused by internal perpetrators. The actual threat to a network posed by vandalism is difficult to assess because vandalism is generally not motivated by a conscious effort to compromise a network. Like theft, vandalism can be expensive due to the necessity to replace damaged equipment and software.

- **Threats Posed by Internal and External Staff**—Internal and external intruders may attempt to manipulate or destroy IT equipment, accessories, documents, and software. The potential of damage caused by intruders' manipulation increases the longer they remain undetected, thereby increasing their knowledge of the system and their ability to wreak havoc on a network. The threats may include unauthorized access to sensitive data and outright destruction of data media or IT systems.

  Internal staff may attempt to modify privileges or access unauthorized information, either for their own purposes or for others. This may result in system crashes or breaches in other areas of the network opened up through configuration errors.

  Temporary workers, contractors, and consultants represent a unique security threat in that they are generally not subject to the same background checks as a department's full-time employees, but they may be granted the same high level of access to the system and network. Contractors and consultants will sometimes know the applications and operating systems running on the

network better than department employees. Temporary employees should be closely scrutinized until a level of trust can be established. Question consulting firms and contract agencies about their hiring policies and standards. Threats may also arise from the conduct of cleaning staff by theft of system components or from using the system improperly by accidentally detaching a plug-in connection, allowing water seepage into equipment, or mislaying or discarding documents as trash.

An intruder may attempt to masquerade as or impersonate a valid system user by obtaining a false identity and appropriating a user ID and password. Someone may be misled about the identity of the party being communicated with for the purpose of obtaining sensitive information. An intruder can also use masquerading to connect to an existing connection without having to authenticate himself, as this step has already been taken by the original participants in the communication.

Social engineering can be used by internal or external intruders to access sensitive information. Intruders act like department staff and use keywords during conversations to obtain information. "Sounding" occurs by telephone when intruders pose as staff, as in the following examples:

- A staff member who must urgently complete an assignment but has forgotten his password.
- An administrator who is attempting to correct a system error and needs a user password.
- A telephone technician requesting information, such as a subscriber number or modem configurations and settings.

Applying the following physical security measures mitigates these threats.

- **Identification of Unauthorized Hardware Attached to a System**—Establish policies to limit employees from attaching unauthorized hardware to the office system. Unauthorized hardware includes computers, modems, terminals, printers, and disk or tape drives. The policies should also restrict software that employees may load onto the office system. Implement policies regarding opening unidentified e-mail attachments and downloads off the Internet.

  Perform monthly audits of all systems and peripherals attached to the network infrastructure. Make random inspections of equipment to search for unauthorized attached hardware to the network. Identify missing or misplaced hardware. Search and identify any unauthorized hardware attached to the network.

Inspect computers and networks for signs of unauthorized access. Search for intrusion or tampering with CD-ROMs, tapes, disks, paper, and system components that are subject to physical compromise by damage, theft, or corruption.

- **Protection Against Break-in**—Intruders choose targets by weighing the risk and effort versus the expected reward. Therefore, all measures implemented to prevent break-ins should increase the risk to the intruder of being caught. The possible measures for protection against break-ins should be adapted to each specific situation. Protect doors or windows by adding security shutters. Add additional locks or security bars. Add additional lighting inside and outside the building. Seek advice from police and security professionals. When planning physical security measures, care must be taken to ensure that provisions relating to fire and personal protection (e.g., regarding the serviceability of escape routes) are not violated. Staff must be trained on the antiburglary measures that are to be observed.

- **Entry Regulations and Controls**—A fundamental but frequently overlooked aspect of sound internal security is the physical restrictions placed on access to systems and networks. Having good physical security in place is a necessary follow-up to whatever office building security an organization may have in place. Know who is entering department offices at all times, and ensure all secure computing areas are locked and access restricted. Network security measures can be rendered useless if an intruder can bluff his way past the entrance security; walk into a computer room; and take diskettes, tapes, or servers.

  Strangers, visitors, craftsmen, and maintenance and cleaning staff should be supervised. Should the need arise to leave a stranger alone in an office, the occupant of that office should ask another staff member to supervise or request the visitor to wait outside the office. If it is not possible to accompany outsiders, the minimum requirement should be to secure the personal work area: desk, cabinet, and computer. The requirement for this measure must be explained to the staff and should be made part of department policy and training.

  Control entry into buildings and rooms housing sensitive equipment. Security measures may range from issuance of keys to high-tech identification systems. When implementing policies for entry regulation, consider the following:

  - The area subject to security regulations should be clearly defined.
  - The number of persons with access should be reduced to a minimum.
  - Authorized persons should be mutually aware of others with access authority in order to be able to recognize unauthorized persons.

- Visitors should only be allowed to enter after the need to do so has been previously verified.
- The permissions granted must be documented.
- Access should be limited by locked rooms/entrances, physical zones, and identification badges.
- A record must be kept of accesses.
- Challenge protocols should be added.

❑ **Entrance Security Staff**—Establishment of an entrance control service has far-reaching, positive effects against a number of threats. However, this presupposes that some fundamental principles are observed in the performance of entrance control. Entrance security staff must observe and/or monitor all movements of persons at the entrance. Unknown persons must prove their identity to the entrance security staff. Before a visitor is allowed to enter, a check should be made with the person to be visited. A visitor must be escorted to the person to be visited or met by the latter at the entrance. Security staff must know the office employees. In case of termination of employment, security staff must be informed of the date from which this member of staff is to be denied access. A visitor log should be kept to document access. The issuance of visitors' passes should be considered. The job duties of security staff should be designed specifically to identify their tasks in support of other protective measures, such as building security after business hours, activation of the alarm system, and checking of outside doors and windows.

❑ **Alarm System**—An alarm system consists of a number of local alarm devices that communicate with a control center through which the alarm is triggered. If an alarm system covering break-ins, fire, water, and gas is installed and can be expanded at reasonable cost, it should be considered whether, as a minimum, the IT core areas (such as server rooms, data media archives, and technical infrastructure rooms) could be included in the surveillance provided by this system. This will enable threats, such as fire, burglary, or theft, to be detected in good time so that countermeasures can be taken. To ensure that this is the case, it is imperative that the alarms be sent on to an office that is permanently staffed. It is important that this office have the expertise, equipment, and personnel required to respond to the alarm. The guidelines of the organization concerned for connection to the respective networks should be considered here.

❑ **Security of Windows and Doors**—Windows and outward-leading doors (e.g., balconies, patios) should be closed and locked whenever a room is unoccupied. Instructions to close windows and outside doors should be issued, and regular checks should be made to see that windows and doors are closed by occupants after leaving the rooms.

The doors of unoccupied rooms should be locked. This will prevent unauthorized persons from obtaining access to documents and IT equipment. It is particularly important to lock individual offices when located in areas accessible by the public or where access cannot be controlled by any other means. Staff should be instructed to lock their offices when they leave, and random checks should be made to determine whether offices are locked when their occupants leave.

In an open office, where cubicles dominate and it is not possible to lock individual offices, employees should lock away their documents in their desks, and a secure desktop workstation policy should be implemented (additional information on formulating this policy can be found later in this chapter).

- **Unauthorized Admission to Rooms Requiring Protection**—If unauthorized persons enter protected rooms, damage may be caused by intentional and unintentional acts. After an unauthorized intrusion, office routines may be disrupted in order to search for damage, theft, and unauthorized or missing hardware/software. Intentional or unintentional damage to systems may be caused by temporary help who are employed to substitute for cleaning staff. Temporary help may accidentally clean workstations and sensitive equipment with solutions or by methods damaging to hardware.

- **Identification of Secure Rooms**—Secure rooms such as the server room, computer center, data media archives, and air conditioning unit should not be identified on office locator boards or by name plates affixed to the room door. Identifying these sensitive areas enables a potential intruder to prepare more specifically and thus have a greater chance of success.

- **Location of Secure Rooms in Unexposed Areas of Buildings**—Secure rooms should not be located in areas exposed to view or potential danger. They also should not be located on the first floor of buildings that are open to view by passersby or that are exposed to attack or vandalism. First floor rooms are more likely to be easily observed or exposed to breaking and entering. Rooms or areas requiring protection should be located in the center of a building, rather than in its outer parts.

- **Inspection Rounds**—The effectiveness of any measure will always be commensurate to the enforcement of that measure. Inspection rounds offer the simplest means of monitoring the implementation of measures and the observance of requirements and instructions.

  Inspection rounds should not be aimed at the detection of offenders for the purpose of punishing them. Rather, controls should be aimed primarily at remedying perceived negligence at the earliest possible moment, such as by closing windows or taking documents into custody. As a secondary objective, security breaches can be identified and possibly avoided in the future. Inspection rounds should also be made during office hours to inform staff members about how and why pertinent regulations are being applied.

Thus, they will be perceived by all persons concerned as a help rather than a hindrance.

- **Proper Disposal of Sensitive Resources**—Sensitive information not properly disposed of may be the source of valuable information for persons seeking to do harm. An intruder, competitor, or temporary staff can gain valuable information in a low-tech manner by simply going through trash for discarded paperwork that might contain sensitive information. At a minimum, shred all papers and documentation containing sensitive company information, network diagrams, and systems data to prevent a security breach by those who might seek information by rummaging through trash. Employees should be advised against writing down user IDs or passwords.

  In the case of functioning media, the data should be overwritten with random patterns. Nonfunctioning data media, such as CD-ROMs, should be destroyed mechanically.

  The recommended disposal of material requiring protection should be detailed in a specific directive and in training; adequate disposal facilities are to be provided. This includes storage devices and media (i.e., floppy and hard disks, magnetic tapes, and CD-ROMs/DVDs). If sensitive resources are collected prior to their disposal, the collected material must be kept under lock and be protected against unauthorized access.

Secure Desktop Workstations—The first line of defense in physical security is to secure desktop workstations. Effective training in the organization's policies and procedures to secure desktop workstations should be a significant part of network and information security strategy because of the sensitive information often stored on workstations and their connections. Many security problems can be avoided if the workstations and network are appropriately configured. Default hardware and software configurations, however, are set by vendors who tend to emphasize features and functions more than security. Since vendors are not aware of specific security needs, new workstations must be configured to reflect security requirements and reconfigured as requirements change.

Remote Workstations—There is usually a higher risk of theft at home because homes are usually not protected to the same extent as the workplace. Workstations at home are accessible to family members and visitors who may intentionally or unintentionally manipulate business-related data on the workstation, if data is not properly protected. Inadvertent or intentional manipulation affects the confidentiality and integrity of the business-related information, as well as the availability of data and IT services on the workstation. Appropriate procedures should be implemented to achieve a degree of security comparable with that prevailing on office premises.

- **Suitable Configuration of a Remote Workplace**—It is advisable to assign a secure room for use as a workplace at home. Such a workplace should at least be separated from the rest of the premises by means of a door.

IT equipment intended for professional purposes should be provided by the employer, and the use of these services for private purposes should be prevented by formal policies. Employees who work at home should be questioned regularly or periodically as to whether their workplace complies with security and operational requirements.

- **Theft of a Mobile IT System**—Laptop or mobile IT systems create a greater risk of theft or damage. Due to the inherent nature of a mobile system, it will often be removed from the confines of a secure office. Therefore, policies should be implemented to safeguard mobile IT systems.

- **Suitable Storage of Business-related Documents and Data Media**—Business-related documents and data media at the home workstations must only be accessible to the authorized employee, and when they are not in use, they must be kept in a locked location. A lockable desk, safe, or cabinet must be available for this purpose. At a minimum, the lock must be capable of withstanding attacks using tools that are easy to create or purchase. The degree of protection provided by the drawer should be appropriate to the security requirements of the documents and data media contained therein.

References

- Allen, Julia & Stoner, Ed. *Detecting Signs of Intrusion*. (CMU/SEI-SIM-009). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2000, <http://www.cert.org/security-improvement/modules/m09.html>.

- Ford, Gary, et al. *Securing Network Servers*. (CMU/SEI-SIM-007). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1999, <http://www.cert.org/security-improvement/modules/m10.html>.

- Kossakowski, Klaus-Peter, et al. *Responding to Intrusions*. (CMU/SEI-SIM-006). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1999, <http://www.cert.org/security-improvement/modules/m06.html>.

- Federal Agency Security Practices. National Institute of Standards and Technology Web site. Available at <http://csrc.nist.gov/fasp/>.

1-3. Personnel Security Screening

Description

Ensuring that the personnel within an organization who have authorized access to sensitive systems are suitable and trustworthy is the cornerstone of a good security system. Statistics show that the majority of system misuse is conducted by those with authorized access to the information. As trusted partners in justice and public safety information sharing, it is imperative that employees undergo a significant screening process to determine their suitability for access to sensitive systems and those to which they are connected. This applies to all positions and to all phases of the contracting process where access to critical systems is authorized.

Purpose

The personnel security screening discipline describes the methods that agencies must use to screen an applicant's background for past inappropriate behavior that may put unclassified but sensitive data at risk. The rigor of the screening may vary based on the applicant's access requirements to computer systems and databases. It is imperative that all applicants be screened in a standardized manner. Personnel security screening will promote trust among agency partners.

Principles

- The level of assurance of the screening mechanism employed should be balanced against the cost of the mechanism and the risk associated with incorrectly "passing" an individual trying to gain access to the information system.

- Users should be properly screened. Proper screening requires that an employer use a consistent and reliable means to conduct such screening to perform an adequate background check before authorizing access to the system.

- Personnel with direct and appropriate access to critical systems and partner systems should undergo a more rigorous background check than those with secondary access.

- Mechanisms should be in place to relieve personnel from duties requiring direct access to critical systems should their initial or subsequent background checks reveal information that would preclude their access.

Policies

Once an organization decides on an approach for personnel screening, the policies related to that approach should be documented so that there is a written guideline specifying the consistent and comprehensive application of the screening process. The personnel department will play an important role in this policy development, and new tools may need to be developed for the selection process. The Global Security Working Group maintains a library of security screening policies samples.

Best Practices

It is a best practice to require background checks on all employees every five years. The initial personnel screening process comprises the following steps.

Step One: Determine the Appropriate Screening Requirements—Screening must be carried out according to the highest level of information that will be accessed in the performance of assigned duties or during the contracting process. If the employee will access only information contained within their jurisdiction with no gateway access to justice partners, the screening process may differ from that incumbent who has access to multiple justice partner information.

Step Two: Identify Required Checks—

- **Basic Reliability Check for No Direct Access to Other Systems**—When a basic reliability check for no direct access to critical and other systems is needed, the following checks may be appropriate: (1) verification of personal data, education, professional qualifications, employment, and references; (2) a declaration signed by the incumbent concerning any conviction for a criminal offense (may be a part of the application process); and (3) a criminal history records check based on a full name and date-of-birth search of state and federal records for criminal justice employment (which should be completed within thirty days of employment and after a name and date-of-birth check is completed with either positive or negative results).

- **Enhanced Reliability Check for Direct Access to Critical Systems and Other Systems**—When a reliability check for direct access to critical systems and other systems is needed, the following checks may be appropriate: (1) verification of personal data, education, professional qualifications, employment, and references; (2) a declaration signed by the incumbent concerning any conviction for a criminal offense (may be a part of the application process); (3) a criminal history records check based on a full name and date-of-birth search of state and federal records for criminal justice employment (which should be completed within thirty days of employment and after a name and date-of-birth check is completed with either positive or negative results); (4) a credit check, when duties or tasks performed would require it or in the event of a discovered criminal record; and (5) a criminal

history records check with the submission of a completed applicant fingerprint card to the FBI CJIS Division through the state identification bureau, when the state is a single-source participant.

Step Three: Obtain Consent—The screening process involves the review of personal information, and while it must be a mandatory requirement for a successful applicant, consent is required prior to beginning the process. Written consent may only be given by those persons who have reached legal age; otherwise, the signature of a parent or guardian is required. Make certain the screening process does not begin prior to receiving this written consent. Inform those who do not consent to the screening process that they cannot be considered further for employment or contractual work.

For all security screenings, a declaration regarding the existence of a criminal record must be obtained. The applicant will be required to state whether he or she has been convicted of a criminal offense. This may be a part of the application process form(s).

Step Four: Process the Required Checks—

- **Criminal Records Name and Date-of-Birth Check**—To initiate this type of check, access to the state and federal criminal history record systems is required. In most cases, employment within criminal justice agencies allows, if not demands, that this check be minimally completed prior to allowing direct or secondary access to systems that may contain sensitive information. If state and federal criminal history records access is not available within your agency, it will be necessary to determine internal procedures within your city, county, state, or federal jurisdiction to conduct these name and date-of-birth criminal history background checks. Proper legal identification must be presented by the applicant, as the inquiry must be made by using legal full name and accurate date-of-birth information. It is important to note that these checks may cause multiple hits on common names, and the only accurate method of determining whether the person inquired upon matches any possible response is through fingerprint comparison.

- **Fingerprint Check**—When required, fingerprints are to be taken after the consent form is completed and will normally be taken at the jurisdiction's enforcement unit, such as the state police, county sheriff (bailiff for courts), local police, or booking unit. Every effort should be made to ensure the comfort of the applicant during this process. The completed fingerprint (normally done in duplicate) should be forwarded to the appropriate entity within the jurisdiction for processing.

- **Credit Check**—Where required, the credit check is conducted by the agency, at their expense, through the associated credit bureaus. While not necessarily an accurate indicator of an employee's suitability for a position, it may be used in addition to other information obtained to make an informed decision.

- **Contracts**—For contracting firms, the contracting authority is responsible for ensuring that the firm verifies its employees' personal, educational, and employment data and conducts reference checks. The contracting authority initiates criminal records checks and conducts other appropriate checks.

Step Five: Evaluate the Results of Required Checks—Once the checks are completed, a decision must be made based on the information gathered. Factors to be considered are subjective and varied and cannot be adequately discussed here. In most cases, a gross misdemeanor or felony conviction within the past ten years is just cause for denial of employment with direct access to these systems. Consult the personnel department and legal department for additional information.

Step Six: Grant or Deny Access—Based on final evaluation, access to the system is granted or denied.

Step Seven: Brief the Screened Person—If negative information is obtained from the screening process, this step must be completed. The applicant may be in possession of additional information that may make the evaluation process more complete. If a name and date-of-birth check has revealed a match, a fingerprint comparison may be necessary to adequately protect the applicant from any false-positives that result from such a check.

References

For a listing of applicable security screening standards, see:

- *<http://www.leo.gov/lesig/cjis/cjis_pub/information/poly2002_feb/POLY 2002_Feb.htm>.

- *Personnel Security Standard*, Treasury Board of Canada: <http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/CHAPT2-4_e.asp>.

- Web site for National Association of State and Chief Information Officers (NASCIO) security policy: <http://www.nascio.org>.

  *Note: Only Law Enforcement Online (LEO) members may access the www.leo.gov Web site.

1-4. Separation of Duties

Description

Separation of duties is a critical element of a robust security policy. It requires the allocation of distinct information system duties such as database administration, security, user functions, and source code access into separate job functions performed by different individuals. Separation of duties should be incorporated into change management procedures (see Section 2-5, Change Management, in this chapter).

Purpose

Separation of duties segregates critical, operational IT functions into distinct jobs to prevent a single person from harming a development or operational system or the services they provide, whether by an accidental act, omission, or intentional act.

Principles

The approach to separation of duties should be defined in an organization's security policy.

Separation-of-duties procedures should be developed by the information system management team.

Policies

A separation-of-duties policy should be established and documented that encompasses programming, database administration, security, user functions, and source code access into separate job functions performed by different individuals. A training program should be established for impacted personnel on separation of duties, and an audit plan should be established and executed periodically to ensure compliance with the separation-of-duties policy.

Best Practices

An individual should not have access to more than one critical task as identified by management. Personnel should only perform those duties specified in their job descriptions; therefore, programming and operations functions should be performed by different individuals.

Programmers should not be able to execute any jobs in a production mode, perform database administration functions, perform application security functions, or have access to production databases.

Operators should not have the ability to make changes to production applications or system software libraries, and database changes should be administered by database administration personnel only.

Security responsibilities should be clearly separated from processing operations functions. Security functions (i.e., authority, access to data, restricting functions) should be performed by security personnel.

Reference

- International Standard, ISO/IEC 17799, Information Technology – Code of Practice for Information Security Management.

Security Disciplines for Objective 2: Prevention

2-1. Identification and Authentication 2-27

2-2. Authorization and Access Control..... 2-35

2-3. Data Integrity 2-39

2-4. Data Classification..... 2-43

2-5. Change Management 2-49

2-6. Public Access, Privacy, and Confidentiality 2-53

2-7. Firewalls, VPNs, and Other Network Safeguards 2-59

2-1. Identification and Authentication

Description

Identification and Authentication (I&A) are the first line of defense in many information systems. I&A mechanisms provide a basic security function: they ensure that those wishing to gain access to information resources are indeed who they represent themselves to be. There is increasing focus on authentication protocols and technology. Today, the most common form of authentication is password control. In general, technologies for authenticating a potential user of an information system are organized into three identification factors: something you know, something you have, and something about yourself. An example of something you know is a password or a personal identification number (PIN). Something you have might be a smart card. Something about yourself can be a biometric such as a fingerprint, iris pattern, facial pattern, handwriting, or voice pattern. Highly secure systems can use multiple factors. For example, a biometric authentication system may also require the entry of a password to mitigate the risk of false-positive matches.

Purpose

I&A describes the methods and technology that users engage to identify themselves to an information system. There is a wide range of alternatives available in both method and technology. These alternatives vary in rigor (i.e., the security assurance level or the degree of protection that they provide) and cost. In general, rigor and cost are directly proportional—the more rigorous a method/technology, the more it costs. The information system owner/designer should look to methods that provide as high a level of assurance as possible within cost constraints.

Principles

- The level of assurance of the I&A mechanism employed should be balanced against the cost of the mechanism and the risk associated with incorrectly identifying an individual trying to gain access to the information system.

- Users should be properly registered. Proper registration requires that users provide a consistent and reliable means to identify themselves to a registration authority before receiving the credentials used in I&A. For example, the user may be required to produce a driver's license and a work identification to receive a smart card used to gain access to an information system.

- There should be a unique set of identification credentials for each individual user. For example, two users should not share a username and password when accessing an information system.

- There should be a procedure in place to efficiently grant and revoke I&A credentials.

- There should be mechanisms in place to allow audits and reviews of the identities of users that have valid or revoked I&A credentials.

Policies

Once an organization decides on an approach for authentication, the policies related to that approach should be documented so there is a written guideline specifying the consistent and comprehensive application of authentication throughout the information enterprise. The policy should identify scope, methods, standards, and organizational and individual responsibilities. The Global Security Working Group maintains a library of authentication policies samples at the Web site <http://www.it.ojp.gov>.

Reference the following documents for examples of I&A policy statements:

- The Kansas Department of Administration Information Technology Security Policy, Section 7C User Accountability: UserIDs and Passwords, and 7D Access Controls, <http://da.state.ks.us>.

- State of Arizona Statewide Standard P800-S820, Authentication and Directory Services, <http://gita.state.az.us/policies_standards/html/p800_s820_authentication.htm>.

- The Missouri Office of State Court Administrators (OSCA) Data Security Guidelines, Access Controls.

Best Practices

Most authentication techniques follow the "challenge-response" model, in which an individual is prompted (the challenge) to provide some private information (the response). The complexity of this interaction is governed, in part, by the number of I&A factors included in the response.

Both cost and level of protection increase as the number of factors increase. Generally, the factors are added in the following order: (1) something you know, (2) something you have, and (3) something about yourself. For example, system designers may start with a something-you-know factor and add a something-you-have factor to get the next increment of protection. The following paragraphs provide background on the three factors and summarize best practices under each. This overview is concluded with a discussion of authentication servers-systems that are added to an information network for the sole purpose of completing the authentication process.

Something You Know: Passwords—Passwords remain the most common form of I&A. Unfortunately, passwords can be easily misapplied and provide a weak level of security. One reason is that users tend to pick simple passwords that are easy to remember. For example, there are approximately 50,000 words in the English dictionary. If a dictionary word is used as a password, it is a fairly quick and easy task for a computer program to try each one of the 50,000 and guess the password. System administrators should use software that enforces the selection of strong passwords (eight characters or more with a mix of lowercase, uppercase, and special characters with no simple words or names.) Furthermore, system administrators should periodically run security software utilities that scan for weak passwords. Password security mechanisms can be strengthened further through the use of "one-time passwords." One-time passwords can be implemented through either software or hardware. Hardware implementations, typically dependent on the use of a token device, are described in the next chapter.

New products are currently available that apply to the something-you-know factor in a slightly different way. These products use information that is available about individuals from large, public data sources to "test" the individual and confirm identity. For example, someone claiming to be John Ashcroft might be asked to enter John Ashcroft's social security number and the address of his last three residences. This type of authentication may be appropriate in situations where the authentication subject is from the general public. Because data sources for personal information are generally accessible databases, it may be inappropriate to rely solely on knowledge of this information to verify identity. For example, to improve the assurance level of the process, the individual may be asked to produce some form of formal identification in addition to correctly responding to questions on personal background. As in all I&A approaches, care must be taken to match the level of assurance of the method to the risk of a false-positive or negative authentication.

Something You Have: Token Devices and Smart Cards—Probably the simplest and least costly hardware token device is one that is used to implement a one-time password. The security limitations of passwords can be summarized briefly: easy passwords are easy to "crack"; complex passwords are hard to remember. Passwords that are hard to remember are often written down somewhere. In some cases, they are written down in dangerous places, such as Post-it notes attached to a workstation. A one-time password token provides a code that can be appended to the user's password. This code changes on each use so that the password is different each time it is entered. This addition makes simple passwords more complex. Even if the password is "sniffed" (inappropriately intercepted and stolen), there is little harm since the compromised password cannot be used again.

A one-time password token device often resembles a credit card-size pager. Many token devices work by displaying a code that the user can append to his/her password. The code is calculated by encrypting the time of day with a secret encryption key stored on the device. The authentication server (i.e., the computer system with which the user interacts for the purposes of I&A) knows what encryption key is assigned to the holder of the token and applies the same calculation to the time of day. The user reads the number currently displayed on the token and enters it along with his/her password. This type of system is much easier and less costly to administer than smart cards that depend on public key

cryptography. Furthermore, this approach does not require reader devices to be installed on the laptop or workstation being used to gain access to the information system or network.

Smart cards are an expensive and more complex way to implement I&A. They can also provide more flexibility and functionality. A smart card is a credit card-size device that contains a computer processor chip and solid-state storage. In many I&A applications, the smart card will store the user's digital certificate. The digital certificate is a data file that contains the user's private key. (Please refer to the chapter on data integrity for a more detailed description of digital certificates and private keys.) To authenticate to an information system or network, the user will insert his/her smart card into a hardware reader connected to a workstation or laptop computer. The processor on the smart card will encrypt a text string with the user's private key. The authentication server can confirm the authenticity of the smart card by decrypting the text string with the user's public key—if the text correctly decrypts with the user's public key, it could only have been encrypted with the user's private key. In this approach, the user's private key never has to be communicated outside of the smart card—it never "leaves" the smart card's circuitry. This helps preserve the integrity of the private key.

Whoever holds the smart card also holds all of the access privileges associated with the user. To minimize the risk associated with lost or stolen smart cards, another identification factor is often required with each smart card use. The user may have to enter a password or a PIN whenever the smart card is placed in a reader. The password or PIN is said to "unlock" the private key for use in I&A. An even more rigorous approach would be to require biometrics to unlock the private key stored on the smart card. Several smart card vendors are currently developing technology that will place a fingerprint reader directly on the smart card. The result will be a very secure and easy-to-use I&A mechanism.

There are several reasons why smart card-based I&A systems can be costly to implement and operate. The cost associated with the smart cards and the readers can be significant when considering a system that supports a large community of users. In addition, the administrative burdens of issuing and managing smart cards increase the cost of using a workstation or laptop computer.

Something About Yourself: Biometrics—Biometrics can offer a rigorous means of authentication by requiring physical identification in addition to something you know or something you have. Biometric methods take several different forms, and they result in varying levels of cost and complexity, depending on the type of information being accessed.

When evaluating different biometric devices and alternatives, it is important to consider the "false rejection rate" (FRR), or type I error, and the "false acceptance rate" (FAR), or type II error. The FRR measures the percentage of rejections that should have been accepted (a valid user who used the device but was not properly identified); the FAR measures the percentage of accepted or validated logins that should have been rejected (an invalid user who was improperly identified as a valid one). These two ratings are closely related. On average, today's biometric devices typically have a 4 to 5 percent error rate. The correlation between the two rates can be expressed in the following manner: for a highly secure solution, the FAR would be zero percent and the FRR would be 5 percent. If the FAR were to increase to 3 percent, the FRR would need to lower to 2 percent. All manufacturers

provide their average FRR and FAR ratings. Other factors to consider are cost, environmental conditions (weather, dust, humidity), and intrusiveness to users.

The different types of biometrics can be grouped into two categories: physical and behavioral. Examples of physical biometrics are a fingerprint or iris pattern; examples of behavioral biometrics are a voice or keystroke pattern. The following paragraphs summarize physical and behavioral biometrics.

- **Fingerprints**—This is perhaps the most well-known and accepted form of physical biometrics in use today. The uniqueness of fingerprints has been recognized for a long time, and fingerprints are the de facto standard identifier in the justice and public safety communities. It is not surprising that this is also the most common form of electronic biometrics identification currently in use. The unique patterns of a given finger are analyzed and stored in a database and compared against a user attempting to gain entry into a system. If a matching pattern is found in the database, the user is granted access. The particular methods of validating a given pattern may differ (for example, minutiae or moiré fringe), but the end result is the same. Some newer scanners detect the temperature or electrical impulses of the digit being scanned, thereby confirming that the finger is currently attached to a living being. Fingerprints are very easy to obtain through scanning, and the technology is nonintrusive.

- **Hand Geometry**—This physical biometric method involves measuring and analyzing the shape of the hand. Different individual characteristics, such as length or width of a certain digit, are combined to ensure a unique pattern. This method can be quite accurate. It is relatively easy to implement and fairly nonintrusive.

- **Retina Scanning**—The retina of each eye is as unique as a fingerprint and relatively easy to scan. Scanning maps the layers of blood vessels on the retinal surface at the back of the eye. This physical biometric method requires that the person stand completely still for a period of time while focusing on a given object. While highly accurate, this method is not widely used due to its intrusive nature and the necessity to remove eyeglasses and, in some cases, contact lenses.

- **Iris Scanning**—Iris scanning is relatively new and very accurate. It works by comparing the color patterns in the iris with a sample or template stored in the database. This physical biometric method is somewhat intrusive but not nearly as much as retina scans. Although it is not necessary to remove eyeglasses, the method may not work on a person wearing colored contact lenses. This method is very easy and inexpensive to implement; a simple electronic camera device can be used to perform the scan.

- **Facial Recognition**—This area of physical biometrics has received much attention lately due to the widespread appeal of its variety of methods. Facial recognition works by combining many different characteristics of the face, such as size, shape, width, color, and even heat patterns. It is nonintrusive and fairly easy to implement, although its overall accuracy is not as good as fingerprints or retina and iris scans.

- **Voice Recognition**—Voice recognition is not simply a matter of recognizing a person's voice but rather an overall analysis of several different factors, such as inflection, gait, and volume. Voice recognition is inexpensive in most applications because it requires little additional hardware beyond the microphones that are standard on most workstations. This behavioral biometrics method is nonintrusive and easy to install but is not necessarily the most accurate.

- **Signature Analysis**—Signature analysis captures and monitors several different aspects of a live signature. Users sign their name as usual on a device such as a touch screen or digitizing tablet, and the system monitors the creation of the signature. Characteristics such as velocity, pressure, and pattern are compared to a known sample. This behavioral biometric method is widely accepted as nonintrusive because all users frequently sign their name as a form of identification. The method is neither expensive nor difficult to implement, but its overall accuracy has yet to be proven.

The overall strategy for deploying and implementing biometrics in an information system is perhaps more important than the type of biometric methods and devices. Biometric methods are typically a very good way to identify an individual, but they should be used in conjunction with another method of verification. If a fingerprint scanner is the sole method of verification, a user with an injured or bandaged hand may not be able to log on. This type of problem exists with many biometrics: a user with a cold sounds different; certain drugs affect the eyes; and heat, cold, dust, and other environmental elements can affect the accuracy of many biometric devices. For these reasons, it is important to consider the operating location of the measuring device—whether it is a laptop installed in a police patrol cruiser or a desktop at the precinct. It may also be appropriate to provide different authentication methods for different levels of information sensitivity.

NIST is currently evaluating biometric technology and products for the United States Congress, as mandated by the USA Patriot Act of 2001. The Act calls for biometric identifiers on noncitizens' travel documents by October 2004. NIST has come to four preliminary conclusions:

- Iris scans rely on proprietary technology that makes evaluation of their accuracy difficult.

- Fingerprints work well, but accuracy needs to be better for wide-scale use.

- Facial recognition technologies are not mature yet.

- No biometric technology works well enough to be relied on by itself.

One of the NIST researchers commented that biometric identifiers "…always look stronger and easier in theory than they are in practice. Effective enrollment is difficult, and physical spoofing is a lot easier than we would like." While it must be noted that the NIST study is being conducted for a very specific application of biometrics, some of their preliminary conclusions are relevant to I&A for information system access. With the exception of fingerprint systems, there are very few examples of production biometrics authentication. In contrast, the law enforcement, justice, and public safety communities have relied on fingerprints for investigative and positive identification purposes for decades. As biometric technology matures, the full range of physical and behavioral features described in this chapter will become more important as means of positive I&A. In the meantime, the majority of production I&A systems will continue to focus on fingerprints when adding biometrics as an additional factor for increased levels of assurance.

Authentication Servers and Single Logon—Frequently, in justice applications, a user will first authenticate to a network and then require access to several systems and information repositories connected to that network. For example, a corrections officer may need to access the jail information system as well as the courts' case management system to coordinate the transportation of an inmate to a trial. One way to reduce the number of authentications required and to manage user privileges is to incorporate an authentication server into the network. The authentication server can be used to implement a security service called "single sign-on." The sole function of the authentication server is to validate the credentials of a user prior to granting access to network resources. To accomplish this, there must be electronic trust relationships between the authentication server and the other servers in the enterprise—in our example, between the authentication server, jail information system, and court case management servers.

The authentication server is a single point of access to many of the enterprise resources. For this reason, additional system management attention must be focused on the authentication server to maintain the integrity of the network. However, it is often easier to focus on one server and make sure it is protected and well-managed, to ensure the authentication process is not compromised, than to divide efforts over every server in the network. There are several advantages in using a central authentication server:

- All user IDs and passwords (or other I&A credentials) can be managed from one location. This simplifies the task of adding and deleting users.

- The user needs to only go through the authentication process once—even if he/she needs to access multiple servers to complete a job function (single logon). In a password-based network, the user would not need to remember multiple passwords, and it is easier to maintain a strong password.

- A consistent, secure authentication process can be maintained throughout the enterprise.

While these are strong advantages, it must be reiterated that the authentication server places all of the authentication "eggs in one basket." If the security of the authentication server is compromised, all of the information systems that rely on it for access control can also be

compromised. For this reason, it is imperative that considerable attention be paid to the management and monitoring of the authentication server.

If all of the servers in a network use the same operating system (e.g., UNIX, Windows 2000, Netware, or OS390), centralized authentication service may be a native feature of the enterprise network design. For example, in a homogenous Windows 2000 network, the user can authenticate to the "primary domain controller" and use trust relationships between the servers to access information anywhere in the network where the proper authorization exists. However, many networks are heterogeneous and include several types of servers and operating systems. Heterogeneous server networks are almost a fact of life in larger networks where information systems are owned and operated by different organizations. The court case management system may operate on a central mainframe. The sheriff's jail system may operate on a UNIX server housed in its facilities. Police files may reside on Netware file servers. An authentication server can be used to help manage user I&A in this type of environment.

References

For a listing of applicable biometrics standards, see:

- <http://www.itl.nist.gov/div895/biometrics/standards.html>.
- <http://www.biometrics.org/html/standards.html>.

2-2. Authorization and Access Control

Description

After identification and authentication is properly performed, the system knows who a user is. The next equally important step is to determine what permissions and access authorizations the user holds. Authorization and access controls are an essential part of maintaining need-to-know and privacy policies and protecting sensitive information. They also support data integrity by restricting the rights to modify information to those who are authorized to do so.

Purpose

This authorization and access control chapter provides an overview of the methods and technologies used to define, enforce, and manage the allocation of resource access permissions to users of justice information systems. A discussion of some of the unique access management issues encountered in sharing information among disparate organizations is also provided.

Principles

- Access privileges should be granted based on a written policy that identifies user roles and the information required by individuals performing in that role.
- Access to multiple information systems should be managed with as much central control as possible. Where diverse organizations are involved, the system software that supports access management must honor the access policies of each organization while automating as much of the administrative process as practical.
- Access management policies and procedures should be defined to permit user privileges to be easily modified, added, or deleted by authorized administrators.
- User privileges should be auditable.

Policies

Well-defined access policies are important to the security of an information system. The policy statement should provide clear guidelines on how to assign, remove, modify, authorize, and audit access privileges. The policy should consider the sensitivity of the information, need-to-know considerations, and privacy restrictions. The Global Security Working Group maintains a library of policy samples at the Web site <http://www.it.ojp.gov>. (For more information and examples of access control policy statements, refer to *The Missouri OSCA Data Security Guidelines, Access Controls*.)

Best Practices

Managing and controlling access to information resources is a long-standing and well-studied problem. As a result, there is a rich and evolving set of technologies to address the problem. There are two fundamental types of access control: mandatory and discretionary, sometimes referred to as MAC and DAC, respectively. MAC and DAC can be defined as follows:

Mandatory Access Control (MAC)—In most MAC-based systems, both users and information resources are labeled. A familiar MAC implementation is the one used for national security information. In that implementation, the labels may include "Unclassified," "Confidential," "Secret," and "Top Secret." In order to obtain access to secret information, the user needs at least a "Secret" clearance. In this regard, access controls are mandatory—they cannot be changed at the discretion of the system administrator.

Discretionary Access Control (DAC)—In DAC systems, there are no explicit security-level labels on users and information. The system administrator plays a much more significant role in assigning permissions to users. Access to a resource may be granted to a user based on the discretion of the system administrator. Although there is no formal concept of security level, DAC systems are usually based on some kind of policy that instructs the administrator on how to determine who gets access to what.

This section focuses primarily on DAC, since it is the dominant type of access control in justice applications. While attempts have been made to define security levels and labels for information, there is no well-accepted standard on par with the national security-level MAC system. Lack of standards, however, does not eliminate the need to understand and categorize the access sensitivity of information. This topic is addressed further under Section 8, Data Classification.

DAC is typically implemented through some form of an access control list (ACL). A sample ACL appears in Table 2-2: Sample Access Control List. The ACL is a table that allocates the right to access an "object" to "subjects." An access right traditionally includes permissions such as *create*, *delete*, *read*, *write*, and *modify*. A subject might be a specific user, such as "Officer Jones," or a group of users, such as "police officers." ACLs are typically implemented in vendors' system software products. An operating system (such as Windows 2000) will have an ACL, as will a database management system (such as Oracle).

Table 2-2: Sample Access Control List

Subject	Access	Object
Officer Jones	Create, read, modify, delete	Criminal history database
Officer Jones	Read	Arrest record database
Officer Smith	Create, read, modify, delete	Criminal history database

Role-Based Access Control (RBAC)—builds on the model for an ACL subject. In RBAC, permissions are associated with roles, and users are made members of appropriate roles. This model simplifies access administration, management, and audit procedures. The role-permission relationship changes much less frequently than the role-user relationship. RBAC allows these two relationships to be managed separately and gives much clearer guidance to system administrators on how to properly add new users and their associated permissions. RBAC is particularly appropriate in justice information sharing systems where there are typically several organizationally diverse user groups that need access, in varying degrees, to enterprisewide data. For example, when Officer Jones joins the police, he/she will be given the information access privileges that are due the "police officer role." Some of these privileges may be associated with information maintained by other organizations, such as the sheriff or the courts.

Environments in which users must gain access to multiple information systems create additional administration and management challenges. Each information system will maintain its own ACL. The administrators for each system will be required to maintain current and accurate ACLs that may include users from other organizations. There will need to be policies and procedures used to validate the credentials of users from external organizations. Ideally, the ACLs would be integrated so that, within a single organization, access to multiple information systems can be managed in a centralized manner, and across multiple organizations, additions and changes to access privileges can be coordinated and supported. Products and technologies that address this problem are named Extranet Access Management (EAM).

The problem of managing access to multiple applications is not a new one, and several solutions exist. For example, the well-known mainframe utility, Resource Access Control Facility (RACF), allows the system administrator to manage user access permissions to multiple databases and software applications. There are mechanisms within the mainstream server operating systems (e.g., Netware, Windows 2000, and UNIX) to establish privileges for registered users on different systems. EAM tools extend the ability to centrally manage access to a wide variety of information systems, including Web services. The problem becomes more complex as the information systems become more diverse and spread over multiple agencies. In some cases, for example, the administrators from "Agency A" may not want users from "Agency B" to be automatically added to their system by "Agency B" administrators without their explicit knowledge and approval. The ideal access management solution will honor the user permission policies of each agency it serves while making administration as easy and automated as possible. The following technologies support this type of solution.

Lightweight Directory Access Protocol (LDAP)—Lists of users and their privileges (ACLs) are typically stored in data structures called directories. The standard for accessing directories is the LDAP. While LDAP is only an access method and does not define the content or format of the ACL information, it is a broadly implemented standard and provides an important tool to enterprisewide access management.

Security Assertion Markup Language (SAML)—SAML is an emerging standard and does not yet have broad industry support. SAML is Extensible Markup Language (XML)-based and provides a standardized way to exchange information about authentication and access privileges. Industry watchers predict that it will improve the integration of access control and management among multiple, diverse information systems.

References

For applicable standards, see:

- Lightweight Directory Access Protocol (LDAP): <http://www.ietf.org/rfc/rfc1777.txt>.
- Security Assertion Markup Language (SAML): <http://www.oasis-open.org/committees/security/>.

2-3. Data Integrity

Description

Data integrity refers to the processes and mechanisms used to ensure that data cannot be accidentally or maliciously modified, altered, or destroyed. In order to maintain data integrity during operations such as transfer, storage, and retrieval and to ensure preservation of data for their intended use, several threat types must be addressed by policy, practice, and/or security technologies.

Purpose

The task of trying to maintain data integrity is compounded by the fact that threats can originate from hardware defects, software errors, poor design concepts, internal component and telecommunications interference (noise), friendly humans, and hostile humans, to name just a few. The purpose of this chapter is to discuss some of the more common threats to data and some of the preventative security measures available.

Best Practices

System Failures, Communications, and Program Threats—There are many possible causes of data corruption in a computer system, such as electronic noise, physical hardware defects, hardware design errors, data communications and transfer, and software (systems) design errors.

Most system managers rely on basic precautions such as a properly sized, uninterruptible power source (UPS) and instituting an offline data backup program to protect against data integrity problems resulting from hardware, software, and/or communications systems failures.

For situations where businesses cannot afford to risk the integrity of their data, purchasing specialized equipment can provide additional protection. Systems are available, usually at increased cost, that deploy parallel processors that cross-check each other's output and perform end-to-end checksums on all data being transported.

Unintentional Human Threats—Users who want to simply view a file but are unfamiliar with read-only viewing tools may revert to using file editors. When editors are used to view data, it is very easy to unintentionally delete or modify characters while reading a file.

When deleting files, extreme care must be taken to not delete some files by mistake. This is especially true when using a wild card command. If, for example, in order to delete files coff001.dat through coff009.dat, the command "delete coff*.dat" is used, a file that should be retained called coffee.dat will also be deleted. Selecting the wrong backup tape, when doing a file restore, is a common way to corrupt data, as well.

Unintentional human threats should be addressed by using improved software utilities and training, training, and more training.

Protection can be improved by using good file name standards, access control restrictions, and utilities that detect and compensate for possible human error. For example, most properly installed and configured tape management utilities will prevent restoring a file from other than the most current finalized backup copy. If an older version needs to be used, a manual override must be applied.

Utilities that come with most of today's modern operating systems can be configured to provide protection from many of the unintentional user threats. For example, many file deletion utilities can be configured to create a backup copy of every file that is deleted. Although there are software solutions available to restore deleted files and to correct corrupted records, there is little that can be done to prevent the harm that can come from using data that has been corrupted.

Unintentional human threats will continue to evolve with improvements in technology. The more common threats will be eliminated by software improvements, only to be replaced by threats that are introduced by new software capabilities. Systems administrators must remain aware of the situations and software vulnerabilities that contribute to unintentional human threats. Software remedies should be implemented when available, and policy updates combined with training should be used to address the threats that remain.

Intentional Human Threats—Intentional human threats are, unfortunately, not limited to external perpetrators. Disgruntled and/or dishonest employees with access privileges and knowledge of the target system(s) pose significant threats that are much more difficult to detect.

External Human Threats—Other chapters of this document describe some of the security services available to reduce the risk of intrusions and protect internal resources, including data, from being compromised. Two of the primary objectives provided by this suite of security services are *origin authentication* and *content authentication*.

Both origin and content authentication are required to protect systems resources, and it is common for both to be provided by the same security services.

Origin authentication allows the identity of a message originator to be verified. This service denies access to unauthorized originators and counters the threat of masquerades. Content integrity service complements origin integrity service by allowing the originator to provide proof that the content of a message has not been modified.

Content integrity methods vary somewhat depending upon the type of origin integrity being used. The basic methodology involves the sender including an integrity control value that is computed using a cryptographic algorithm or private key to "fingerprint" message content. Message content is used to construct the integrity control value or hash value so the probability is minute that another piece of plaintext or encrypted text could hash to the same value. The longer the hash, usually 112–168 bits, the more minuscule the probability.

The receiving system uses the same hash algorithm and/or digital signature to recalculate the hash total for the message received. If the recalculated hash matches the hash sent with the message, the message was not altered while in transit. It is recommended that hash totals be at least 128 bits.

When digital signatures are used to support data integrity, a public key infrastructure (PKI) may be required to manage encryption keys. The PKI keeps track of the assignment and revocation of public encryption keys to users and organizations.

Public keys are associated with a user or an organization by using a computer file called a "digital certificate." The digital certificate includes the certificate holder's name, serial number, and the identity (name and digital signature) of the "Certification Authority" that assigned the certificate.

When used to provide integrity services, a hash derived from the block of data to be protected is encrypted with the sender's private key. This encrypted hash code is the sender's digital signature. Upon receipt, the sender's digital signature is decrypted and a new hash function calculated from the protected data block. If the sender and recipient's hash values match, the data has not been altered. The fact that the digital signature of the sender was created using his private key also provides "nonrepudiation" (i.e., the sender cannot deny that it was his message).

As an alternative to digital signature and PKI, secret cryptography can be used to provide data integrity. A secret key application is simpler in that only one key is used and must be in the possession of both the sender and the recipient for the encryption and decryption to function. Secret key systems are widely used but suffer from the difficulties that come with the task of distributing the secret keys in a secure manner.

Internal Human Threats—Data integrity cannot be maintained adequately without protection from disgruntled and dishonest employees. Sections 1-2, Physical Security, and 1-3, Personnel Security Screening, within this chapter, cover some of the core security services and policies that are necessary to reduce the risk of internal human threats. For example, all employees that handle sensitive information should have background checks completed (see Section 1-3, Personnel Security Screening, in this chapter), and a separation of duties should be implemented. If an employee does not need access to systems resources, deny access (see Section 1-4, Separation of Duties). Consider creating a security policy manual that includes a chapter on internal threats for employees to have on hand. Implement two-level authentications (what you know and what you have), strict password policies, and logoff procedures for access to information resources. And last but not least, use audit system and intrusion deletion software.

Prevention and Recovery

- **Prevention**—The following simple precautions can significantly reduce the chances of experiencing data integrity problems.

- Back up data and other software resources on a regular schedule, and store current copies at a secure off-site location.

- Avoid using freeware or any other software that does not originate from a trusted source.

- Back up data at intervals determined by the length of the recovery process.

- Always use up-to-date virus protection software.

- Have a properly maintained UPS and power-conditioning equipment operational at all times.

- Enable auto-save features in system software and utilities, when available.

- Implement and maintain auditing/detection tools capable of detecting and reporting changes to mission critical system files. See Section 3-1, Intrusion Detection Systems, in this chapter for more information.

❑ **Recovery**—Prepare a thorough plan for responding to data integrity problems. This plan can be a subset of the Intrusion Detection Response and/or Disaster Recovery Plans. More information on recovery planning is available at <http://www.cert.org/security-improvement/modules/m06.html>.

References

❑ Federal Information Processing Standard Publication 180-1, April 17, 1995. Service Hash Standard, <http://www.itl.nist.gov/fipspubs/fip180-1.htm>.

❑ MD5 Command Line Message Digest Utility, Author - John Walker, <http://www.bacula.org/html-manual/md5.html>.

2-4. Data Classification

Description

One of the key steps in securing electronic information is to determine what data needs protection. Information varies in its degrees of sensitivity, need for integrity, and its criticality. Therefore, the required protection measures to secure the data vary also. An information classification scheme should be developed to designate classes of information and their associated protection measures.

Purpose

Data classification describes methods to categorize information for different levels of security protection. Alternatives vary in rigor (i.e., the degree of protection that they provide) and cost. Cost can be in dollars or in manual effort. In general, rigor and cost are directly proportional—the more rigorous a method, the more it costs. The justice information system owner should select methods that provide as high a level of assurance as possible within cost constraints.

Principles

The level of assurance of the classification method employed should be balanced against the cost and the risk associated with unauthorized disclosure, uncontrolled modification, or the inability to access the data by authorized users. Information is classified based on its need for:

- Confidentiality or sensitivity (i.e., its need to be protected from unauthorized disclosure).
- Integrity or accuracy (i.e., its need to be protected from unauthorized alteration or destruction).
- Availability or criticality (i.e., its need to be available to the users).

An owner should be designated for each set of information. Generally, this should be the person in charge of the unit that produced the data. It is the responsibility of the information owner to determine to which class the information belongs and to whom the information may be disclosed. The security administrator ensures the proper classification measures, as determined by the information owner, are enforced according to the security policy. There should be mechanisms in place to allow audits and reviews of the classifications assigned and associated security measures implemented. All data should be classified, regardless of the media on which it resides.

To achieve increased granularity when securing data, use data classification in conjunction with Role-Based Access Control (see Section 2-2, RBAC).

Policies

Once an organization decides on an approach for classification, it should document the policies, providing a consistent and comprehensive application of classification throughout the enterprise. The policy should identify scope, methods, standards, and organizational and individual responsibilities. The reader may refer to the following documents for examples of classification policy statements:

- The Missouri OSCA Data Security Guidelines, Section 5.5.1, Information Sensitivity Levels.
- The University of Massachusetts, Data Classification section, <http://www.umassp.edu/policy/data/itcdatasec.html>.
- Institute for Intergovernmental Research, Sample Operating Policies and Procedures, <http://www.iir.com/28cfr/sample_operating_Policies_procedures.htm>.

Best Practices

The following tables represent sample data classification schemes under the categories of confidentiality, integrity, and availability, respectively. Under the confidentiality category, Table 2-3 suggests five levels in order of increasing sensitivity: public, internal, confidential, restricted, and sealed. Under the integrity and availability categories, Tables 2-4 and 2-5 suggest four levels: very low, low, medium, and high.

Table 2-3: Confidentiality Classification

	Public	Internal	Confidential	Restricted	Sealed
Description	Not sensitive; available to anyone	Slightly sensitive; not intended for external entities	Sensitive; required to be controlled	Very sensitive	Extremely sensitive
Impact of Unauthorized Disclosure	N/A	Adversely affect the organization	Adversely impact the entire system, individual persons, and the public; incur financial or legal liabilities; and undermine confidence in and the reputation of the organization	Seriously impact the entire system, individual persons, and the public; incur serious financial and legal liabilities; and damage confidence in and impair reputation of the organization	Severely impact the entire system, individual persons, and the public; may cause loss of life; organization may be disbanded; and irreparable destruction of confidence in and reputation of the organization
Possible Examples	Criminal convictions; published phone numbers	Internal phone numbers; organization charts	Criminal cases with "not guilty" verdicts, open paternity cases, and ongoing investigation documentation	Personnel information, court documents on juveniles and adoptions	Sealed or expunged court cases
Access	All	Available to employees and approved nonemployees	Available to employees and authorized nonemployees with a nondisclosure agreement	Available to select employees and authorized nonemployees with a nondisclosure agreement, granted on a need-to-know basis, and an access list must be maintained	Available to specific individuals and only in exceptional cases, granted on a need-to-know basis, and an access control list must be maintained

Table 2-4: Integrity Classification

	Very Low	Low	Medium	High
Definition	80 - 90% error-free	90 - 95% error-free	96 - 99% error -free	100% error-free
Impact of Unauthorized Modification	Adversely affect the local organization	Adversely impact the entire system, individual persons, and the public; incur financial or legal liabilities; or undermine confidence in and reputation of the organization	Seriously impact the entire system, individual persons, and the public; incur serious financial or legal liabilities; or damage confidence in and impair reputation of the organization	Severely impact the entire system, individual persons, and the public; may cause loss of life; organization may be disbanded; or irreparable destruction of confidence in and reputation of the organization
Possible Examples	Public Web page displaying information on elected officials	Court schedules	Public access to records of conviction or court judgments	Records of conviction for law enforcement use, fingerprint and other identification records for law enforcement use, emergency contact information for the public, warrants and orders of protection

Table 2-5: Availability Classification

	Very Low	Low	Medium	High
Definition	No interruption of access beyond 30 days	No interruption of access beyond 7 days	No interruption of access beyond 1 day	No interruption of access
Impact of loss in availability	Adversely affect the organization	Adversely impact the entire system, individual persons, and the public; incur financial or legal liabilities; or undermine confidence in and reputation of the organization	Seriously impact the entire system, individual persons, and the public; incur serious financial or legal liabilities; or damage confidence in and impair reputation of the organization	Severely impact the entire system, individual persons, and the public; may cause loss of life; organization may be disbanded; or irreparable destruction of confidence in and reputation of the organization
Possible Examples	Public Web page displaying information on elected officials	Court schedule	Public access to records of conviction	Records of conviction for law enforcement use, fingerprint and other identification records for law enforcement use, emergency contact information for the public, warrants and orders of protection

References

- ANSI Standard A/I 11179, Information Technology – Specification and Standardization of Data Elements – Part 2: Classification for data elements.

- U.S. Department of Energy, EO12356. See Oak Ridge National Laboratory Web site, <http://www.fas.org/sgp/library/quist2/chap_7.html>, Classification Levels.

2-5. Change Management

Description

Security is achieved by establishing a set of controls, configurations, protocols, policies, and practices. Systems are never static and neither are the controls, because things change. But uncontrolled change means an unknown state of control, so change must be managed. In this way, the state of our security measures, the knowledge of who has access to make changes and what types of changes, will be known at any given time. Capability to roll back changes, if they prove inoperable or problematic, and to change schedules to meet business needs will be possible.

Purpose

Change management is important for minimizing security risks and ensuring business continuity. It describes methods, approaches, and policies which organizations can use to make system changes in a controlled way and to assure that configurations are standardized, documented, and maintained. Different organizations will have varying needs, dependent on such factors as whether software is outsourced or developed in-house and how the network infrastructure is provided and maintained.

Principles

- All programs, settings, and configurations should be documented, and that documentation should be kept current. The documentation provides an authoritative source for how things are intended to function. Program documentation includes requirement documents that tell the story of what functions the users should expect, design documents that show how the system meets those business needs, documentation of the program code that addresses what business rules are being implemented and the origin of those rules, and data dictionaries that explain what the various data elements are and what the coded values indicate. Network and hardware configurations are documented in network diagrams and in various logs that document set-up and maintenance activities.

- Changes to programs or physical infrastructure should be documented using a change request process. This process should show the reason or source for the change. It should have rules about who in the organization must approve what types of changes.

- Access to critical systems should be limited and controlled. Limiting access reduces the risk that systems will be compromised and reduces the work involved in incident response. Controls need to be in place to assure that access limits are enforced. Actual access should be monitored and tested.

The overall approach is to document what we expect the system to look like, to have a process to assure that changes are approved and added to the documentation, and to control who can make changes to the systems.

Policies

Access Control Policy—This policy should address who can have access to critical systems and infrastructure and how this access will be controlled. It should also address the methods to be used to audit compliance. The access control policy should incorporate separation of duties so that any single staff member has a limited scope of influence.

Documentation Policy—This policy should establish what the required documentation should be for each critical system, whether software or hardware. The documentation should address current status or configuration. It should also provide some context for why the system settings are as they are. In software, this may tie back to the business rule that is being implemented. For infrastructure, it should reference overall network design documents.

Change Request Procedure—For each critical system type, this should address how to ask for a change, what information needs to be supplied, who needs to approve that change, how it is to be implemented and tested, and how the change is to be documented in the system documentation.

Audit Plan—Policies are useful, but to assure compliance with controls and procedures, staff needs to understand and expect that there will be some type of periodic audit activity. The audit plan may need to be treated as a confidential document, since it will address how controls are tested.

Best Practices

Evaluate all network design documents, security policy and procedure documents, and application architecture documents from a security risk perspective before publishing or otherwise disclosing them. Create tools and establish practices for reviewing the operation of internal controls and conducting audits of their effectiveness.

Establish procedures and internal controls on how changes can be made to network components, applications, or security settings. Limit the scope of changes that a single individual can make. If possible, require two or more individuals to make changes.

Establish a notification procedure that determines who must be notified for what types of changes and within what time frames. Create and maintain a set of approved standard configurations. When changes are made, the date and time of the change, the objective of the change, the details of the change itself, and the implementing and approving of staff members should be logged.

Establish a procedure for keeping software patches current. Set standards for acceptable elapsed time between the issuance of a patch and its implementation. This includes antivirus software.

Samples of Best Practices

- Develop and enforce a change management policy.
- Convene an Infrastructure Configuration Control Board (ICCB) with members of key management and section chiefs.
- Develop and enforce architectural and engineering standards.
- Create a test and integration laboratory.

Reference

- *IEEE/EIA STD 12207*. Software Lifecycle Processes, <http://standards.ieee.org/reading/ieee/std_public/description/se/12207.0-1996_desc.html>, <http://standards.ieee.org/reading/ieee/std_public/description/se/12207.1-1997_desc.html>, and <http://standards.ieee.org/reading/ieee/std_public/description/se/12207.2-1997_desc.html>.

2-6. Public Access, Privacy, and Confidentiality

Description

Public access denotes the extent to which the public (and the news media representing the public) are able to view and copy information collected and used by a criminal justice entity. It includes not only whether a particular piece of information is available to the public but also when, where, and how access is provided. The principle public access issue today is the extent to which information is made available electronically, especially on the Internet. In the past, much information—for instance, court files—has been public as a matter of law but private as a matter of practice due to the difficulty of accessing it. Only those who are intimately familiar with the operations of the entities know how to obtain the information. When court and other criminal justice entity data is placed on the Internet, or otherwise made available electronically, information that was protected by its "practical obscurity" becomes readily, cheaply, and practically available to the public and to the news media. Disclosure of certain information can be life-threatening to the subject: for example, victims of domestic violence (when the victim is at risk if the abuser locates the victim) or a criminal informant (if the criminals with whom the informant is associated learn of the informant's status).

Confidentiality is the assurance that information is shared only among authorized users. The sensitivity classification level of the information should determine its confidentiality and, hence, the appropriate safeguards.

Privacy requires confidentiality mechanisms. Privacy applies to when, how, whom, and to what extent personal information is shared. There exists no explicit federal constitutional right to privacy. However, privacy rights have been articulated in federal and state case law and statutes governing the areas of medical, financial, educational, and consumer data.

Personal information may be linked to an individual at the time of release or subsequently linked through analysis. It may be accessed or released inappropriately, causing possible loss of employment, diminished social status, or other highly adverse consequences. Personal information may include:

- Race, national or ethnic origin, religion, age, sex, sexual orientation, or marital or family status.
- Education, medical, psychiatric, psychological, criminal, financial, family, or employment history.
- Any identifying number, symbol, or other particular assigned to the individual.
- Name, address, telephone number, fingerprint or voiceprint, photograph, blood type, or DNA.

Purpose

Criminal justice entities have historically dealt with and instituted policies concerning access to the information they collect in the course of their work. For instance, the National Crime Information Center (NCIC) has had privacy and security policies in effect for over thirty years. However, the ubiquity of electronic data and electronic documents, their exchange among criminal justice agencies, and their increasing availability over the Internet have caused the public, legislators, and criminal justice entities themselves to reexamine their historic practices. Entities are deciding that certain "public" information should no longer be public or should be made public only through traditional, paper-oriented processes. Further, concerns about public access, privacy, and confidentiality of their data create reluctance on the part of some criminal justice entity leaders to enter into information sharing arrangements. Consequently, it is critically important in today's environment for every entity to review and restate its own public access, privacy, and confidentiality policies and for information sharing agreements to include formal understandings regarding these matters.

Principles

- The public possesses statutory, First Amendment, and common-law rights to access most justice information.

- Justice agencies use information to protect society at large. The way in which a justice agency uses personal information in the administration of justice is crucial to the protection of society and can result in life-or-death consequences. Confidentiality is required during open investigations to preserve information sources, prevent interference with the enforcement proceedings, ensure a fair trial, prevent disclosure of investigative techniques and procedures, and preserve life and safety.

- An individual's right to privacy has been articulated in state and federal case law and statutes governing the areas of medical, financial, educational, and consumer data.

- Conflicting interests must be weighed between the data subject, justice system, and the public, including the media and commercial sector.

Policies

- Washington State Privacy Policy, <http://www.wa.gov/dis/aboutdis/pdpnotice.htm>.

- Justice Information Privacy Guideline, Developing, Drafting, and Assessing Privacy Policy for Justice Information Systems, National Criminal Justice Association, September 2002, <http://www.ncja.org/publications.html#>.

- State of Arizona, Government Information Technology Agency, Statewide Privacy Policy, <http://gita.state.az.us/policies_standards/html/p170_privacy_policy htm>.

Best Practices

Public Access—Public access has changed with the development of technology. Privacy issues for public access include:

- **Should the information be made public at all?** Keep in mind the possibility of lawsuits for inappropriate release or for not releasing information, as well as the need to release data necessary for public safety. Also, once data is made public, it is forever public and beyond the control of the disseminating agency. Corrections and updates might be impossible to circulate. Each justice component must have some public access method.

- **At what point should justice information be made public?** For example, information should remain closed during an investigation but be made public during the trial.

- **How long should it be accessible?** Should there be a record that the deleted record once existed?

- **What is the fiscal cost of making the information public?** Ideally, it should be disclosed using all access methods (in person, telephone, or Internet). Should fees be charged to recoup the cost, or would the charges be so high that they unreasonably limit access to the information? A privacy plan must be implemented that protects the privacy of the information yet allows the agency to still protect society at large. A plan is necessary to ensure standardized implementation and enforcement of privacy.

Privacy Principles—The first step in implementing a privacy plan is to develop a privacy policy. Those developing privacy policies should look at all applicable laws, regulations, and policies already in effect. More often than not, legislative action may be needed to put the policy in place. There are eight principles to be included in the privacy policy that enforce privacy of personal information while allowing the agency to perform its vital function:

- **Purpose Specification**—Document the purpose for which personal information is collected no later than the time of data collection. Design technology to allow access restrictions to outside parties.

- **Collection Limitation**—Collect personal information by lawful and fair means, and try to collect only pertinent data. Where applicable, obtain the subject's consent. Design the technology to not require unnecessary data.

- **Data Quality**—Personal information collected must be accurate, complete, and current. Public access to inaccurate data may be worse than no access at all. If the subject has access to the data, allow for them to verify the data. If the subject does not have access, set up other means for verification, such as passive data analysis, including cross-referencing that identifies anomalies. Require logging whenever the data is accessed or modified, recording the

changes by whom, when, and for what reason, to ensure accountability. Try to include tags for confirmed or unconfirmed and accurate or inaccurate.

- **Use Limitation**—Personal information is to be used solely for the purposes specified, except with the consent of the data subject, by authority of law, for the safety of the community, or pursuant to a public access policy. Use limitation is generally applicable to disclosure outside the justice system but may also apply between agencies if disclosure is not mandated by law. The policy should also consider possible secondary or third-party usage of the information. An audit trail should be incorporated in the technology to enable a use assessment.

- **Security Safeguards**—Protect personal information with reasonable safeguards against risk of loss or unauthorized access, modification, use, destruction, or disclosure. A risk assessment should be performed with security modifications made as necessary. Also, an information classification review should be done periodically to ensure data is being safeguarded at the proper security level. The system should log all attempts to alter information or attack the system.

- **Openness**—Provide notice to the data subject about how the personal information is collected, maintained, and disseminated. Provide notice to the public of the existence of personal data and access to data in accordance with a public access policy. Openness includes public access to the management practices of the data, except where it directly relates to an investigation, a pending or open case, or safety concerns and other factors that a government determines as necessary exceptions. The technology system must log all transactions on an individual's file and allow for independent oversight for accountability purposes.

- **Individual Participation**—Allow affected individuals to access their personal information, except where it would compromise an investigation, case, or court proceeding. Subjects should be able to:

  - Obtain confirmation that the agency has their data.

  - Obtain data relating to them within a reasonable time, at a charge (if any) that is not excessive, in a reasonable manner, and in a form that is readily intelligible.

  - Be given reasons if an access request is denied.

  - Challenge a denial and, if successful, have the data erased, rectified, completed, or amended.

  - Provide an annotation to data where an organization decides to not amend the information as requested.

The technology must be designed to create copies of the personal information and to amend or annotate information subject to disagreement over accuracy. The system must also have the capacity to notify third parties, in a timely manner, which have either provided or received incorrect information.

- **Accountability**—Oversee and enforce the other seven privacy principles. An individual must be designated as the information steward responsible for establishing regular security audits, privacy impact assessments, and privacy audits. The steward should have a procedure in place for challenges to the system and should assure that timely, fair responses are made to inquiries. He is also responsible for training staff on privacy protection requirements.

  A privacy plan requires cooperation between each agency accessing the data. Sharing personal information becomes even more difficult because agencies have different functions and differing statutes and regulations. What one agency considers sensitive may be open to the public in another agency. For instance, information from closed-record states becomes publicly available once it is shared with an open-record state. Compiling public data from several different agencies may also yield obviously confidential information.

  Current systems range from paper-driven to the highly automated. Also, many of the current systems were developed without proper thought to privacy concerns. This can result in having to manage unintended privacy issues and having to retool the system—both of which can be quite expensive. The ideal is to address privacy during the planning stages of information system design.

  Each agency should classify the information they create and maintain with an appropriate confidentiality level (see Section 4, Data Classification, in this chapter). Procedures should be documented stating when and where this information may be disclosed to the public or other agencies. Disclosure should be determined by the type of information and the context in which it is shared. For example, local security procedures should be classified at least at Level 3. Each agency must also review the privacy and public access policies of the agencies with which it exchanges information. To ease the transfer of data, the agencies should adopt the same terms, data entry fields, data definitions, and data structures.

  The information steward for each agency should perform a Privacy Impact Assessment which has three components:

  - A map of the information flow. Each justice agency should map the flow of the information it maintains. The map must include each data element in the justice record. At each mapped decision point, it should indicate the type of received information, the purpose for which it may be used, whether it is personally identifiable, and when and to whom it may be disclosed.

- A privacy analysis of the information flow, indicating adherence to the privacy policy.

- An assessment of the issues uncovered in the analysis and options to mitigate privacy risks.

After each agency has performed their Privacy Impact Assessment, a second assessment should be completed on the entire integrated information sharing system for the information exchanged between agencies.

References

- Organization for Economic Cooperation and Development (OECD), Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, <http://oecdpublications.gfi-nb.com/cgi-bin/OECDBookShop.storefront/EN/product/932002011P1>.

- Health Insurance Portability and Accountability Act (HIPAA) of 1996, Standards Model Compliance, <http://www.cms.gov/hipaa/>.

2-7. Firewalls, VPNs, and Other Network Safeguards

Description

The trend toward increasing network connectivity has increased the threat to information resources. There are many tools available to mitigate the risk of exposure of justice information systems that results from interconnection to public and private networks. This discipline focuses on those that are in the most common use and represent a minimum level of precaution that system owners must take to protect against network-related threats—firewalls, virtual private networks (VPNs), and virus protection systems.

Purpose

Technologies such as firewalls, virtual private networks, and virus protection systems have become a fact of life for justice system managers who want to benefit from the connection to public and private networks but need to protect their information resources from outside, malicious threats. Well-planned and configured implementations of these technologies can mitigate many of the threats associated with data sharing and allow the true value of the information to be achieved.

Principles

- The rules table in the firewall should reflect an organization's security policy and be as restrictive as possible. The basic computer security tenet which should be the basis of all security policies is "That which is not expressly permitted is denied."

- Whenever public networks are used to provide communications between two parties that may exchange sensitive justice information, a VPN should be used to protect the confidentiality of that information.

- Up-to-date virus protection software should be maintained on all workstations and servers that process sensitive information.

Policies

A comprehensive set of security policies should be developed and maintained through periodic review and updates. The System Administration, Networking, and Security (SANS) Institute has developed a suggested list of security policies which an organization should consider. They include:

- Acceptable Use Policy
- Encryption Policy
- Audit Policy

- Antivirus Policy
- Remote Access Policy
- Password Protection Policy
- VPN Security Policy

Best Practices

Firewalls—Firewalls are a security system to protect a network containing servers, client computers, and intelligent communication devices from intentional or accidental damage or unauthorized access implemented by either hardware or software. Firewalls typically provide three fundamental services:

- Packet filtering rejects packets from unauthorized hosts and rejects connection attempts to unauthorized services. Packet filtering should be implemented to eliminate traffic for services that are not being utilized. It should also be used to eliminate traffic related to specific known security weakness.

- Network Address Translation (NAT) translates the Internet protocol (IP) addresses of internal hosts to hide them from outside monitoring. NAT can allow use of IP addresses that are not routable on the public Internet.

- Proxy services make high-level, application-based connections on behalf of internal hosts to break the network layer connection between internal and external hosts. Proxy services can incorporate a high level of intelligence that can scan traffic for known security issues.

Many firewall products incorporate all the above features into a single product, providing multiple security benefits.

Today, most firewall hardware configurations utilize two network adapters on a common machine to create a dual-homed host firewall. One network adapter is attached to an unsecured environment, and the other is connected to a network that is being protected. Many firewalls are equipped with a third interface that creates a demilitarized zone (DMZ). This provides a location to place servers that need to deliver services to external users while still establishing a level of security that would not be available if the server were located directly on an unsecured network, such as the Internet. Examples of servers that might be located on a DMZ are Web servers or electronic mail servers that provide connectivity services to the Internet. Whether two or three interfaces, the basic purpose of these configurations is to limit security risks by putting some intelligent agent between the network interfaces to control access from one interface to another interface. This intelligence may be in the form of a proxy application or a packet filter.

A firewall proxy is an application that acts as an intermediary between trusted and nontrusted networks. The proxy application fulfills requests for service that come from the public network by interfacing with the necessary resources on the private side. By handling the

outside request itself, the proxy server makes sure that no "outsiders" communicate directly with private servers. Most security professionals consider the proxy-based firewall to be the most secure; however, the type of traffic (Web, electronic mail, etc.) and service requests that a proxy firewall will handle can be limited.

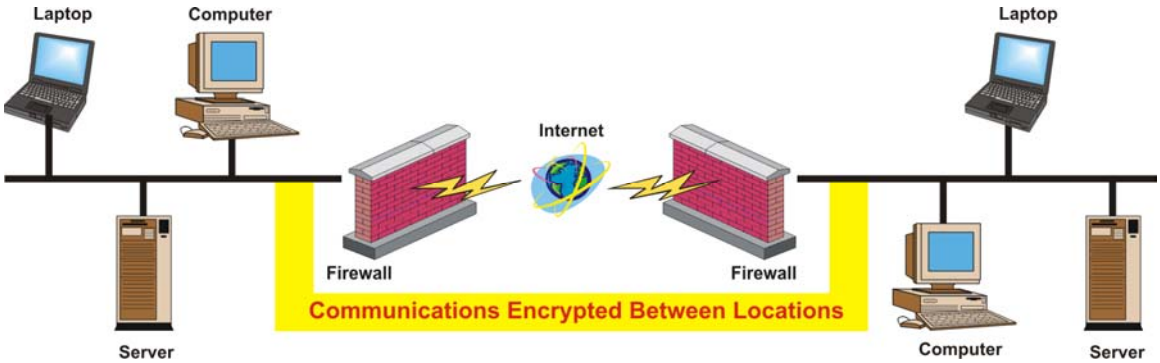
Packet filter firewalls are another more basic alternative. These firewalls use a rule table that identifies valid communications paths by endpoint (e.g., source address X is allowed to communicate with destination address Y) and the types of messages that can flow over each path. The level of protection offered by a packet filter firewall depends on the quality of the rule table. This technology, when paired with well-thought-out rules governing a packet filter firewall, can limit connections based on source and destination, combining to create a secure and flexible firewall alternative.

The growth of always-on, high-speed Internet connections has helped to proliferate a new type of firewall known as personal firewall software. This software is installed on a user's computer and evaluates all incoming and outgoing network communications. Personal firewall software performs essentially the same function as a stand-alone, hardware-based firewall, except it only protects the computer on which it is installed. Many security-conscious users are taking a layered approach to firewall deployment. A hardware-based firewall is deployed to protect the majority of system resources that reside on a network, and personal firewall software is used to protect particularly sensitive data on a computer.

Regardless of the type of firewall that is chosen, it is imperative that research be done to determine what services are required. Once this analysis has been performed, the firewall should be configured to allow only the types of traffic that are absolutely necessary. Default settings should be rigorously reviewed. Default passwords should immediately be changed. Additionally, changes should be made to adapt the system to meet the user's specific needs.

Virtual Private Networks (VPNs)—VPNs are a technology that allows two or more networks and/or hosts to connect over a wide area network (WAN) or public network, such as the Internet, while having the appearance and functionality of being connected with private communications lines. VPNs can be used to connect local area networks (LANs) in different locations (see Figure 2-1: Site-to-Site VPN). The technology is also used to connect individual remote users to resources on a remote network for telecommuting. VPNs operate by encrypting transmissions of data between two systems after each system has authenticated itself to the system with which the communication is being shared.

Figure 2-1: Site-to-Site VPN

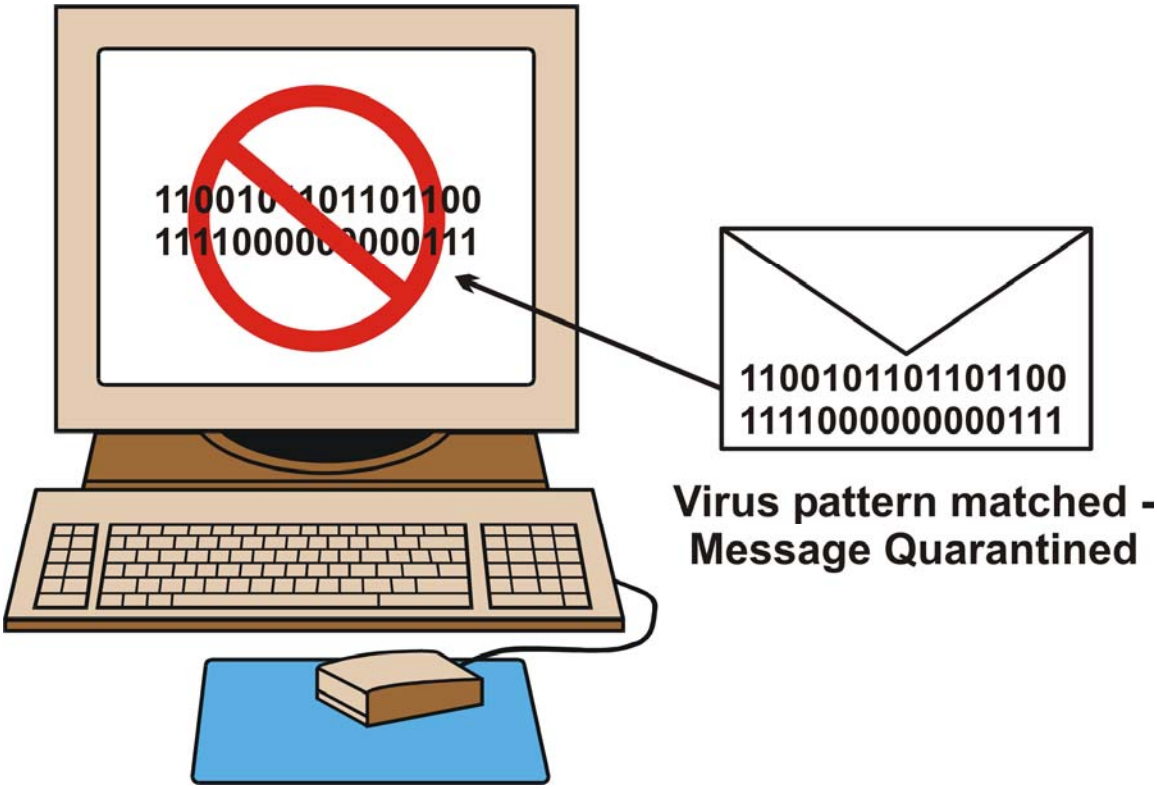


Antivirus Software—A computer virus is a malicious set of programming instructions that are disguised and incorporated into files. When activated, they perform some task designed to infect the recipient's computer. Viruses are typically activated by opening a file that has executable code. The task that a virus performs varies greatly. Some viruses may delete or rename files. The most common computer viruses today are carried as attachments to electronic mail that infect the computer and then send copies of infected files to many other recipients. This is particularly troublesome because the e-mail recipients that receive the infected messages generated from the infected system are taken from its e-mail address book. The result is a message that many times appears to have come from someone the recipient trusts. This misplaced trust may cause the recipient to open a message, never suspecting that the content may have a copy of the virus that will be perpetuated. Some of the more common file types that are susceptible to computer viruses have the following extensions: exe, bat, vbs, scr, pif, and doc. Files with the "doc" extension are Microsoft Word files. These files are susceptible because of the macro programming language capabilities that are available in Microsoft Word and several other Microsoft Office products.

The increase in viruses and the publicity surrounding them has created a related threat—the virus hoax. A virus hoax is a message that informs the recipient of an e-mail message of a virus threat that may have a potentially devastating outcome. The message seems to come from a credible source and informs the recipient to notify everyone they know of the danger; however, the goal of a virus hoax is to clog e-mail systems with a message that has no real credibility. Some of the signs that an e-mail message may be a hoax are that it typically reports dire consequences that a virus may inflict, using very emphatic terms which are frequently all capitalized; it typically is believable, citing a source that may be associated with a credible organization; and it typically calls for action by usually requesting the recipients to send the message to everyone they know. The intended result is loss of time and energy to deal with the issue at hand.

There are a couple of things that can be done to protect agencies from these annoying and potentially destructive distractions. Minimally, every desktop computer should have an antivirus software application installed on it. It is preferable to install antivirus software at the server level as well, if possible. This is typically a more controlled environment that information system professionals can monitor, hopefully reducing the chance of error or omission. Antivirus software examines files and looks for patterns that have been previously associated with known viruses (see Figure 2-2: Antivirus Software Pattern Searching). The antivirus software can be configured to look at all files or only selected files that may be more prone to infection. Second, just like human viruses, computer viruses are capable of being mutated. Antivirus software uses a list of known viruses to match potential viruses it may detect. This list of virus definitions should be updated regularly on all computers. Most of the larger providers of antivirus software are capable of being configured to update these files automatically on a computer as long as the computer has access to the Internet. Finally, much should be learned about what viruses and hoaxes are being circulated. There are several mailing lists that can be subscribed to that provide early warning information. F-Secure, Symantec, and McAfee are very reputable antivirus software providers that offer this service. The Web sites of these vendors are also extremely helpful in dealing with both viruses and virus hoaxes.

Figure 2-2: Antivirus Software Pattern Searching



References

- Generally Accepted System Security Principles (GASSP) as defined by the International Information Security Foundation, <http://web.mit.edu/security/www/GASSP/gassp11.html>.

- The National Institute of Standards and Technology – Computer Security Division, Computer Security Resource Center (NIST CSD CSRC) maintains a compilation of many computer-related security best practices, <http://csrc.nist.gov/>.

- Internet Protocol security (IPsec) is a set of protocols developed by the Internet Engineering Task Force (IETF) to support secure exchange of data at the IP layer. IPsec has been deployed widely to implement VPNs, <http://www.ietf.org/html.charters/ipsec-charter.html>.

Security Disciplines for Objective 3: Detection and Recovery

3-1. Intrusion Detection System (IDS) 2-67
3-2. Critical Incident Response 2-71
3-3. Security Auditing 2-79
3-4. Disaster Recovery and Business Continuity 2-83

3-1. Intrusion Detection System (IDS)

Description

Intrusion detection is the process of monitoring events occurring on a network or in a computer for evidence of intrusions, which can be unusual usage patterns or attempts to bypass security to compromise the integrity, availability, or confidentiality of a network or computer. An Intrusion Detection System (IDS) is just one of the many safeguards required to protect an organization's information technology resources.

An IDS can be compared to a home alarm security system because they both provide an alert when an abnormal or predefined event occurs. IDS technology has evolved over the past 20 years, and IDSs currently available can identify the type of event that has taken place, when the event occurred, and in some cases, the sources of the intrusion. The more advanced IDSs provide the capability to program automated responses and deterrents to some alerts.

Purpose

IDS technology allows organizations to protect their systems from the ever-escalating threats that come from their growing dependence on information systems and network connectivity. IDS technology is by no means a total security solution. It represents a very necessary component in an organization's arsenal of security tools.

IDSs are gaining acceptance as a vital addition to most organizations' security infrastructures. Despite this growing acceptance, IT professionals still must struggle to justify the acquisition of IDS technology. An IDS will allow an organization to:

- Detect probes or penetrations that are not prevented by other security measures.
- Prevent problems by increasing the perceived possibility of being discovered, which is most effective with an organization's employees.
- Document the existing threat. This feature helps justify the cost of additional security measures.
- Measure the effectiveness of current security infrastructure.
- Collect useful information about intrusions that could direct recovery efforts and support civil or criminal legal remedies.

Principles

- The risk to and value of information resources protected by the IDS deployed should be balanced against the cost of the system and the perceived vulnerabilities.

- IDSs are designed to monitor and protect networks and host computers. Both capabilities are usually required to provide comprehensive detection.

- IDSs should not run on the host and target systems they are designed to protect. Any attacker that successfully attacks a host or target system could simply disable the IDS.

- Increased bandwidth on a network may equate to increased risk. An increase in raw bandwidth by a factor of ten means that an attack that would normally take ten days to accomplish can take place in one day. Intentionally slow attacks that are spread out over ten days can become much harder to detect because they can be imbedded in ten times more data.

Policies

IDSs are designed to detect attacks on network and host computers and to detect violations of internal system's usage policies that should be documented as part of the security policy. A properly structured security policy is needed to serve as a template for determining how an organization's IDS will be configured. The policy should explain in detail what the IDS operational staff is to do when a violation is reported and the violator is identified. The security policy should clearly define what system components, if any, can be accessed by the public and determine if there are any restrictions placed on the level of access for each component. The security policy should include any special legal, accreditation, or audit requirements that will impact the configuration of its IDS.

Best Practices

It is generally agreed that a properly configured IDS should include both host computer and network protection and should accomplish the following tasks:

- Detect/validate and report that the system's resources have been compromised.

- Determine and report how the system's resources were compromised.

- Preserve data documenting the compromise of each component.

- Determine and report any changes to the system as a result of each compromise.

- Determine and report any data that has been viewed or retrieved as a result of each compromise.
- Determine and report if the system's resources are being used by foreign executables introduced by a system's compromise.
- Determine and report the source of each compromise.
- Assist proactively in halting any compromise detected.
- Assist in recovery and restoration of all resources altered by a system's compromise.

Many IDSs use signature-based detection and anomaly detection routines to identify an intrusion. Signature-based detection routines are based on recognizing known patterns. They are not effective when a new pattern is introduced and often recognize known patterns only after the target system(s) has been compromised. Anomaly-based detection systems can detect new but unusual exploits earlier in a compromise attempt, but they are highly prone to false-positive alerts. A single IDS, on a busy network, can produce over 1,000 alerts per hour during peak periods. This level of reporting activity often leads to alerts being ignored when anomaly-based detection is producing a high number of false-positive alerts.

Some of the newer IDSs are handling the management of high-alert volumes by providing an enterprise-level security management capability to cross-correlate alerts from multiple IDSs. These devices can develop a global enterprise knowledge that can be used to eliminate many false-positive alerts and standardize reporting from different IDS vendors. When these security management consoles are networked with other security consoles and security management services to create a Distributed Intrusion Detection (DID) system, the alert data from many different sources can be captured to provide a global view of malicious network activities. This information allows detection, analysis, and remedial activities to get under way much earlier. This cooperative process was recently credited with stopping the rapid spread of the worm called "LION" that was implanting software to launch denial-of-service attacks. More information on DID systems can be obtained at <http://www.incidents.org/>.

References

The highly proprietary nature of vendor-supplied IDSs has slowed the development of industry standards. The Internet Engineering Task Force, Intrusion Detection Working Group (IETF/IDWG) is developing a Detection Exchange Protocol. This standard protocol will allow different IDSs to communicate in a standard format. The IDWG has published the following four documents for review and eventual distribution by the Internet Engineering Steering Group as requests for comments (RFC), located at <http://www.ietf.org/ids.by.wg/idwg.html>:

- Intrusion Detection Message Exchange Requirements.
- Intrusion Detection Message Exchange Format Data Model and XML Document-Type Definition.
- The TUNNEL Profile.
- The Intrusion Detection Exchange Protocol (IDXP).

The Defense Advanced Research Program Agency has funded development of the Intruder Detection and Isolation Protocol (IDIP). IDIP is designed to integrate IDSs and automate response components under development at the University of California, Davis. IDIP integrates various IDSs and major components, such as hosted firewalls, routers, and network management components. The result of this integration is the capability to trace and block intrusions that traverse multiple network boundaries. For more information on IDIP, see "Summary of the Intruder Detection and Isolation Protocol Project" at <http://seclab.cs.ucdavis.edu/projects/idip.html>.

3-2. Critical Incident Response

Description

Critical incident response should be a part of a comprehensive information security program. The components of a critical incident response program include a warning network that communicates actual or potential risks in time for intrusions to be prevented, IDSs, and other technical tools and processes for uncovering breaches in security and reporting them to a central response team (CRT). The CRT will ideally be able to modify security parameters in the target information systems in time to prevent costly attacks to resources.

The cornerstone of incident response capability is an incident response plan that documents the parameters of response to an incident affecting information infrastructure. An information infrastructure incident is a real, perceived, or threatened event that involves data, agency applications, computers, networks, or communications with the potential to have a major negative impact on business operation. The plan uses a risk-management approach to characterize appropriate responses to incidents ranging in seriousness from no direct impact to customers to major disruption of agency operations or significant impact to the agency reputation.

Purpose

In conjunction with a notification network and CRT, a well-defined, documented, active incident response plan allows effective, efficient, and coordinated response to adverse circumstances, such as cyberterrorism and cybercrime. Incident response plans define the process of characterizing and responding to information infrastructure incidents that significantly impact critical business functions. Incident response plans document procedures for responding to situations that affect the ability to provide services to customers or meet legal or regulatory requirements. The communications network used to collect and disseminate security-related information provides internetworked criminal justice agencies with technical information, tools, methods, assistance, and guidance. The existence of a dedicated, central team allows proactive response to threats and provides liaison activities and analytical support. The team provides a focal point for collaborative relationships with federal civil agencies, the U.S. Department of Defense, academia, and private industry.

Principles

- Incident response plans detail the responsibilities and actions to be taken to identify, notify, contain, eradicate, recover from, record, and report incidents. Creation of the plan should lead to:
  - Facilitating timely assessment of potential problems.
  - Ensuring a coordinated and comprehensive response to incidents that cross agencies.

- Minimizing the impact of information infrastructure incidents on the ability to provide service.
- Maintaining a positive public image and credibility.
- Facilitating prosecution of offenders, as appropriate.

❑ Procedures for responding to attacks (e.g., unauthorized access, denial of service, and virus infections) must be defined, documented, and tested. They should be linked with administrator/user communication and training. Automated systems management tools can notify administrators of attack, but procedures ensure the desired response. Specific procedures in the incident response plan must detail the following:

- How a decision to activate the plan is made and by whom.
- Rapid notification, deployment, and coordination of community resources to assess and respond to the incident.

❑ The plan describes a central organization to implement the response and includes definition of the roles of the team leaders and members.

❑ The plan defines a central organization responsible for providing the communication vehicle(s) and establishing service(s) in support of agency incident handling and reporting. Agencies request assistance from that central organization, as needed, to troubleshoot unusual or difficult-to-isolate threats.

❑ The plan establishes out-of-band communication alternatives wherein the "compromised" device, platform, or media is not used to notify users or to report the incident.

Policies

Incident response priorities and procedures should be defined consistently with the security policy for the target information systems. The security policy should define the organizational responsibility and the priorities associated with incidents related to specific resources.

Best Practices

The incident response plan provides a collection point for the practices and "minimum" requirements related to critical incident response, as agreed to by the community. The following items, as best practices, need to be clearly defined within the incident response plan document.

Central Response Team (CRT)—The CRT registers security coordinators for contact at community member organizations. It collects "requests for response," proactively monitors the environment within its sphere of control, and remains connected to higher-level communications networks. As the CRT creates or receives computer security alerts, it forwards them to all community chief information officers (CIO) and/or security coordinators. Each alert states, as a minimum, the identity of the risk, level of risk, and any available patches or inoculants to mitigate the risk. The CRT frequently informs the help desk(s) of the status and progress of any incident.

Organizational Responsibilities—A central security organization will use risk analysis instruments to determine what security threats are present to assets under the community's control or custodianship. As threats are identified, ways to eliminate them or reduce them to acceptable levels will be put in place, with the full support of organization management. Internetworked partners must establish a mechanism that defines responsibilities for responding and reporting incidents and for sharing information about potential threats and intrusions in two directions.

Agency responsibilities include monitoring their own networked resources using an IDS. Upon receiving a security alert, agency CIOs and/or security coordinators notify agency personnel about the alert to raise awareness and reduce the number of help desk calls. When possible, alert notifications are sent by e-mail, and based on the content, determination should be made whether to distribute to "Agency All," specific divisions within the agency, or only to specific individuals. Security coordinators report any local incidents to the CRT and work with team members to contain and recover from incidents.

Help Desk Responsibilities—As problems are reported by users, data is collected and communicated to the CRT for determination of incident level and response required. Incident status/response progress must be tracked for communication to any affected customers who call. The help desk can also act as a valuable out-of-band communication source for the CRT, depending on the particulars of the incident.

Phases of Response

- **Alert Phase**—The alert phase is the process of learning about a (potential) security incident and reporting it to the CRT. Alerts may arrive from a variety of sources, including firewalls, intrusion detection systems, antivirus software, threats received via electronic mail, and media reports about a new threat. Many of these alerts will be processed by the CRT Incident Analysts and will be presented as requests for response, requiring triage.

  When incident notification is phoned in by an agency to a central help desk, on-duty help desk personnel complete the request for response and notify the Incident Manager. The Incident Manager then responds directly to the contact at the compromised agency.

- **Triage Phase**—The request for response, with all available information about the incident, gets processed by the Incident Manager to determine whether a real incident exists. A severity level is assigned.

  If the incident's severity warrants Level 4 or 5, (see Levels of Incidents, in this section), the CRT will also notify all other concerned parties in the agency/community. The CRT Manager, while collaborating with all concerned parties, must accomplish two important tasks in this phase:

  - Decide whether to "pursue" or "protect." In other words, decide whether the community will attempt to catch the perpetrator(s) of the attack for later criminal or civil action or whether it simply wants to stop the incident and restore normal operations. This decision must be made *before* the response begins, because it influences how the response will be undertaken.

  - Allocate resources and authority (personnel and financial) to the response and recovery teams at a level commensurate with the severity of the incident.

- **Response Phase**—CRT response engineers then gather evidence (audit trails, log files, and contents of files). If the "pursue" option was chosen in the triage phase, this process will be performed in a forensically sound manner so that the evidence will be admissible in court. The team may need specialized technical assistance and advice from a third party.

  Once evidence has been gathered, it is analyzed to determine the cause of the incident and the vulnerability or vulnerabilities being exploited. An assessment is also made of how far the incident has spread (i.e., which systems are involved and how badly they have been compromised). The CRT then determines the most effective methods to stop the incident and/or eliminate the vulnerabilities.

- **Recovery Phase**—The recovery phase can overlap with the response phase as the CRT response engineers begin to actually restore the systems affected by the incident to normal operation, working with agency security personnel. This may require reloading data from backup tapes, reinstalling systems from their original distribution media, or commencing alternate-site operations. Once the affected systems have been restored, they are tested to make sure they are no longer vulnerable to the attack(s) that caused the incident. They are also tested to make sure they will function correctly when placed back into production.

- **Maintenance Phase**—To develop "lessons learned," the CRT reviews the incident, as well as the response, to determine which parts of the incident response plan worked correctly and which parts need improvement.

The areas needing improvement are then corrected, and the plan is updated and communicated accordingly. Other areas that need to be changed (policies, system configurations, etc.) may also be identified during this phase.

Levels of Incidents—Table 2-6 describes sample criteria that could be used to classify a security incident level and suggests accompanying responses in the incident response plan. (Actual definitions and levels of response have to be negotiated among community members.)

Table 2-6: Security Incident Levels and Responses

Incident Level		Response
1	Small numbers of system probes or scans detected on internal systems; isolated instances of known computer viruses.	Easily handled by installed antivirus software.
2	Small numbers of system probes or scans detected on external systems; intelligence received concerning threats to which systems may be vulnerable.	Communicate potential risk to security coordinators, CIOs, and help desk contacts and remind about installing latest patches and virus signatures.
3	Significant numbers of system probes or scans detected; penetration or denial-of-service attacks attempted with no impact on operations; widespread instances of known computer viruses easily handled by antivirus software; isolated instances of a new computer virus not handled by antivirus software.	CRT must allocate available resources to monitoring/communicating to prevent damage.
4	Penetration or denial-of-service attacks attempted with limited impact on operations; widespread instances of a new computer virus not handled by antivirus software; some risk of negative financial or public relations impact.	CRT takes action, in coordination with system administrator(s) affected, to prevent more widespread damage.
5	Successful penetration or denial-of-service attacks detected with significant impact on operations; significant risk of negative financial or public relations impact.	CRT notifies business leadership, authorized action initiated, all available resources allocated at CRT and affected agency(ies).

Central Response Team (CRT) Roles and Responsibilities—The CRT consists of the Manager, Incident Manager(s) (depending on size of community), Incident Analysts, and Response Engineers. Their suggested roles and responsibilities are as follows:

- **CRT Manager**—The CRT Manager oversees the operation of the CRT and provides communication and coordination functions at the highest level, including notification of incidents, their severity, and the status to various officials, agency leaders, organizations, and committees. Immediately upon discovery of a Level 4 or 5 incident, the CRT Manager receives a full briefing from the Incident Manager. Only the CRT Manager has the authority to approve disconnection or quarantine of a community member agency in response to an incident. The CRT Manager assists with decisions to pursue legal action by coordinating with the appropriate legal authorities when necessary.

- **Incident Manager**—The incident manager manages the overall response and recovery activities for all security incidents, deciding the severity level of each incident and assigning staff members to perform response and recovery tasks accordingly. Additionally, the Incident Manager consults with the victim agency regarding the decision to pursue legal action and gather evidence or quickly react to protect the affected systems and return operations to normal as quickly as possible. When disconnection authority has been granted by the CRT Manager, the Incident Manager informs the victim agency of the recommendation to shut down or disconnect all affected systems from the network.

- **Incident Analysts**—Incident Analysts are responsible for the 24-hour-a-day/7-day-a-week monitoring of Intrusion Detection System data. They process requests for response from monitored data and directly from the central help desk and member agencies. A request for response may be submitted by the on-duty Incident Analysts before the victim agency is even aware of the incident. When a request for response is processed and completed, the Incident Analyst sends it to the Incident Manager for a severity level designation and Response Engineer assignment. Incident Analysts may also perform trend analysis and other proactive duties as assigned by the Incident Manager.

- **Response Engineers**—The Response Engineer functions represent the core of the central response and recovery efforts. Being highly skilled in the technical details of IT security, Response Engineers perform the initial incident response; collect and gather evidence for forensics; assist with incident policy development and incident response education; and perform postincident compliance, restoration, and vulnerability testing. Based on skill levels, Response Engineers are assigned specific incident response tasks by the Incident Manager and may be assigned other proactive duties as seen necessary by the Incident Manager.

Reference

One sample standard can be found on Arizona's State Web page. Arizona's standards document, P800-S855, *Incident Response and Reporting Standard*, provides a sample for a working, multiagency program, including a CRT membership application. It is available at <http://gita.state.az.us/policies_procedures/p800_s855_incident_resp.htm>.

3-3. Security Auditing

Description

A security audit consists of examining and verifying that the security of the information technology system(s) has been properly implemented according to the organization's security policies, government regulations, and perceived security risks.

Purpose

The audit discipline defines the standards and procedures that need to be implemented to confirm that a security policy has been properly implemented and maintained. The ever-increasing complexity of security policies will require equally complex audit procedures to guarantee that all aspects of the security policies are respected.

Principles

- Objectivity of auditors must be guaranteed by selecting a team independent from the team who implemented and/or maintains the security infrastructure. When possible, an independent organization from the IT department should be considered.

- Qualification of auditors must match the level and complexity of the security policy put in place.

- Audits must be performed on a regular basis to ensure proper maintenance and application of security policies over time. At a minimum, organizations should alternate between internal and external audits every other year.

- Auditors must look beyond the IT systems and consider also the human interface to the IT system.

- The security audit must begin with the security policy to assess its relevance and completeness.

- Previous audits' findings must be reviewed to ensure that appropriate corrective measures have been applied.

- Audit trails must be maintained to provide accountability for all security administration activity.

- The audit organization must provide assurance that it is following applicable auditing standards.

- Audit reports must contain sufficient information to enable outside parties to ascertain the evidence that supports the auditor's conclusions.

- Details of noncompliance should be communicated to the appropriate level of management to allow for the development of a corrective plan of action.

Best Practices

Project Preparation—It is important that auditors have an understanding of the organization under review. They must have the proper security clearance to access the systems holding the data. Auditors must decide how selective the audit must be and how deep it needs to go with each of the system's components. All security auditing tools must be verified for accuracy and reliability, and the scope of the audit should be clearly defined at the beginning of the project.

It is recommended that auditors have experience with risk analysis and management in order to properly assess the level of exposure created by each noncompliance finding.

Information Gathering—The process for gathering information should include formal and informal interviews with technical staff, end users, and other personnel services.

The auditor must check all documentation related to the system in place, focusing on details with security implication, and determine if users have seen and read the security policy.

Reporting—The audit report should have a logical structure, including an executive summary, prioritized recommendations, the scope of the audit, more detailed information followed by final conclusions, and detailed recommendations.

All findings must be clearly explained with the facts and information that was gathered during the information-gathering phase.

If previous audits have been done, the new audit should document whether or not the previous findings have been addressed.

Remediation—Once the written report has been presented, all responsible personnel should meet to discuss what action items should arise from the audit. Due dates must be attached to each action item in order to ensure that necessary changes are implemented prior to a security breach.

References

- Washington State Information Technology Security Policy Audit Standards, <http://www.sao.wa.gov/StateGovernment/ITSecurity/ITStandards.htm>.

- NIST: Security Self-Assessment Guide for Information Technology Systems, <http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf>.

3-4. Disaster Recovery and Business Continuity

Description

A disaster is any event that can cause a significant disruption in operational or computer processing capabilities for a period of time. Disasters can include the loss of a critical file, the rapid spread of a virus, a denial-of-service attack, the loss of a network segment or critical link, or loss of an entire facility or personnel from a fire or bomb. Although the probability of a major disaster is remote, the consequences of an occurrence could be catastrophic, both in terms of operational impact and public image. Disasters have an uncanny habit of occurring at the most inconvenient times, damaging equipment and materials one can least afford to lose.

Disaster recovery focuses on handling the immediate emergency, whereas business continuity takes effect after a disaster and focuses on getting the critical business functions operational and eventually restored to full capabilities. Together, they cover what to do, beginning with the emergency response; continuing through crisis management, prioritized business operations recovery, and detailed recovery; and ending with full business restoration. Knowing what needs to be done before, during, and after a disaster can prevent panic, reduce the extent of the damage, and help in a coordinated recovery effort.

Purpose

The purposes of disaster recovery and business continuity plans are to prevent serious impact, to avoid disruption of services, and to coordinate the recovery tasks so that normal business operations may resume as quickly as possible. Plans are different from one organization to another because risks vary widely, as do the organizational priorities and goals. There is also a wide range of alternatives available in both method and technology. These alternatives vary in rigor (i.e., the security assurance level or the degree of protection that they provide) and cost. In general, rigor and cost are directly proportional—the more rigorous a method, the more it costs. The information system owner should look to methods that provide as high a level of assurance as possible within cost constraints.

Principles

- The amount of time and effort put into a plan should reflect the value of the information or service provided by the organization and the amount of effort required if the system had to be rebuilt from scratch. It is normally much more cost-effective to prevent or minimize damage than to repair it after the fact.

- The disaster recovery plan should address procedures such as employee safety, emergency services notifications, family and employee notifications, operational communications, identification of key personnel, emergency authorizations, power and hardware recovery, media backup and recovery, and maintaining event logs.

- The business continuity portion should address procedures such as manpower recovery, alternative business processing methods, administration and operations, budget for replacements and/or insurance, customer service, identification of key vendors, office supplies, public affairs, and premise recovery. Nontechnical management should own and control the business continuity plan in order to ensure proper funding.

- The plan should be practiced and tested. A failed test of the plan still provides valuable information about the organization and where changes should be made. It is also an invaluable tool to train personnel on how they should react in an emergency.

- No matter how good a plan is when first finished, it will almost immediately become out of date. Constant review and update is required to keep the plan pertinent and useful.

Policies

Once an organization decides on an approach for disaster recovery and business continuity, the policies for that approach should be documented. The guideline ensures the consistent and comprehensive application of disaster recovery throughout the information enterprise. The guideline should identify scope, methods, standards, and organizational and individual responsibilities. The reader may refer to the following documents for examples of disaster recovery and business continuity policy statements:

- Massachusetts Institute of Technology, Emergency Response System, <http://mit.edu>, and search on "emergency response system."

- Massachusetts Institute of Technology Business Continuity Plan, <http://web.mit.edu/security/www/pubplan.htm>.

Best Practices

Disaster Recovery Team—A team needs to be assembled that will respond in the event of a disaster. This team should include a member of management, members of the technology unit that will perform the assessment and recovery, representatives from facilities, and members from the information user community to determine what level of recovery is needed and to verify when recovery is complete. The team takes an active part in developing the plan and carrying it out in the event of a disaster.

Threat/Risk Assessment—A threat is anything that can adversely affect the operation of an organization; i.e., fire, natural disaster, virus, bomb, and strike. The threat assessment is the process of formally identifying the nature of the threats and degree of damage each can do to an organization. This includes damage to all assets, including, but not limited to, personnel, facilities, computer systems, and reputation.

The risk assessment takes the threats identified for the organization, assesses the adequacy of the controls in place, determines the expected loss for each threat, and then establishes the degree of acceptability to system operations. It will also recommend changes to controls to improve the current security protection. Steps include the following:

- Assess the current computing and communications environment, including personnel practices, physical security, operating procedures, backup plans, systems development and maintenance, database security, data and voice communications security, systems security and access control, application controls, security administration, insurance, and personal computers. Inventory all equipment, and make a list of the vendors.

- Define all critical information needed to operate. Retention schedules, federal mandate, state law, or business needs will define this subset of data. Note the location of all critical information. Depending on the criticality of the information, either backups or safe storage containers should be considered. Store backups of critical information off-site.

- Define critical personnel, equipment, facilities, and single points of failure. Try for redundancy, or make arrangements to quickly replace these assets. Potential sources of failure include network, hardware, software, malicious attack, physical damage to the facility, and loss of personnel.

- Assess the insurance needs of the organization and the budget required to purchase replacements.

- Assess any dependencies on critical partners. Utilities, vendors, customers, and building partners are examples.

Business Impact Analysis (BIA)—Complete a BIA to identify the critical processes and functions of the organization.

- Set priorities for restoration based on the overall impact by looking at the interdependencies of the departments within the organization.

- Determine maximum acceptable losses, and define the window of time available to resume operations. The analysis will then define the restoration timeline and the possible need to use alternate facilities in different scenarios.

- List resources required to restore those critical functions identified in the BIA. This should include the hardware, software, documentation, facilities, personnel, and outside support needed for recovery. Different strategies could be formed for short-term, intermediate-term, and long-term outages.

Mitigation of Risks—Mitigate risks identified in the risk assessment by implementing new procedures and providing redundancy wherever possible. This includes cross-training personnel on other job duties as well as making plans for extra hardware and backup software.

Store electronic media in protective jackets or media boxes. Consider purchasing data safes (fire-resistant safes, specially designed to protect magnetic media from damage caused by magnetism, fire, heat, water, and airborne contaminants such as smoke and dust). A water vacuum or roll of plastic can be extremely useful with a water leak or malfunctioning sprinkler system.

Power is critical to computing environments. It is common to provide protection of computing equipment through UPS systems, connection to two different power grids, and the use of diesel generators.

Hardware Redundancy—The following techniques are used to provide hardware redundancy:

- **Disk Mirroring**—Disk mirroring is the duplication of data from one hard disk to another. Mirrored drives operate in tandem, constantly storing and updating the same files on each hard disk. Should one disk fail, the file server issues an alert and continues operating. Should the controller fail, access to either disk may be denied.

- **Disk Duplexing**—This is similar to disk mirroring except each drive has its own controller circuitry. Should one disk or controller fail, the file server issues an alert and continues operating.

- **Disk Arrays**—These enable the administrator to replace a failed drive while the server is still running, and users can continue operating. The system automatically copies redundant data on the file server to the new disk.

- **Hot Backup**—Two file servers operate in tandem, and data is duplicated on the hard disks of the two servers. This is like disk mirroring but is across two servers instead of one. If one server fails, the other automatically assumes all operations without any outage.

- **Cold Site**—A cold site is an emergency facility containing a heating, ventilating, and air conditioning (HVAC) system and cabling, but not computers. When outsourcing, evaluate providers on high availability and disaster tolerance. Such arrangements may be informal (as a reciprocal agreement) or formal (a separate recovery site or a contract with a third-party provider). Cold sites are generally cheaper than hot sites. They should be a reasonable distance away from the main facility to prevent the same disaster from destroying its capabilities as well as the primary facility. Also, they should not be overextended in the number of organizations for which they

provide this service. In a massive disaster, all of the organizations will want the facility at the same time.

- **Hot Site**—A hot site is an off-site facility contracted to have compatible systems ready to restore an organization's backups and run them as if in their own facility. Hot sites contain computers, backup data, and communication equipment. Written agreements should be signed if contracting with another unit for alternate processing of critical systems in the event of a disaster. Again, they should be a reasonable distance away from the main facility to prevent the same disaster from destroying its capabilities as well as those of the primary facility. They should not be overextended in the number of organizations for which they provide this service.

Software Redundancy—There are several different types of data backups. Determine the level and frequency of backups (e.g., daily incremental backups with weekly full backups). Consideration should be given to using more than one technique to better ensure the information gets backed up promptly.

- **Full Backups**—All files on a hard disk should be copied to a tape or other storage medium. These are used for total system recovery and are often done once a week.

- **Differential Backups**—These are done only for the files that have been changed or added since the last full backup. Earlier versions of these files will be replaced in differential backups and are often done nightly.

- **Incremental Backups**—These are completed only for the files that have changed or been added to a system since the last backup and are often done whenever work is finished on the computer. These backups use less storage space and are faster to run. They are generally used to aid in the recovery of old versions of files and the restoration of file integrity when files become corrupted.

- **Off-site Storage**—At least two copies of server backups should be made. One copy is kept on-site to restore files. The second backup should be stored off-site, or an electronic tape vaulting service should be used. A mutual agreement should be signed with the off-site facility to ensure that it provides the security needed to protect the information at the same level as that provided by the primary facility. Fire protection, air conditioning, heating, moisture control, availability, and other security factors should be considered. Regularly scheduled delivery of the backup media will help ensure the backups are available when needed. Backup and recovery functions should be limited to the administrator and alternate.

Plan Development—Procedures should be documented for various types of disasters, such as fire, flood, extended power outages, bomb threats, chemical spills, and loss of personnel. This phase also includes the implementation of changes to current procedures to help prevent disasters and to support recovery strategies and vendor negotiations with recovery services or off-site storage. Individual responsibilities for members of the Disaster Recovery Team should be defined, and recovery standards are also developed at this stage.

The first priority should always be the safety of personnel. Escape routes and evacuation procedures should be documented and made clear to all personnel, and the availability of adequate medical and first-aid supplies should be ensured.

Testing the Plan—Practice and test the plan. Set up a mock disaster, and work through the plan to discover its weaknesses and make necessary changes. Routinely perform restorations from the various kinds of backups (full, incremental, or differential) to ensure they will work when needed. Plans tested less than once a year will probably not support critical business requirements.

Plan Maintenance—Regularly review the plan once it is complete. The information within the plan constantly changes. Critical functions, telephone numbers, and job duties change. Even organizational priorities and goals may change.

References

- National Institute of Standards and Technology, Gaithersburg, MD: U.S. Department of State, Washington, DC, Domestic Disaster Recovery Plan for PCs, OIS, and Small VS Systems, see <http://www.ntis.gov/search/product.asp?ABBR=PB90265240&starDB=GRAHIST>.

- Federal Emergency Management Agency. Emergency Management Guide for Business and Industry: A Step-By-Step Approach to Emergency Planning, Response, and Recovery for Companies of All Sizes. Washington, DC: FEMA, 1993. Order from: Publications Distribution Center, Post Office Box 2012, Jessup, MD 20794. Telephone: (800) 480-2520.

- National Archives and Records Administration, Office of Records Administration. Vital Records and Records Disaster Mitigation and Recovery. College Park, MD: NARA, 1996. Available from: Publications and Distribution Staff (NECD) RM. G-9, National Archives, Washington, DC.

Chapter 3: Models for Justice Information Sharing

Introduction

The appropriate application of security practices is highly dependent upon the specifics of the information systems to be protected. Characteristics such as connectivity to public networks, the scope and composition of the user community, the sensitivity of the information, and the level of acceptable risk should all have strong influences on the security approach used. This chapter provides further guidance to justice information system managers and owners by defining general models for justice information sharing, recommending security guidelines, and citing usage examples.

The following sections describe four justice information sharing models that are frequently encountered in justice applications:

- The Joint Task Force (JTF) Model
- The Centralized Information Repository (CIR) Model
- The Peer Group (PG) Model
- The Justice Interconnection Services Network (JISN) Model

These four models are simplified representations of the organizational relationships, computer systems, and the flow of information encountered in the justice and public safety communities. They serve as illustrations of "best-of-breed" security practices. In application, most "real life" justice information systems are a combination of these models, although they are described here individually. The justice information system professionals faced with an enterprise that combines several of the models will need to identify common security services that can apply to all of their systems. It should be noted that some justice information system professionals may unpredictably encounter a fifth model: the disorganized, fragmented, run-by-another-part-of-the-city model.

Readers are encouraged to compare the four models against operational systems under their management so that the security guidelines may serve to provide useful advice on how to improve the protection of shared justice information.

Chapter Structure

In general, each justice information sharing model section is constructed as follows:

- Introduction
- Security Guidelines
- Operational Examples

Guidelines for Applying Information Security Practices

Each justice information sharing model includes guidelines for security practices. The guidelines are organized around the following: (1) the flow of information for each model and (2) the security disciplines defined in Chapter 2. The flow of information represents the principal sharing transactions in each of the models. There are many other aspects to securing computer systems, such as protecting the confidentiality and integrity of data storage. The focus of these guidelines is on secure information sharing in terms of the flow of information. With regard to the security disciplines, rather than repeat the general guidance provided in Chapter 2, Security Disciplines, these sections address only those elements that are unique and specific to each model.

It should also be noted that within these models, the issue of size and scope will also influence the selection of security practices—for small systems it may be impractical and/or prohibitively costly to apply the same level of security rigor appropriate to a large system. Since we have not provided a spectrum of guidelines based on available funding, it is incumbent upon system owners and designers to make the trade-offs between risk; information asset value; and investment in security technology, process, and procedure. Where possible, we provide ways that cost may be trimmed to accommodate budget constraints.

Current Information Sharing Systems and Their Relationship to Each Model

Under each model, existing, operational systems are identified, and it is shown how they map to the four justice information sharing models. The intent is to draw best practices from existing systems and, from those practices, develop the guidelines presented in the next section.

Table 3-1: Operational Examples of the Justice Information Sharing Models identifies examples of each model from the many justice information systems operating in our nation.

Table 3-1: Operational Examples of the Justice Information Sharing Models

Existing System	Sharing Model			
	Joint Task Force Model (JTF)	Centralized Information Repository Model (CIR)	Peer Group Model (PG)	Justice Interconnection Services Network Model (JISN)
Federal Bureau of Investigation National Crime Information Center (FBI NCIC)		√		
Arizona COPLINK			√	
Wisconsin Integrated Justice Information Sharing			√	
National Law Enforcement Telecommunication System (NLETS)				√
Regional Information Sharing Systems (RISS)				√
American Association for Motor Vehicle Administrators Network (AAMVAnet)				√

Justice Information Sharing Models

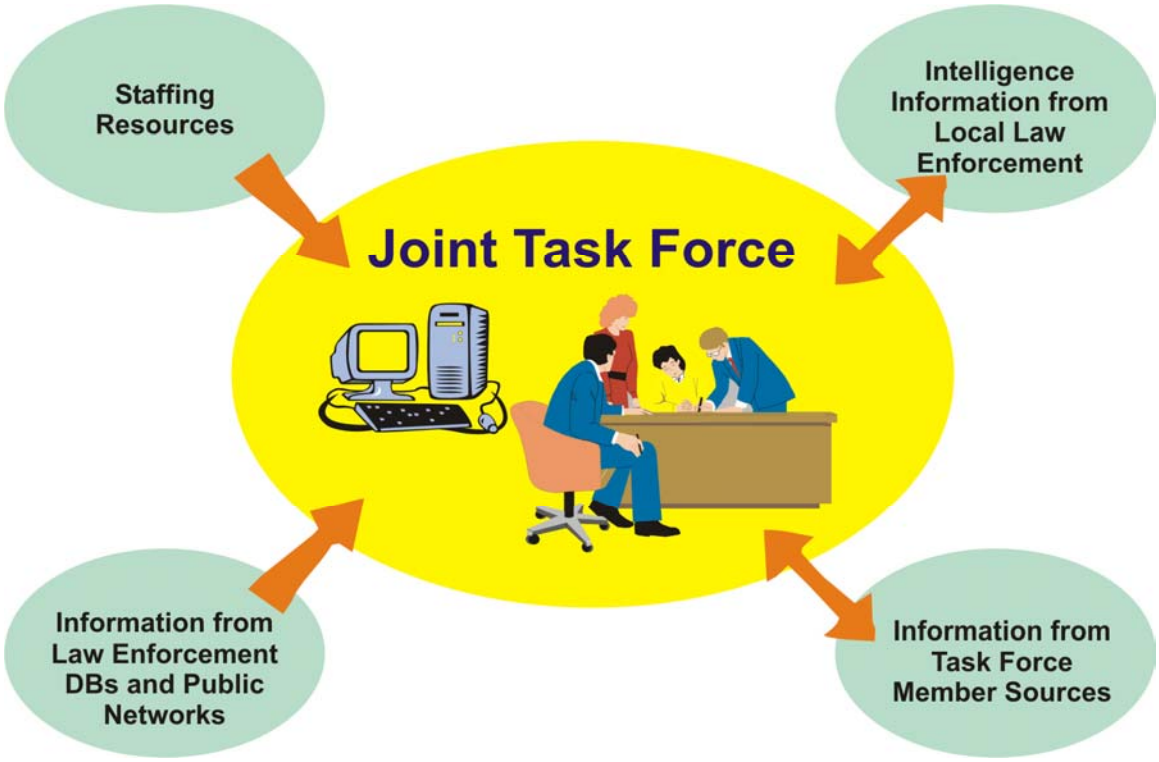
1. The Joint Task Force (JTF) Model 3-7
2. The Centralized Information Repository (CIR) Model 3-15
3. The Peer Group (PG) Model 3-31
4. The Justice Interconnection Services Network (JISN) Model 3-41

The Joint Task Force (JTF) Model

Introduction

It is often appropriate to combat a common threat by assembling a joint task force. The joint task force is typically made up of specialists from a wide variety of justice organizations within single or multiple jurisdictions. This model is represented conceptually in Figure 3-1.

Figure 3-1: The Joint Task Force Model



The task force model simplifies some of the problems associated with securely sharing information. The member specialists can be "cleared into" the task force by verifying that they meet predefined security background requirements. The task force members can define appropriate security rules independently from participant organizations. Within the operation of the task force, there is no strong need to accommodate the security practices established by each of the member organizations or to find a way to build "electronic trust" between the organizations. Instead, each participant organization must comply with the security policies and practices defined for the task force by the founding members.

However, there are many unique security challenges that typically accompany providing secure information sharing in the JTF model. In many cases, the task force is assembled rapidly, uses ad hoc facilities, and has limited access to information security expertise.

Further, the task force needs a written security policy that accommodates the restrictions placed on information that is funneled into the task force from outside sources.

The flow of information in and out of the task force involves:

Information from member databases—Task force members will bring information or access to information from their home organizations. For example, if an agent from a federal agency participates in a law enforcement task force, he will have access to information in case files that may be pertinent to the investigation at hand. It is the responsibility of the individual task force members to ensure that the security policies governing any information that they contribute are enforced, since the task force uses that information. In addition, the task force may wish to provide computing facilities to store and access information and make it generally available to all task force members. These facilities must adhere to the policies defined by the original owners of the source information.

Information from private, state, and national law enforcement information repositories—The task force may establish its own access to centralized repositories, such as the National Crime Information Center (NCIC), Integrated Automated Fingerprint Identification System (IAFIS), and LexisNexis, to support research and analysis activities. Many of these repositories have detailed information security practices governing the access and use of their data resources. The task force security policy must accommodate the practices required by government and private information repositories to which it provides access.

Intelligence information exchange with local law enforcement groups—Information in local databases spanning a very diverse set of sources, such as police, fire, motor vehicle, utility, and tax records, may be required by the task force. The task force must honor the use policies established by each of the information owners. Often the security policies associated with locally owned and maintained information may not be as well-defined as those for national level databases. In some cases, security and use restrictions for this type of information will be driven by privacy concerns.

The objectives of the task force information security policies and practices will be to protect these information flows, as well as maintain the security and integrity of the data stored on task force computing systems.

Security Guidelines for the Joint Task Force (JTF) Model

Security can be a critical success factor in the mission of a task force. Information leaks and misinformation in a law enforcement task force, for example, can undermine otherwise well-planned and well-executed investigations and operations. The focus of the guidelines in this section is to create as secure an information systems environment as possible to support the task force mission.

Figure 3-2: Security Practices to Support Information Flow Into the Joint Task Force Model overviews some of the security practices and mechanisms that apply to the joint task force information sharing model. At the center of the task force information systems environment is a computer system dedicated to task force use. This system generally includes a "server," providing database storage facilities, task force user PC workstations, and a local area network connecting the components and providing communications functions. Further, there may be workstations that are not connected directly to the task force server but provide access to external databases. Finally, there may be connectivity provided to public networks, such as the Internet, to further support communications, research, and analysis.

Figure 3-2: Security Practices to Support Information Flow Into the Joint Task Force Model

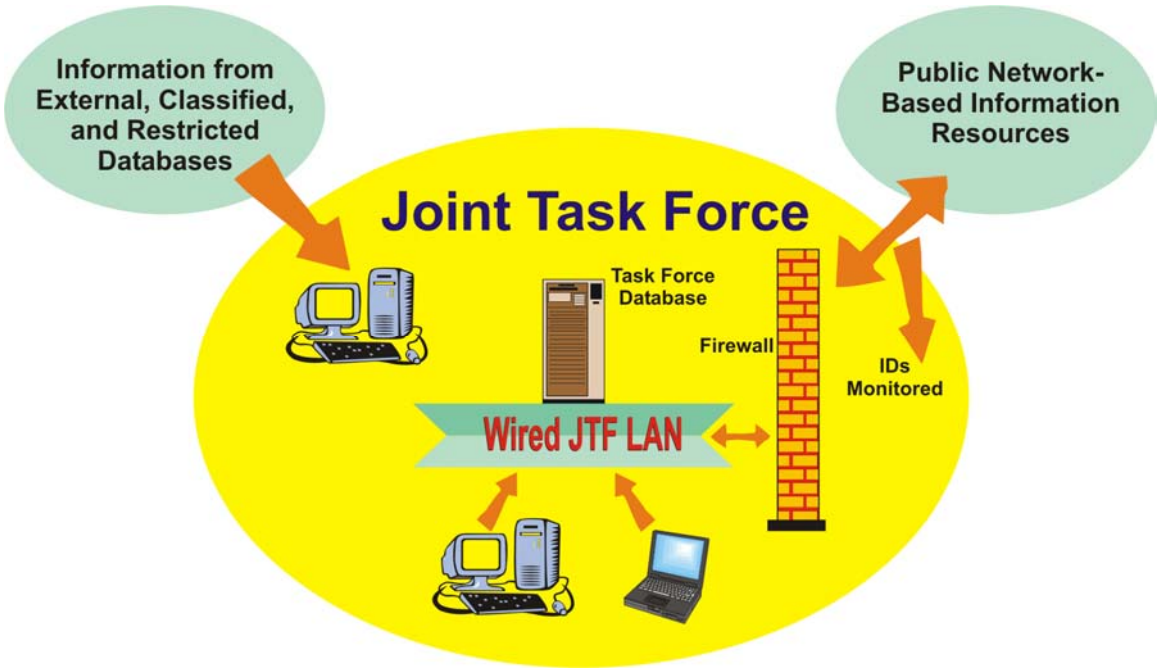


Figure 3-2 includes several security features that are geared towards secure information sharing among task force participants.

- **The LAN is wired, not wireless**—Wireless network technologies such as "WiFi" provide a very convenient local area networking mechanism, particularly for the quickly assembled systems common in joint task force initiatives. Unfortunately, the level of security offered by current wireless products is typically not suitable for protecting justice information. It is too easy for unauthorized PC workstations to connect to the JTF network. In some cases, it is possible for PC workstations or laptops that are located outside of the physical boundaries of the JTF "data center" to access the WiFi networks. Encryption mechanisms used in WiFi networks typically do not have rigorous enough protocols to adequately protect shared justice information in this environment.

- **Laptops are not permitted to connect to the LAN**—The JTF is typically a very dynamic environment. While some task force participants will prefer to work with laptop computers because of their inherent mobility, the laptop provides too easy a path for information to leave the confines of the JTF data center and increases the risk of access by individuals.

- **The connection between the server and the outside world is protected by a firewall and, in some cases, an IDS**—The JTF server will likely need to provide access to external systems. If the external systems reside on private networks, the interface to the private network should be protected by a firewall so that information message traffic into and out of the JTF can be carefully monitored. If the external systems reside on public networks, such as the Internet, there is greater risk of exposure and potential for unauthorized access to the task force database. In that situation, the JTF information system managers should consider employing an IDS to monitor patterns of message traffic into and out of the JTF and further mitigate the risk of information system compromise.

- **There is an "air gap" between restricted/classified external information systems and the JTF server**—There may be task force participants that can contribute intelligence and research information from classified or restricted access information systems external to the task force itself. It may be necessary to keep the PC workstations used to access such information physically isolated from the remainder of the JTF internal network. The specific requirements for handling access to restricted/classified network access will generally be governed by published policy for the specific network.

- **Virus and worm protection is carefully managed**—Because individuals from different organizations man the task force, its computer systems are more susceptible to viruses and worms brought in from outside sources. All JTF PC workstations and servers should be loaded with virus protection software that is regularly updated. The information system manager(s) that administer the task force computer systems should periodically verify that workstations and servers are up to date with the appropriate software security patches. There are automated tools that can scan a network and report on the status of security patches in server and workstation software to help automate this important job.

- **Participants should be aware of the task force security policies**—As new participants join the task force, they should be briefed on the policies and procedures for handling and safeguarding task force information.

Joint Task Force Disciplines

Identification and Authentication

The expected life cycle of the JTF will impact the mechanism and level of rigor that can be applied to identification and authentication—the procedures used to gain access to the task force databases and other information resources. In situations where the task force has a short-term mission (i.e., weeks or months) and staff changes rapidly, it may be difficult to manage I&A procedures that are any more complex than username and password. In this case, JTF computer systems should be programmed to accept only strong passwords (see Chapter 2, "Security Disciplines," Section 2-1, Identification and Authentication, Best Practices, Something You Know—Passwords).

Task forces that have long-term missions can consider more rigorous authentication methods, such as the addition of a hardware token or biometric identifier.

Authorization and Access Control

In a large, long-term task force, a RBAC model may be appropriate. A role-based model would include predefined access privileges for groups such as sworn officers, intelligence analysts, federal agents, and district attorneys. Defining an appropriate set of roles makes it easier to add and delete new members and their privileges.

In some cases, the task force mission is better served by granting to a wide range of participants the flexibility to look at all of the collected JTF information. This situation results in there being a much smaller set of roles, perhaps only two: system administrator and user. An authorization policy in which there is a reduced number of roles places more responsibility on the task force participants to understand the sensitivity level of each piece of information and the appropriate handling thereof.

Security Auditing

The guidelines provided in Chapter 2, "Security Disciplines," need to be altered to accommodate the JTF model. The typical short duration and the somewhat volatile population of participants make the use of security auditing difficult and less practical to implement. Realizing that security audits will often not be put in place, sponsors of the joint task force must pay particular attention in setting up security procedures and processes that are effective and easy to implement.

Intrusion Detection Systems

JTF models commonly start out as single networks, with one or more attached servers that house data that is available only to task force members. The need for intrusion detection should be based upon the sensitivity of the information being processed and retained.

More often than not, joint task force operations are quickly assembled to accomplish defined tasks over an established period of time or until special funding is exhausted. It is not unusual for all JTF members to be sworn personnel with limited knowledge of proper security practices. Task force budgets are seldom adequate to fund information systems personnel, and members are sometimes reluctant to involve nonsworn personnel, especially when data is highly sensitive.

It is not uncommon to have sensitive data on task force servers without the benefit of being protected by anything more than limited physical security. Basic security safeguards such as passwords, encryption, authentication, firewalls, and data backups are often not included. Intrusion detection, which today is not commonly included among the safeguards for criminal justice systems, would be a rare find in JTF configurations.

JTF participants often find that they are reentering information that is available (housed) in other systems or that they need access to information from other systems. These realizations can lead to requests for connectivity to other systems or asking trusted individuals to download needed information and manually transport it to JTF facilities. Both of these situations can place highly sensitive data at extreme risk.

JTF operations should not attempt to automate sensitive data without proper security safeguards being in place, such as intrusion detection. The necessary safeguards need to be determined by qualified information systems professionals.

Data Classification

The JTF should create a security policy that includes procedures for handling sensitive or critical information. Information collected by the JTF should be labeled as it comes in to indicate the appropriate confidentiality, integrity, and/or availability levels. As task force members and local law enforcement utilize the information, they will be made aware of the required security policies and procedures for the information, as indicated by the classification levels.

Since the JTF is made up of individuals from a wide variety of home organizations, each with different information classification rules, it is the responsibility of the members to ensure that any information they contribute from their home organization receives the appropriate security classification in the JTF.

Physical Security

The JTF should assemble in a location suited to providing the maximum physical security for information and equipment. If the task force has an established command post, measures should be taken to provide for security of information and equipment that will remain at the command post for the term of the joint task force. Measures should include, but not be limited to, building entrance security and room security.

Measures should be taken to secure information and equipment. Documents and electronic information brought to the task force by participating justice organizations and information

generated by the joint task force should be secure from intrusion, damage, theft, and misuse. Measures should also be taken to properly dispose of sensitive information. Secure information can be obtained in a low-tech manner by someone simply going through trash for discarded paperwork.

The final physical measure should include protection against physical intrusion. With a joint task force, it is likely that numerous people unfamiliar with each other may flow in and out of the task force. Security measures should be taken to ensure that persons accessing task force information have been approved by a central command authority. There is also the potential for authorized task force members to be precluded from access to certain information unrelated to their particular assignment. All task force members should be on guard against masquerading or impersonation, which can occur when an intruder obtains a false identity by obtaining a task force user ID. Someone may be misled about the identity of the party he is communicating with for the purpose of obtaining sensitive information.

Critical Incident Response

The critical incident response deployment within a task force involves a shared responsibility among the participating agencies to protect the information resources of the task force entity. The establishment of a plan should involve training and coordination between participating agencies as part of their memorandum of understanding.

Many task forces adopt the security requirement of a single host agency by mutual agreement. Task forces should train task force members in the critical incident response protocols and procedures of the host agency, as well as additional familiarization with the host agency structure, lines of communication, and organization.

Local agencies within a general geographic area should prepare for the cooperative plan and review their response as a general practice. Many task force operations are ad hoc in nature and must be set up quickly in response to a developing crime problem. In this environment, the task force will need to adopt a preexisting plan because they will not have the time or opportunity to develop one once the task force is formed and activated. The lack of such a capability while in the midst of a high-profile task force investigation could have disastrous effects if the information resources of the task forces are compromised.

Disaster Recovery and Business Continuity

Since a JTF is often very short-lived, only the basic disaster recovery procedures may be needed, such as computer backups and designation of an alternate work site.

Public Access, Privacy, and Confidentiality

The JTF must create a security policy that includes procedures for handling information subject to privacy laws. Information collected by the JTF must be labeled as it comes in to indicate its privacy requirements, such as obtaining the subject's consent before disclosure outside the justice system. As task force members and local law enforcement personnel

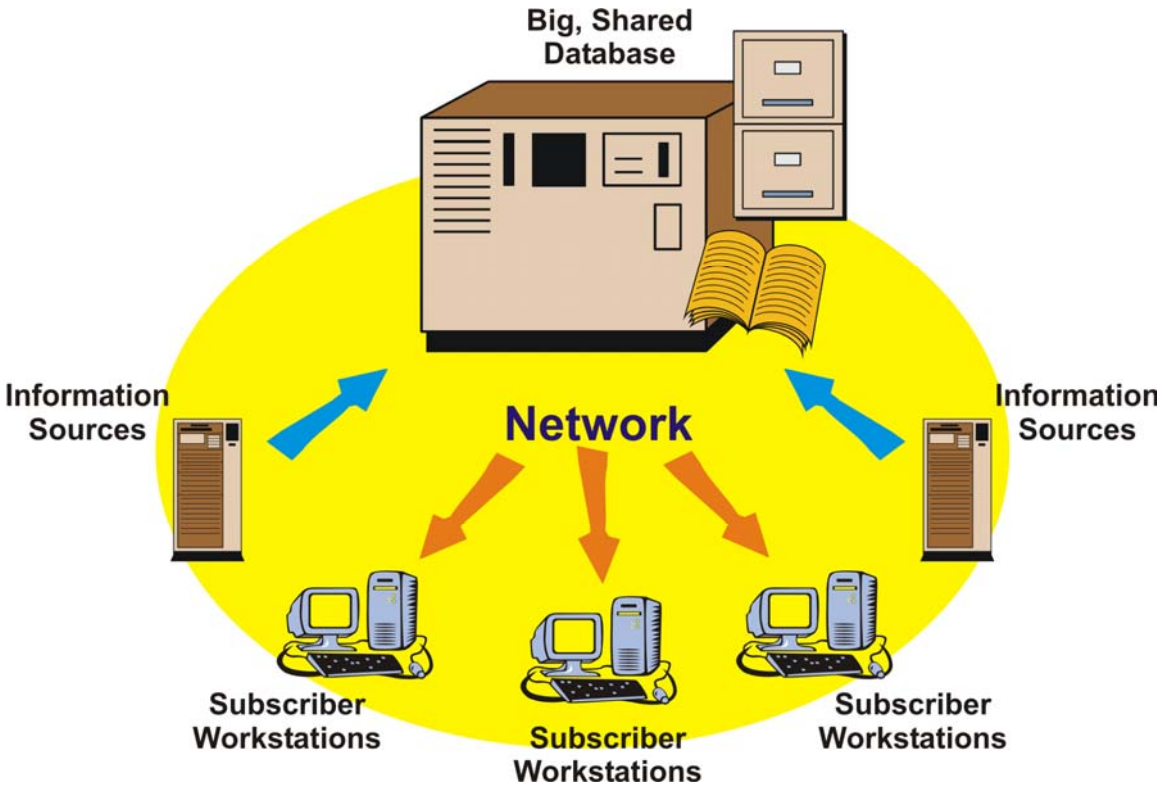
utilize the information, they will be aware of the restrictions in use and dissemination and the required security safeguards for the information indicated by the label.

The Centralized Information Repository (CIR) Model

Introduction

A common approach to information sharing on a wide scale is the establishment of a Centralized Information Repository (CIR) model. Information is generally held in a large database, and justice professionals connected through public or private networks subscribe to the database. With this subscription comes the ability to formulate queries against the database and perhaps generate reports based on the information therein. This model is represented conceptually in Figure 3-3: The Centralized Information Repository Model.

Figure 3-3: The Centralized Information Repository Model



The repository owner has the ability to define all of the security policies, requirements, and practices for information access and use. However, with this flexibility comes the responsibility to implement policies that subscribers can practically implement to enforce the security policy and to safeguard the integrity and availability of the information.

The flow of information within the central repository involves:

Feed from information sources—The central database must be populated and continually updated. Source information generally comes from "the field." For example, fingerprint information comes from booking stations; incident information comes from local and state reporting sources. The integrity of the information stored in the repository is dependent upon the integrity of the sources.

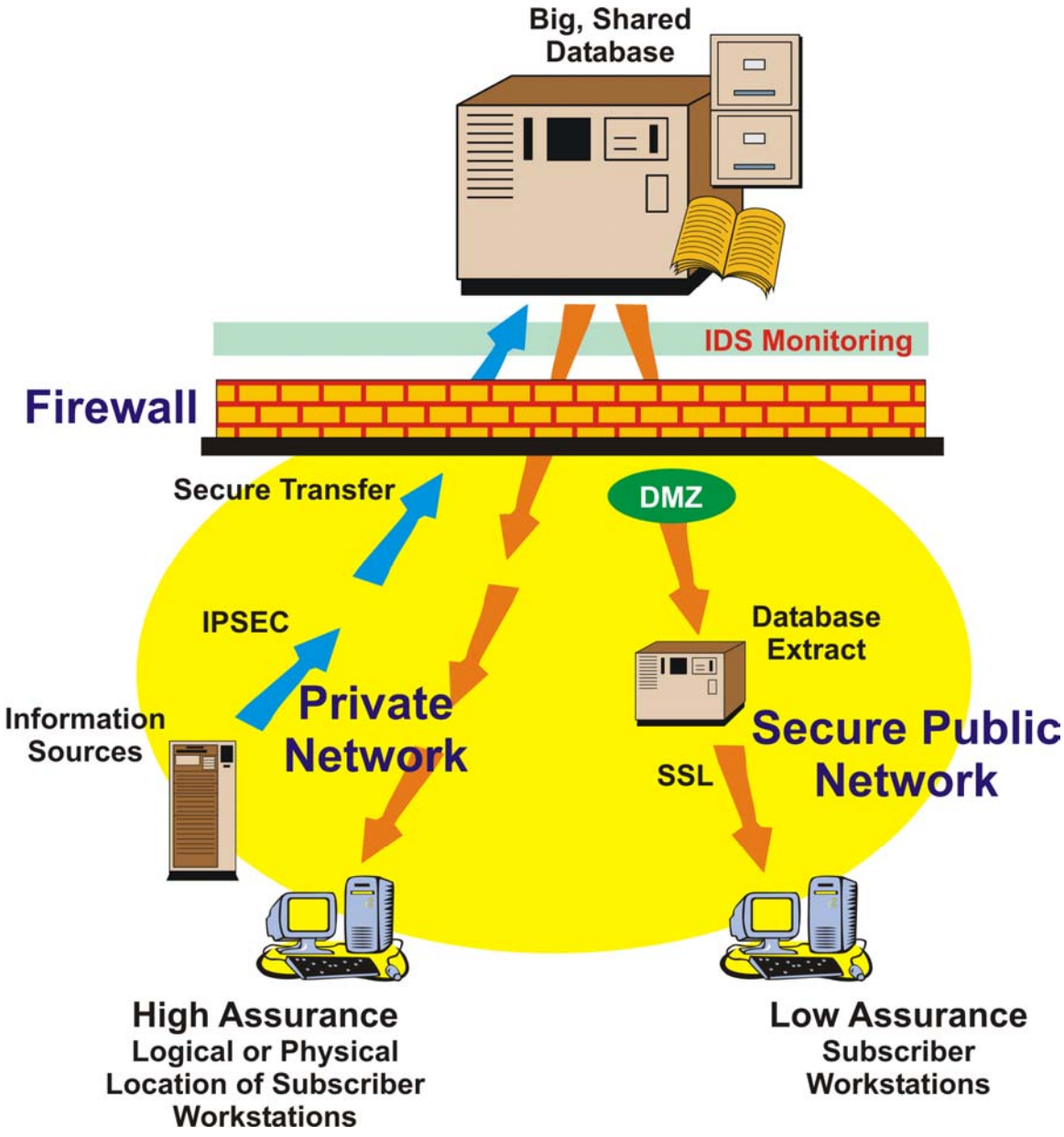
Queries from subscribers—The reason the repository exists is to provide timely and accurate information to its subscribers. The security practices must ensure access is limited to authorized subscribers and that information remains protected once it leaves the repository, transits the network, and arrives at the subscriber workstation.

There should be a written set of information security policies and practices to protect these information flows and maintain the security and integrity of the data stored in the repository.

Security Guidelines for the Centralized Information Repository (CIR) Model

The CIR system supports information sharing by collecting justice information from its sources, processing and storing it, and subsequently distributing it to subscribers. Figure 3-4: Security Practices to Support Information Flow Into the Centralized Information Repository Model shows some of the mechanisms used to protect these information flows.

Figure 3-4: Security Practices to Support Information Flow Into the Centralized Information Repository Model



There are two networks shown in Figure 3-4: a private network for information collection and distribution of highly sensitive information (to high-assurance subscribers) and a public network of distribution of less sensitive information (to low-assurance subscribers). The private network may consist of point-to-point lines connecting directly between source computers, subscribers, and the central repository. Alternatively, the private network may consist of a switched network that routes information over many links to transfer it between the source/subscriber and the repository. The security applied by the CIR managers is dependent upon the encryption capabilities offered by the network itself. Even in networks built on dedicated communications lines, telecommunications providers may merge provided lines onto shared resources. To ensure the protection of the information in transit, the CIR system managers can implement endpoint-to-endpoint encryption between information sources and the repository system. A good way to implement this might be by using IPsec—the secure version of the IP protocol (reference). IPsec provides both encryption and integrity features.

A distinction is drawn in Figure 3-4 between information access by high- and low-assurance subscribers. Low-assurance subscribers connect to the information repository through public networks. The information transfer may be protected by end-to-end encryption protocols, such as secure sockets layer. In order to safeguard the information stored on the primary database, the subset of information that is accessible to the low-assurance subscribers is replicated to a database server that is located on the "DMZ." In contrast, the high-assurance subscribers connect to the private network in much the same way as the information source systems. The CIR managers may insist that subscriber workstations connect solely to the CIR network. Figure 3-4 illustrates this by indicating that the high-assurance subscriber workstations are "logically isolated" from other computer systems and/or networks in the subscriber's facilities. This requirement prevents unauthorized access to the CIR network from subscribers that are in some way connected to the subscribers' workstation through local networks.

Centralized Information Repository Disciplines

Physical Security

The CIR model is based upon a central database from which subscribers are able to feed information into the database and also access information. The physical security measures should be designed to protect the database at the database site, and each subscriber should also adopt physical security measures to protect the information fed into and accessed from the database.

All users should implement policies that instruct employees how to detect signs of physical intrusion. Policies and procedures should also address appropriate reactions to intruders and advise how to respond to incidents where an intrusion has been detected.

Physical security measures should also address masquerading or impersonation by persons who obtain a false identity by obtaining a user ID and password. Someone may be misled about the identity of the party he is communicating with for the purpose of obtaining

sensitive information. An intruder can also use masquerading to connect to an existing connection without having to authenticate himself.

A proven method of enhancing physical security is to secure desktop workstations. Effective policies and procedures to secure desktop workstations should be a significant part of any physical security strategy because of the sensitive information often stored on workstations and their connection to the rest of the networked world. Many security problems can be avoided if the workstation and network are appropriately configured.

Identification and Authentication

Since the CIR managers own the shared data, they can independently define the I&A process for all subscribers. The process can be made more rigorous based on the value of the information in the CIR database. For example, low-assurance subscribers may only be required to enter a user ID and a strong password. High-assurance subscribers may be required to use a smart card and enter a PIN to gain access.

As owners of the information resource, the CIR managers can use a very simple approach to motivate subscribers to adhere to the CIR I&A policy. If subscribers adhere, they may access the data. If they do not adhere, access is denied. However, the CIR managers must have some way to audit subscribers to determine if I&A policies are being followed in practice. For example, the CIR policy may specify that there is a one-to-one correspondence between username/password and specific individuals. While the subscribing organization may agree to this policy in theory, practice may show that users share IDs and passwords as a matter of convenience. It is important to institute some degree of auditing (see Chapter 3, Section 3-3, Security Auditing) to maintain electronic trust in the area of I&A.

Authorization and Access Control

The authorization and access control requirements for this model are generally enforced through the database system software that houses the CIR information. Authorization and access control can use RBAC techniques as described in the Security Guidelines for Joint Task Force Model, Authorization and Access Control section. Since the CIR managers own the shared information resource, they have a great deal of freedom and flexibility in defining access roles, privileges, and qualification requirements.

Data Classification

The CIR should have a security policy that includes procedures for handling sensitive or critical information. Information collected must be labeled as it comes in to indicate the appropriate confidentiality, integrity, and/or availability levels. Special labels should be created to distinguish between the low- and high-assurance subscribers. When subscribers request information, an authorization check must be performed to verify the subscriber meets requirements for access to the information as indicated by the classification levels.

Since the CIR is made up of information from a wide variety of home organizations, each with different information classification rules, it is the responsibility of the contributors to ensure that any information they supply from their home organization receives the appropriate security classification in the CIR database.

Public Access, Privacy, and Confidentiality

The CIR should have a security policy that includes procedures for handling information subject to privacy laws. Information collected should be labeled as it comes in to indicate its privacy requirements, such as obtaining the subject's consent before disclosure outside the justice system. When subscribers request private information, an authorization check should be performed to verify the subscriber meets requirements for use and dissemination of the information.

To ensure the confidentiality of the information as it is transmitted, endpoint-to-endpoint encryption such as IPsec should be used. Also, the CIR management should perform periodic audits of high-assurance subscriber workstations to ensure they are kept "logically isolated" from other computer systems and/or networks to prevent unauthorized disclosure.

Firewalls, VPNs, and Other Network Safeguards

The CIR model was the first information sharing model put into practice. In the situation where a user is accessing resources located in a central repository, there is typically dedicated staff at a data center with adequate training to make certain that the central database is secured by a well-configured and well-monitored firewall. However, a less obvious need for a firewall in the use of resources in a CIR would be the implementation of a personal firewall on a personal computer used to access resources located in the CIR. If a remote user's computer were compromised, it could potentially expose a vulnerability that would allow access to data in the central repository. Typically in this scenario, policies are in place addressing what traffic is allowed, who is responsible for supporting the system, and how vulnerabilities or breaches should be addressed. VPN technology may be employed depending on the sensitivity of the data. However, VPN-client access should be limited to the specific resources that are needed by the user to perform their authorized duties. Client-based VPNs should have realistic time-out parameters to close network sessions that are not in use.

Critical Incident Response

Critical incident response deployment within this model provides a centralized and coordinated response with a uniform rule set, as well as good lines of communication, command, and control. A modification of scale is the primary adaptive measure required for deployment in this model. These adaptive measures are necessary when critical incident response is deployed in a small criminal justice agency with limited resources. In that event, the basic principles of response are still applicable, but the structure of the organization may reduce the coordination steps necessary for successful deployment of the capability.

Disaster Recovery and Business Continuity

The CIR must have a security policy that includes disaster recovery and business continuity procedures. This becomes vitally important as the number of subscribers dependent upon the information grows. A central repository could become a high-target priority because of the large number of users it could disrupt and the widespread damage its loss could cause.

Operational Examples of the Centralized Information Repository (CIR) Model

FBI CJIS/NCIC Case Study

The FBI CJIS/NCIC is an example of the CIR model. The system consists of central databases housed at the CJIS complex in Clarksburg, West Virginia, and interfaces with multiple local, state, tribal, federal, and international criminal justice systems. This "system of systems" provides users with the capability to update and query the CJIS databases.

As described in the model, CJIS, the repository owner, has established security policies to safeguard the system. A security subcommittee composed of system users was established to ensure the establishment of practical security policies which would provide adequate security for the system while controlling impact on the subscribers. These policies address security issues such as physical security requirements, personal background checks, encryption, Internet access, dial-up access, and audits. Since a system's security is only as secure as its weakest link, CJIS conducts periodic audits of interface agencies and requires those agencies to establish an internal audit of their subscribers.

The CJIS/NCIC "system of systems" is a very good example of a CIR model as defined by the GSWG.

Introduction

The FBI CJIS Division's automated identification and information services enable local, state, federal, tribal, and international law enforcement communities, as well as civil organizations, to efficiently access and/or exchange critical information. The CJIS Division System of Systems (SoS) provides advanced identification and ancillary criminal justice technologies used in the identification of subjects.

General policy concerning the philosophy, concept, and operational principles of the CJIS Division SoS is based upon the recommendations of the CJIS Advisory Policy Board (APB) to the Director of the FBI. In its deliberations, the APB places particular emphasis on the continued compatibility of the CJIS Division and state systems; systems security; and the rules, regulations, and procedures to maintain the integrity of the system data. The APB is composed of administrators at the policymaking level from local, state, and federal criminal justice agencies throughout the United States. The APB acts on input from its various subcommittees and working groups to change current procedures, approve changes to current applications, add new files of information, and coordinate these changes with

participants. A federal working group and four regional working groups were established to recommend policy and procedures for the programs administered by the FBI CJIS Division. These working groups are also responsible for the review of operational and technical issues related to the operation of, or policy for, these programs.

The systems within the CJIS SoS have evolved over time, individually and collectively, to add new technological capabilities, embrace legislative directives, and improve the performance and accuracy of their information services. Each of these systems has multiple segments consisting of hardware and computer software that provide the operating systems and utilities, database management, workflow management, transaction and/or messaging management, internal and external networking, communications load balancing, and system security. The increasingly complex requirements of the SoS architecture demand a well-structured process for its operations and maintenance. Future system enhancements, modifications, or technology refreshments must recognize the interdependencies between the systems and must be structured in a way that minimizes the operational impact. Each system has been developed and deployed in the CJIS complex located in Clarksburg, West Virginia. The SoS is in operational service 7 days a week, 24 hours a day.

There are three principal systems in the CJIS SoS. These are the Integrated Automated Fingerprint Identification System, the National Crime Information Center 2000, and the National Instant Criminal Background Check System. The SoS also has other significant systems that provide telecommunications or other information services that support the mission of the three principal systems. Figure 3-5: Federal Bureau of Investigation CJIS System of Systems (shown on page 3-24) provides a top-level view of the FBI CJIS SoS, and the interrelationship of each system follows.

- **The Integrated Automated Fingerprint Identification System (IAFIS)**—IAFIS consists of three integrated segments: the Identification Tasking and Networking (ITN), the Interstate Identification Index (III), and the Automated Fingerprint Identification System (AFIS). The ITN acts as a "traffic cop" for the IAFIS, providing workflow/workload management for ten-print, latent-print, and document processing. The ITN provides the human-machine interfaces, the internal interfaces for communications within the IAFIS backbone communications element, the storage and retrieval of fingerprint images, the external communications interfaces, the IAFIS Back-end Communications Element (BCE), and user fee billing. The III provides subject search, computerized criminal history, and criminal photo storage and retrieval. The AFIS searches the FBI fingerprint repository for matches to ten-print and latent fingerprints.

  Supporting the IAFIS is the CJIS WAN, providing the communications infrastructure for the secure exchange of fingerprint information to and from external systems. The external systems are the state Control Terminal Agencies (CTA), state Identification Bureaus, Federal Service Coordinators, and the IAFIS front-end communications element. Also submitting fingerprint information to IAFIS is another CJIS system called the Card Scanning Service (CSS). The CSS acts as a conduit for agencies that are not yet submitting fingerprints electronically. The CSS makes the conversion of fingerprint information from paper format to electronic format and submits that

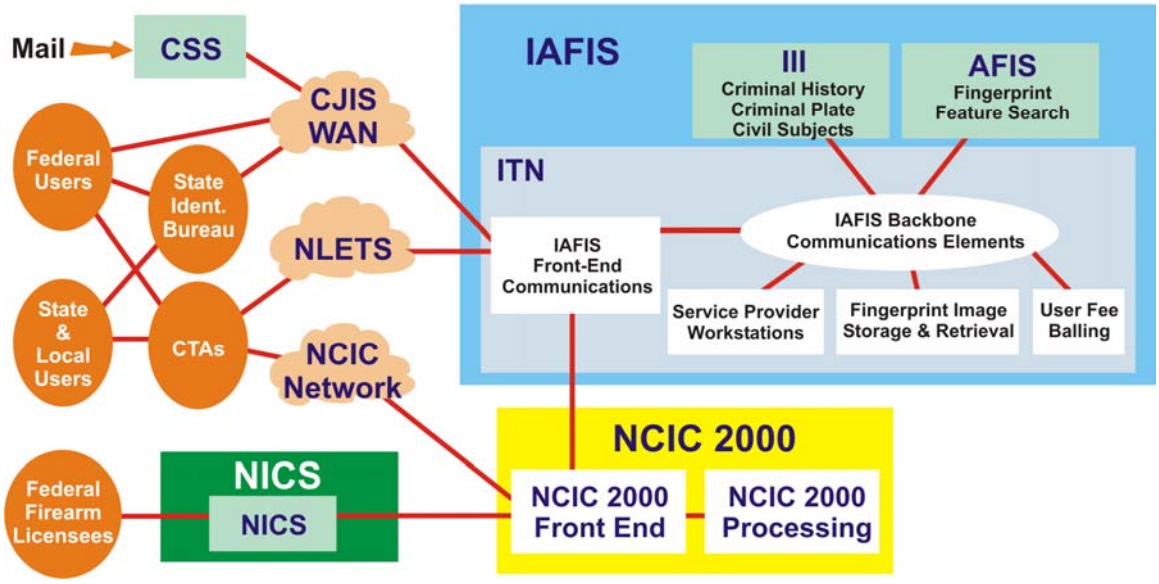
information to IAFIS by way of the CJIS WAN. Another system providing external communications for IAFIS is the NLETS. The purpose of NLETS is to provide interstate communications to law enforcement, criminal justice, and other agencies involved in enforcement of laws. NLETS supports the legacy, binary synchronous communications protocol to state CTAs.

- **The National Crime Information Center 2000 (NCIC 2000)**—NCIC 2002 is an online computerized index that provides law enforcement and criminal justice agencies with information about individuals, vehicles, property, and other facts that are associated with the investigation of crimes. It also includes locator-type files on missing and unidentified persons. Supporting NCIC 2000 is the Law Enforcement Interconnecting Facilities (LEIF). LEIF provides the networking access for FBI Field Offices, Resident Agencies, and Special Task Forces to the NCIC 2000 and state databases. The NCIC International Project for LEIF will also provide database access to foreign countries. NLETS, mentioned under IAFIS, is also a communications system that supports state access to NCIC 2000.

- **The National Instant Criminal Background Check System (NICS)**—NICS is a national system that conducts name searches and provides criminal history records on individuals who are purchasing firearms or transferring ownership of firearms. The system provides Federal Firearms Licensees (e.g., gun dealers) with a determination as to whether transferring the firearm to a particular individual would violate Public Law 103-159, the Brady Handgun Violence Prevention Act.

  The Brady Handgun Violence Prevention Act of 1993 (P.L. 103-159) required the U.S. Attorney General to establish a system that any licensed gun dealer may contact by telephone or by any other electronic means for information on whether receipt of a firearm would violate state or federal law. This legislation initiated the implementation of the NICS system.

Figure 3-5: Federal Bureau of Investigation CJIS System of Systems



Data Integrity

When information is submitted by a participating agency, it is stored in the CJIS SoS data bank. The submitted information is then available in response to queries submitted by other participating agencies. The SoS does not alter the information that is submitted; rather, it stores that information and uses it to respond to queries from participating agencies. The data must be kept accurate and up to date. Agencies that enter records in the SoS are responsible for their accuracy, timeliness, and completeness. To facilitate compliance with hit confirmation requirements, the originating agency must be available 24 hours a day to confirm its record entries. APB policy ensures that all contributing agencies assume responsibility for proper records maintenance.

The FBI, as the manager of the SoS, helps maintain the integrity of the system through the following: (1) automatic computer edits, (2) automatic purging of records, (3) quality control checks, and (4) periodic validation of all records on file.

The integrity of the data is paramount in importance because law enforcement officials throughout the nation rely on its accuracy and completeness. All security-relevant files (system administration, configuration files, audit files, transaction log, and the security log) must be protected, since a compromise of these files could result in the entire system being compromised. The integrity of the data must be adequately protected at the point of entry into the database while being transmitted to the authorized inquiring party. The system users are restricted to the minimum access needed to function effectively in their duties and to monitor their performance.

The CJIS Division systems process information subject to the provisions of the Freedom of Information Act, Privacy Act of 1974, and meet the conditions of disclosure as described in Title 5, USC, 552.A (b) (vii). Information reviews are ongoing, due to the continual use of filings and related material. The loss or abuse of SoS data could result in the unknowing release of a criminal, the wrongful incarceration of persons, the theft of property, or the loss of lives. The inability to access the SoS would prevent law enforcement officers in the field from making informed judgments and can hamper or endanger ongoing missions. Prior arrest information and indirect access to criminal history records is limited to authorized agencies, only due to the possible misuse of arrest data adversely affecting licensing and/or employment of an individual.

System integrity controls are used to protect the operating system, application executables, and configuration data in the system from accidental or malicious alteration or destruction and to provide assurance to the user that the operation of the system meets expectations and has not been altered.

Data integrity controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets expectations about its quality and has not been altered. Data integrity controls include the following:

- Encryption of messages in transit
- Reconciliation routines, such as checksums, hash totals, and record counts of received messages
- Data integrity verification programs for received messages
- Message authentication for received messages

Penetration testing is performed by an independent contractor on a yearly basis. Serious vulnerabilities identified are documented through the Configuration Management process, and corrective actions are taken. The systems may be retested to ensure that the vulnerabilities have been properly addressed.

The CJIS Division SoS is published for public review in the *Federal Register*.

Physical Security

The FBI-controlled components of the SoS are managed through the restricted access to the FBI CJIS facility and the Division Data Center. The facility is protected by armed guards and officers, vehicle barriers, and cameras, as well as a security alarm system. The guards ensure that all drivers coming into the CJIS complex display their FBI-issued badge and vehicle pass. Passengers and pedestrians are also required to show identification badges. The employee badges must be worn at all times while on the CJIS Division facility. Any visitors coming to the CJIS Division facility must be cleared by the appropriate security personnel prior to their visit.

Security staff is posted at the main entrances of the CJIS facility, 24 hours a day, 7 days a week. The Security Unit performs random searches of packages and equipment brought into

the facility. There are alarm systems throughout the facility that will become activated if unauthorized personnel enter restricted areas.

All access to the Data Center areas are controlled by a 24-hour cipher system, and all accesses are monitored by closed-circuit video cameras. Employee identification badges are encoded, allowing or disallowing access to this area. Visitor access to the Clarksburg Data Center is controlled through escort and sign-in. All packages are searched upon entry and departure from the Data Center. Removal of equipment media from the Data Center must be approved in advance.

Physical protection of all hardware components from unauthorized removal is provided by building security measures. Equipment is not allowed to enter or exit the West Virginia facility without being authorized by the FBI security personnel at the ground floor entrance. Individuals removing equipment from the West Virginia facility must have a property removal pass authorized by the CJIS Division, Information Technology Management Section (ITMS), Operations Unit.

Fire Safety Factors

The facility's fire sprinkler and fire alarm/monitoring systems are both fully supervised systems in that an individual (Control Operator) is assigned to monitor the system controls 24 hours a day, 7 days a week. This structure provides complexwide monitoring by both the computerized system and the facilities staff. Both the sprinkler and alarm systems meet the requirements of the National Fire Protection Association, Regulations 13 and 72. A stringent system testing schedule is in place and followed. Annual evacuation drills and emergency evacuation briefings are held for both employees and contractors. Additionally, fire extinguishers and occupant hoses are installed throughout the complex. The facility has redundant utility systems to provide an uninterrupted power supply. These systems were developed to code and implemented during the construction of the complex in 1991.

Personnel Security

All personnel who have been entrusted with the management, operation, maintenance, and use of an FBI Automated Data Processing (ADP) system processing, storing, or transmitting sensitive data require the appropriate personnel security approval. Clearance must be obtained prior to any system access. All positions are reviewed by Human Resources personnel to determine sensitivity level, and most system users are authorized access only to information that is needed to perform their specific job.

Identification and Authentication

Identification and authentication and residual information protection are performed at the operating system level, with some additional checks at the database management system (DBMS) level. All operating system-level passwords are stored in unreadable format in authentication repositories on SoS security servers, as well as cached repositories on workstations and other servers.

CJIS SoS has "security-in-depth" in its security functional mechanisms, in that audit and access controls are performed at the operating system, DBMS, and application levels.

Indirect users are identified by their Originating Agency Identifier (ORI), which is maintained in an ORI/Type of Transaction (TOT) table. Direct users require the use of robust authentication techniques, which include robust passwords or two-factor authentication techniques, such as the addition of biometrics, digital signature, or token-based access. Authentication is enabled at the operating system level. A secondary login may be required at the application and database levels.

The systems must meet government standards for the following:

- Password length
- Allowable character set
- Password-aging time frames and enforcement approach
- Number of generations of passwords disallowed for use
- Procedures for password changes
- Procedures for handling password compromise
- Frequency of password changes
- Mechanism of authentication supporting individual accountability and audit trails
- Self-protection techniques for user authentication mechanisms (i.e., passwords are stored encrypted and remote communications connections are protected with link-level encryption at a minimum)
- Invalid access attempt threshold
- Process for verifying all system-provided administrative default passwords have been changed
- Policies that provide for bypassing user authentication requirements and any compensating controls
- Digital or electronic signatures use

Access Control

Logical Access Controls

The CJIS Division SoS maintains an ORI/TOT table and determines whether the submitter is permitted to perform the requested transaction. Access control to limit what the user can read, write, modify, or delete is handled via the transactions that are defined in the Electronic Fingerprint Transmission Standard for submission, modification, deletion, and retrieval. An indirect user is restricted through ORI/TOT validation.

For direct users, user roles are defined with operating system groups, database groups, and/or application-defined groups. The SoS has the capability to use operating systems or layer security products to define asset groups (i.e., files, directories, and users and groups) in order to provide for discretionary access control. Action is planned to implement these features. The FBI CJIS Division System of Systems supports the objects reuse capability. Each communication device has been scripted to manage access paths between devices.

Public Access Controls

Transactions come from authorized end users through CJIS WAN or NLETS. The CJIS WAN is an FBI network that is managed by the CJIS Division. NLETS is a public network for law enforcement officials. Access to and use of SoS records is governed by the Privacy Act.

Data Classification and Privacy

The SoS files contain documented criminal justice information. Since this data is documented criminal justice information, it is sensitive but unclassified. State and federal laws and statutes also determine the requirement for data confidentiality. Disclosure of sensitive judicial system/law enforcement data to unauthorized persons is prohibited by law.

Change Management

The FBI has established three boards that control baseline changes to NCIC 2000, depending upon the scope of the change. All changes to commercial off-the-shelf software loaded on the system are controlled by a Technical Review Board (TRB). This board is called the Pre-Configuration Control Board (CCB) and is chaired by an Information Technology Management Section (ITMS) representative. The TRB is responsible for the change package level of the products and is the first cross-pollination of groups within the CJIS Units to review the problems or changes. The TRB approves and disapproves the changes. Each change is evaluated as to its impact on the change package cost, schedule, and technical merit.

If a change affects another change package, the change is escalated to the Engineering Review Board (ERB). The ERB is responsible for the release-or-build level of the products. The ERB approves, disapproves, defers, or escalates changes. If a change affects another product within the CJIS Division, it is submitted to the CCB. The ERB and CJIS CCB include representatives from appropriate CJIS functional groups: ITMS, Programs Support Section, Programs Development Section, Finance, Facilities, IT Security, Change Management, and Quality Assurance.

The CCB controls changes to the SoS baseline. The CCB evaluates both the technical desirability and ability of CJIS to support proposed requirement changes and the available resources to respond to change requests. This evaluation includes assessments of the impact of requirement changes and engineering changes, as well as cost, schedule, and performance trade-offs. Program change and control procedures are currently in place. All major enhancements to SoS will be approved by the APB and CCB. All changes are recorded, and an up-to-date list of hardware and software is maintained by the Configuration Management Group.

Security Auditing

Indirect User

Each control terminal agency (CTA) is audited at least every three years by the audit staff. The objective of the CTA audits will be to verify adherence to CJIS policy and regulations. An audit may be conducted on a more frequent basis, should it be necessary due to failure to meet APB policy and regulations. In addition to accuracy, completeness, and timeliness requirements, the audit will verify the ability of a CTA to protect its information against unauthorized access and ascertain that all information released is in accordance with applicable laws and regulations.

Direct Users

FBI management conducts an independent review of records and activities to test the adequacy of controls and also to detect and react to any departure from established policies, rules, and procedures. All SoS audit logs are reviewed daily by the assigned system security administrator.

Conclusion

As directed by the Office of Management and Budget (OMB) Circular A-130, Appendix III, "The Security of Federal Automated Information Resources," the FBI implements the minimum set of security controls identified by OMB Circular A-130. Additionally, because the FBI's IT systems are identified as "major applications" and a critical infrastructure component under Presidential Decision Directive 63 (PDD-63), they must exceed the minimum NIST standards and guidelines. The identified FBI IT systems process sensitive but unclassified information. The cornerstone of the accreditation package is the system security plan, which is developed following NIST guidance.

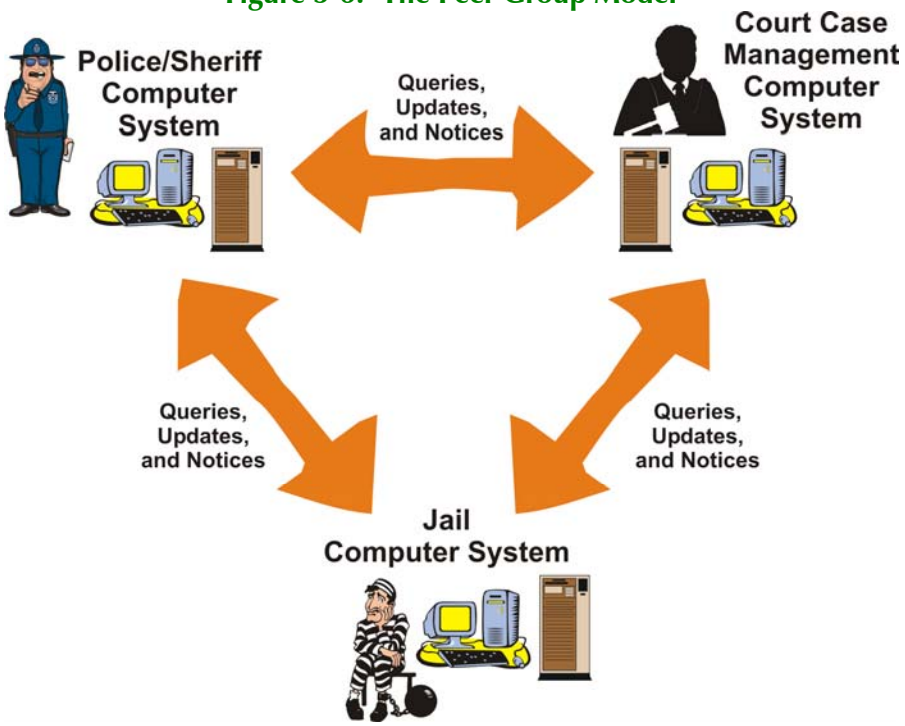
Implementation of security controls for the mission critical IT systems, ensuring the confidentiality, integrity, and availability of these systems, begins in the initial system design phase of the IT project life cycle. Security controls are implemented and monitored throughout the IT system's life cycle by continual evaluation by a team of ADPT security specialists and include the preparation of an IT System Certification & Accreditation (C&A) package, following NIST 800-18 "Guide for Developing Security Plans for IT Systems" and the National Information Assurance C&A Process requirements. As stated above, implementation of IT system security controls begins with full implementation of the requirements of OMB A-130 and all other applicable federal regulatory polices. The implementation of IT security controls then moves to those policies included in the DOJ IT Security Policy (DOJ Order 2640.2D) and finally to implementation of the policies contained in the FBI Security Policy. Each of these implementation levels is layered upon the superseding policy. The cumulative implementation of these policies does in fact exceed the basic NIST standards and guidance, but is necessary and required to ensure that the CJIS Division's IT systems are available to support the nationwide law enforcement community on a 24 hour-a-day/7 day-a-week basis.

The Peer Group (PG) Model

Introduction

The Peer Group (PG) model represents a broad category of justice information sharing in which two or more independent organizations work together to provide each other information access and use. The sharing organizations can be similar in function, such as the sheriffs' offices in adjacent jurisdictions, or quite different, such as a local police department and the state office of taxation. The PG model is becoming more prevalent in integrated justice systems. It is one of the most challenging models in terms of information security issues because there is often no single authority for setting policies and procedures. Instead, information security is a cooperative effort. Participating organizations must be convinced that the information they share will be adequately protected once it leaves the boundaries of their computing and network systems. Further, organizations must be confident that opening up their information systems for others to access will not compromise their own information confidentiality, integrity, and availability. In some cases, one or more of the peers will have connections to other external information systems. If security is not properly addressed, connections may be inadvertently created between these external systems and other unknowing members of the peer group. In these situations, a peer group member may find himself having to trust organizations that one of his peers trusts.

Figure 3-6: The Peer Group Model



The PG model is represented in Figure 3-6: The Peer Group Model. The organizations represented in this figure—police, courts, and corrections—have been selected for illustration

purposes. These are the organizations typically involved in a horizontally integrated criminal justice program—one that follows the justice workflow from arrest to trial to incarceration. In general, the PG model can include a large number and variety of peers participating in information sharing and exchange.

The flow of information within the Peer Group Model involves:

Query to/from a peer organization—A person or a computer program in one organization may request information from another organization on a query basis. For example, a sheriff may want to query court case dispositions prior to serving a warrant to determine the risk of approaching the subject of the warrant. The corrections personnel may want the scheduling software to query the court calendar to produce a report on the prisoners that must be prepared for an appearance. An important security concern in this information flow is mutual identification and authentication to verify the identities and subsequent access privileges of both the information requestor and provider.

Update to/from a peer organization—More complex information sharing tasks may require that updates be performed between peer organizations. For example, information from police arrest documents may electronically follow an arrestee to the corrections facility. This requires the police system to initiate an update to the jail system. This information flow has stronger security requirements than the query since one of the peer organizations will change its production database as a result. Identification and authentication is important, as is data integrity, to ensure that only authorized parties make changes and that information is not inappropriately modified.

Notifications—Notifications are typically exchanged between peers to facilitate workflow. For example, a police officer may want to receive a notification when a "client" has been released on parole. This may require the corrections or court system to generate a message to a user of the police system. One common mechanism used to transmit notifications is e-mail. The basic protocols used to transmit standard e-mail do not have suitable accommodations for security. If e-mail or other messaging systems are to be used in a justice environment, it may be necessary to use security add-ons that protect the information transmitted in notifications. In addition, the above simplified flows may be combined to support information analysis for intelligence-gathering purposes.

The peer organizations that share information must agree on joint security policies and practices to protect this flow of information and convince each other that the risk of opening up their systems to outside use is manageable. As the number of organizations that share data increases, the number of interfaces between systems and the security complexity increases.

Security Guidelines for the Peer Group (PG) Model

In the PG model, there may be many peer group relationships. The peers must establish electronic trust among the organizations sharing information. For simplicity, we will focus our

discussion on two peers. Figure 3-7: Security Practices to Support a Query and Update in the Peer Group Model and 3-8: Security Practices to Support Notifications in the Peer Group Model overview the security practices and mechanisms applicable to an information interchange between two justice organizations communicating as peers.

In Figure 3-7, agency Bob—an information consumer—is querying the database owned by agency Alice—an information provider. The agencies are using a VPN to communicate. This allows the two agencies to use the connectivity options provided by public networks (e.g., the Internet) but still secure their information exchanges. Agency Alice considers her shared data to be extremely sensitive and takes some additional steps in order to secure its production database. She does not provide direct query access to the destination agency. Instead, she publishes the subset of information that she wishes to share to an extract database located in the firewall DMZ (see Section 2-7, Firewalls, VPNs, and Other Network Safeguards, in Chapter 2, "Security Disciplines"). The rule table in the firewall will prevent outside access to the production database. Further, the rule table will limit extract database access to subscribers with network addresses from agency Bob. Agency Alice is also running an IDS that monitors its connection to the public network for attack patterns. In addition to examining network message content, the IDS monitors the extract database server to alarm potential integrity compromises in the shared data. Finally, Alice's system administration staff periodically runs audits on passwords to ensure that the users registered to access the shared information are employing strong passwords.

Figure 3-7 also illustrates a host-to-host connection established through the VPN to support an update to the production database. Agency Alice decided that rather than try to establish identities for outside authorized users on its production database, it would only trust one update-enabled user: agency Bob's server. This level of electronic trust implies that Alice also trusts the security practices that Bob has implemented to protect his server, including disciplines such as authentication, authorization, and physical security. The firewall and VPN software enforce the policy that only Bob's authenticated server can get the access required to update Alice's production database.

In Figure 3-8, Alice and Bob have chosen secure e-mail as the mechanism to send notification among users and justice applications. By secure, they mean that messages are encrypted so that unauthorized individuals cannot read the contents and digitally signed so that the receiver is certain that the sender is genuine. In the example portrayed in Figure 3-8, encrypted e-mail is especially important because the notification may transit a wireless network en route to a user in a patrol vehicle. Wireless networks, whether they are based on cellular protocols such as cellular digital packet data or local area network protocols such as WiFi (IEEE 802.11), are notorious for security vulnerabilities. By using secure e-mail, agencies Alice and Bob have implemented an "end-to-end" encryption strategy and do not have to worry about the integrity of the network hops that the message may transit. In order to support encryption and digital signature, Alice and Bob users must participate in a common PKI (see Section 2-3, Data Integrity, in Chapter 2, "Security Disciplines").

Figure 3-7: Security Practices to Support a Query and Update in the Peer Group Model

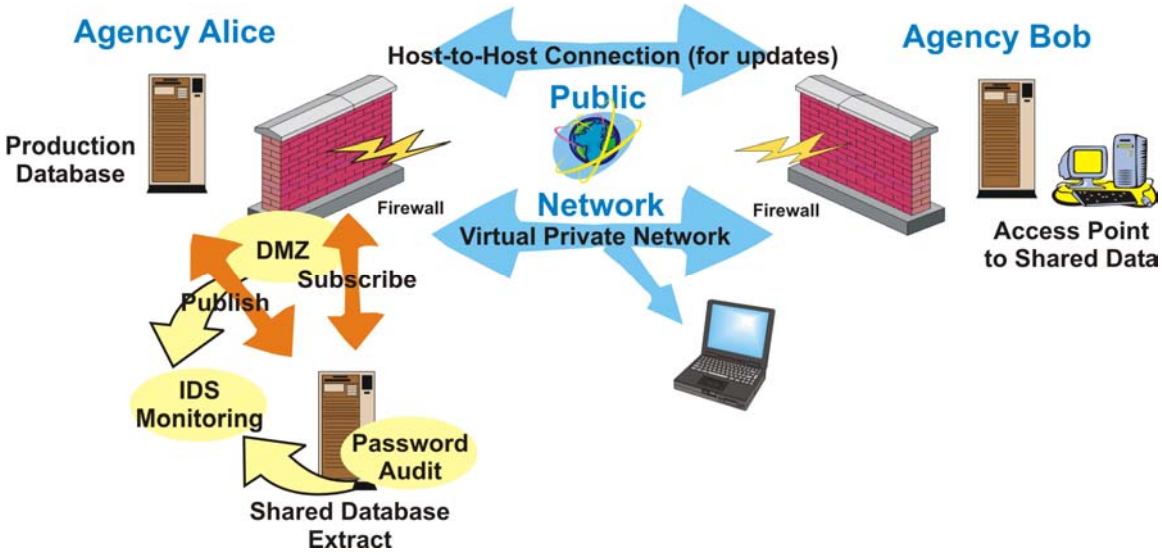
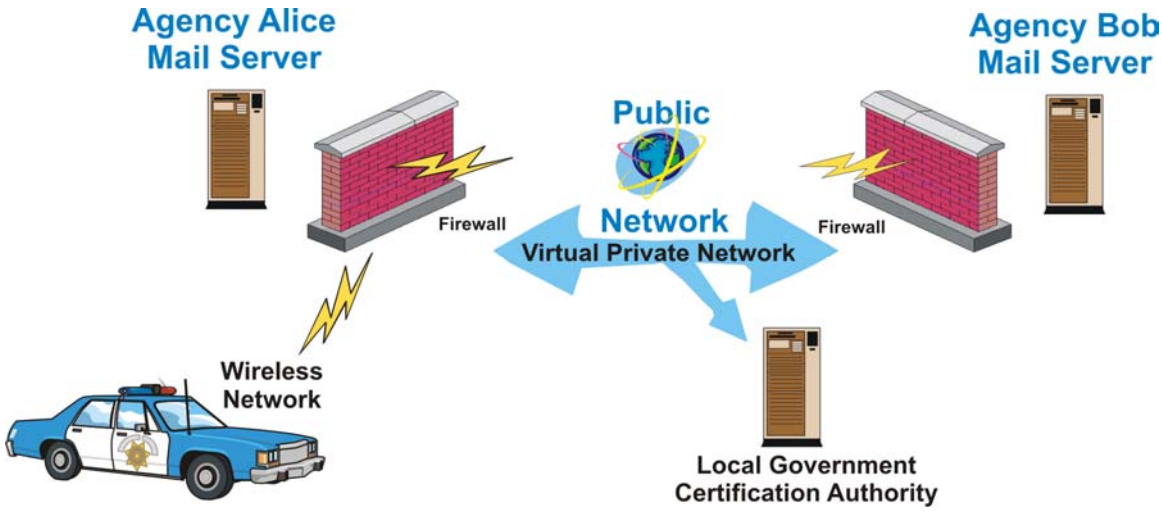


Figure 3-8: Security Practices to Support Notifications in the Peer Group Model



Peer Group Security Disciplines

The remainder of this section provides guidelines under each of the security disciplines.

Personnel Security

The key to peer-to-peer information sharing security lies not only in the technical aspects of securing critical data and systems. It is also critical that the persons accessing the data have been proven, via a standardized and accepted method among all peers, to be suitable and trustworthy to receive and utilize the data in a manner consistent with the provider's policies and procedures.

Peer-to-peer sharing in the law enforcement specific community is generally straightforward. Each law enforcement agency follows a fairly standard background check methodology to ensure that those persons hired meet a minimum set of qualifications allowing them access to information, property, firearms, etc. These background checks generally include full name and date-of-birth inquiries into national and state systems, along with fingerprint-based checks looking for criminal history records that the applicant might not disclose on an employment application. While these checks are generally not adequate for military clearances, they are generally sufficient for most personnel-related information sharing in the justice community.

Other justice partners may conduct very limited reference checks prior to employment. The local or municipal courts may not conduct any background check process prior to allowing the employee access to court databases. In many cases, the information contained at that level is public, and access need not be strictly controlled. The issue is complicated as gateways to information sharing are created. The data being accessed at a peer's location may be at a higher level, requiring differing rules for access and use. A law enforcement agency may allow the municipal courts access to their database, but they would want to be sure that access is strictly limited to that data that they would allow the public to see, unless it was understood that personnel screening has been sufficient to comfortably allow unfettered information sharing. The key is communication between the peers, setting appropriate parameters that are spelled out for both information sharing partners to meet.

In many cases the law enforcement entity in a peer-to-peer relationship is called upon to conduct some of the personnel screening efforts. Many times the criminal history check, both name and fingerprint, is forwarded to the law enforcement partner for completion via their interface with state and national systems. However the peer-to-peer personnel screening issues are handled, communication (along with procedure reconciliation efforts between all peers desiring to share information) is crucial to the success of this aspect of the model. One peer mandating procedures to another peer seldom results in success.

Firewalls, VPNs, and Other Network Safeguards

As multiple organizations are involved, planning becomes paramount in coordinating network security. Each organization involved in the peer model may have different firewalls

in place or no firewall in place. An effort should be made to identify capabilities of all participating systems and define the necessary requirements to allow the exchange of information between systems. If possible, DMZs should be created to allow areas where information can be exchanged without exposing other secure systems on an agency's internal network that will still be protected by a firewall. The scope of the opening of information sharing channels using a firewall should be limited to the specific information exchange requirements. A set of policies laid out in a memorandum of understanding should be defined early in the development of the PG model to address system responsibilities and procedures for addressing potential vulnerabilities or breaches. VPN technology may be employed, depending on the sensitivity of the data. However, VPN-client access should be limited to the specific resources that are needed by the user to perform their authorized duties. Client-based VPNs should have realistic time-out parameters to close network sessions that are not in use.

Critical Incident Response

Implementation of the Computer Security Incident Response Capability (CSIRC) in this environment is a greater challenge than in the CIR model and requires additional planning and cooperation between agencies as well as additional coordination of efforts. The success of the response will depend largely upon the ability of two or more CSIRCs in different locations being able to coordinate their communications, command, and control across a physical distance. It is critical that the peers agree upon a standard set of response rules that will be implemented in all participating peer agencies.

Regular review and coordination of the plans and capability will be necessary to ensure that attacks against the peer entity can be detected, reported, and investigated. This is especially true when the attack involves probes against different points within the peer-to-peer structure. In this case, a single peer may only see part of the overall attack, and there is a risk that the attack may go undetected. To prevent this, peer-to-peer information sharing networks need to establish clear lines of communications to an agreed-upon reporting and coordination point, where security incident information can be collated, processed, and distributed back to the CSIRC at the various peer locations.

Physical Security

The PG model is illustrated by the sharing of justice information between two or more independent organizations. Because there is not a central authority to promulgate policies and procedures for physical security, it is necessary that each independent organization adopt physical security practices to protect computing and network systems of all organizations using the network.

From a physical security prospective, a major threat is unauthorized physical access to the shared network by someone seeking to gain information from one or more of the participating organizations. Each participating organization should also implement policies to secure information in electronic and printed form. Organizations using the PG model should

designate someone from their organization to meet periodically with members from other organizations to discuss security measures and concerns that may impact all users of the PG model.

Identification and Authentication

Because of the complexity of cross-organizational user management, the participating peer group organizations may choose a simple password authentication mechanism. For example, the participating agencies may agree upon the following practices and precautions to promote strong I&A:

- Monitoring software is regularly run on the database extract server to check the strength of passwords. Users with simple passwords are required to change them at their next logon.

- Users are required to change their passwords at regular intervals.

- Users join and leave each organization regularly. This requires the security administrators to add and delete new users from external organizations. For example, when a new user joins agency Bob, the agency Alice administrator may need to give that user access to the extract database. There are several approaches to accomplishing this task. If the agencies are large and there is a large turnover in staff, Alice and Bob may consider an enterprise management security approach that automates external user administration. In the example provided, Alice and Bob administrators can take a simpler approach and use secure e-mail to communicate the need to add a new external user to any of their systems.

Based on budget constraints and the sensitivity of the shared information, the participating agencies may choose to take the next step in terms of I&A rigor: one-time password hardware tokens (see Section 5, Identification and Authentication, in Chapter 2, "Security Disciplines").

Authorization and Access Control

To simplify user privilege administration, the peer organizations can use role-based access control (RBAC). A simplified RBAC privileges list—specifying four roles—might look something like Table 3-2: Sample Roles and Privileges. As indicated in the previous example, agency Alice administrators are required to register and maintain external users on an "extract database" server (not her production database). When agency Bob adds a new user in the "sworn officer" role, a registration request is automatically forwarded to the agency Alice system administrator. Alice's administrator will add the new user into the sworn officer role on the extract database server. Using this procedure, each agency's administrators maintain control over the systems they own.

Table 3-2: Sample Roles and Privileges

Role	Privileges	Object
Sworn Officer (agency Bob user)	Query only	Alice's extract database
Bob's Server	Query and update	Alice's extract database
Court Clerk (agency Alice user)	Query and update	Alice's extract database
System Administrator	All, including privilege allocation and revocation	Alice's extract database

Data Classification

The PG model should have a security policy that creates consistent definitions that all peers agree upon for each confidentiality, integrity, and/or availability level. For example, all open criminal investigation data might be labeled confidential, high-integrity, and high-availability. The policy should also include procedures for handling each of the different levels of sensitive or critical information. For example, confidential information might require encryption during storage and data transfer. Information collected must be labeled as it comes in to indicate the applicable levels.

When peers request information, an authorization check should be performed to verify the peer meets requirements for access to the information as indicated by the classification levels.

Public Access, Privacy, and Confidentiality

The PG model should have a security policy that includes procedures for handling information subject to privacy laws. Information collected should be labeled as it is transmitted to indicate its privacy requirements, such as obtaining the subject's consent before disclosure outside the justice system. An authorization check should be performed to verify the recipient meets requirements for use and dissemination of the information.

Intrusion Detection

PG models often involve connectivity between one or more "trusted networks" and provide full or limited access to internal network resources within firewall boundaries. The level of risk provided by these network connections can be greatly reduced by firewall rule-sets that tightly limit what internal resources are available to approve outside users.

The old saying, "A chain is only as strong as its weakest link," still applies, regardless of how well firewall rule-sets are established. If a network with inadequate security is allowed to attach to a network with adequate security, the result will be two networks with inadequate security.

Networks with inadequate security can host attacks using spoofed credentials of individuals authorized to update and/or query sensitive data on peer networks. Peer group connections increase vulnerability in all situations where security is not centrally managed and evenly applied. Even when security is centrally managed, the increased traffic volume that can come from peer connections can increase risk.

The decision to deploy an IDS must balance perceived vulnerabilities against the cost of implementing and properly using the system. When accessing vulnerabilities, the user must consider the risks and security profiles of all networks requesting peer group connectivity. The decision should also consider that the security profiles of connecting systems are subject to being changed without notice.

Security Auditing

The guidelines provided in the disciplines area of Chapter 2, "Security Disciplines," apply to each of the organizations participating in peer group information sharing.

Disaster Recovery and Business Continuity

The PG model must have a disaster recovery and business continuity plan. This becomes vitally important as the dependence upon the information from other organizations grows. The plan may include having spare equipment in stock or signing agreements between organizations for hot- or warm-site support in the event of a disaster. The plan may also include alternate methods for transferring the information to subscribers, such as secure e-mail, couriers, registered mail, and phone support, depending on the time requirements.

Operational Examples of the Peer Group (PG) Model

Arizona COPLINK

COPLINK is a data-mining tool that is used to combine case data from multiple agencies, in a defined geographic area, for the purpose of sharing information. As deployed in Arizona between Phoenix and Tucson, it provides an excellent example of a PG model.

Because criminals seldom confine their activities to municipal boundaries and most police agencies lack detailed information about criminal activities outside of their municipalities, it became clear that a system was needed to share crime reports, field interrogations, and field look-out notifications.

It is well known that the further the distance from a crime, the less likely it will be that information from other systems will be of value. If too much unrelated data is provided to investigators, they will soon become overwhelmed by data overload and valuable information will be overlooked.

COPLINK addresses these issues by establishing data collection servers in major population centers. In Arizona, Phoenix will collect data from surrounding cities and the county sheriff. Tucson will do the same for agencies in the southern portion of the state. The combined Phoenix and Tucson repositories, or nodes, will eventually contain information on approximately 60 to 70 percent of the crimes taking place in Arizona.

Inquiries run against the Phoenix node will provide valuable information and possible case leads by showing relationships between people, places, automobiles, organizations, and other associative data. Inquiries against the Tucson node will provide similar relationships by mining data from agencies hosted by the Tucson Police Department.

Trying to share information using a distributed model, with each agency retaining its own information and others using multiple peer group connections, was modeled and rejected because smaller agencies lacked the machine resources to support inquiries from large and/or multiple subscriber agencies.

A peer group connection is maintained between Phoenix and Tucson using an intranet-based VPN. The connection between host municipalities (Phoenix and Tucson) and their surrounding feeder/subscriber agencies provides examples of CIR models and confirmation that some systems consist of more than one information sharing model.

Wisconsin Integrated Justice Information Sharing

The Wisconsin Integrated Justice Information Sharing (WIJIS) program has defined a security architecture that proposes the use of centralized, shared security services to allow sheriff, police, and district attorney peer organizations in Wisconsin to securely exchange information. These services are available through an interagency law enforcement network called BadgerNet. Peer organizations, within a given county, connect to BadgerNet through a VPN connection. BadgerNet provides a statewide PKI to assign and manage encryption keys for all authorized BadgerNet subscribers. Each subscriber is assigned an X.509 certificate that holds a public key. This service allows WIJIS information systems to use strong authentication techniques to confirm the identity and access privileges of information requesters across organizational lines.

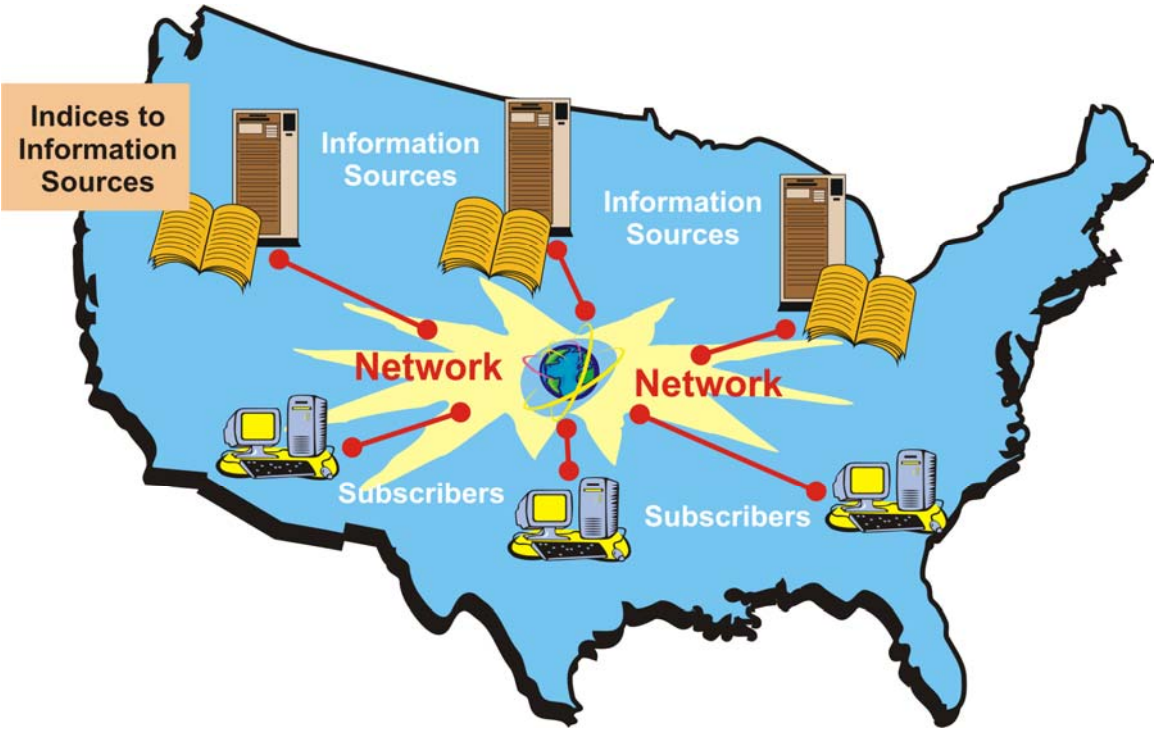
The WIJIS architecture further specifies the use of firewalls and IDSs to protect the boundaries of BadgerNet. Wisconsin uses firewalls to enforce access rules across BadgerNet boundaries, such as the interface to “partner” records management systems. Wisconsin uses firewalls in conjunction with IDSs at interfaces that have more exposure, such as their Internet portal.

The Justice Interconnection Services Network (JISN) Model

Introduction

The Justice Interconnection Services Network Model (JISN) starts with a number of related justice information sources (i.e., databases) that are generally scattered across a geographic region. The network owners provide a way to interconnect these sources and make them available to a large audience of subscribers. The owners of the network are generally not the owners of the information sources. However, the network owners may provide value-added services of their own. These services may include maintaining indices to the information sources; providing a common, simplified user interface; and/or supporting the transmission of free-form messages between subscribers. The JISN model is illustrated at a high level in Figure 3-9: The Justice Interconnection Services Network Model. This model is sometimes described as a "virtual system" or "system of systems."

Figure 3-9: The Justice Interconnection Services Network Model



The JISN owners generally set the security policies and practices that must be adhered to by information providers and subscribers. The policy for the JISN must convince the information providers that the security of their resources will not be compromised. Conversely, the JISN

subscribers must not be overly burdened with security requirements that overwhelm the utility of accessing the information.

The establishment of this consensus security policy and associated requirements is a key challenge for the JISN owners. A simple way to approach this challenge is to pass through the security requirements of each information provider to JISN subscribers. In other words, if a subscriber wants access to a specific database through the network, that subscriber must adhere to the unique security procedures prescribed by the owners of that database. While that makes security management easier for the JISN, it complicates life for the subscribers who now must be aware of and comply with the security practices of each information resource for which they want access.

The JISN owners can (and often do) eliminate this complexity for subscribers by negotiating with all of the information providers and establishing a single JISN policy that meets all of their needs yet does not overburden subscribers. The negotiation process typically results in a memorandum of understanding, with each information provider specifying how the JISN owner will protect information resources and how information providers will ensure the integrity of provided information and not compromise JISN security. Similarly, the JISN owners must issue a security policy document and requirements to subscribers. All parties should establish security audit and reporting procedures to maintain the electronic trust between owners and subscribers.

There is a growing movement to merge existing JISNs to provide even broader access for subscribers and expand information sharing. This movement elevates and complicates the security policy negotiation process. The final objective is to establish common, agreed-upon procedures among the JISN owners.

The flow of information into and out of the JISN model involves the following:

- **A subscriber queries an information source**—In this basic information flow, a subscriber is using the facilities of the JISN to query a connected database. This query may involve an access to the JISN index file to obtain information on where to look for information. For example, a local police officer may be looking for information on vehicles of a given make/model involved in a crime. The JISN must identify and authenticate the subscriber and protect the information in transit.

- **An information source causes an index to be updated**—The information resources connected to the JISN are likely to be dynamic. If the JISN maintains an index to these resources to assist in subscriber searches, the index must be updated on a periodic basis. The integrity of the index is a JISN security requirement.

- **A subscriber sends a message to another subscriber**—In some networks, simple subscriber-to-subscriber messaging is used as a means to collect information. The subscribers may use messaging to send informal information requests to other subscribers who are not formal information providers on the

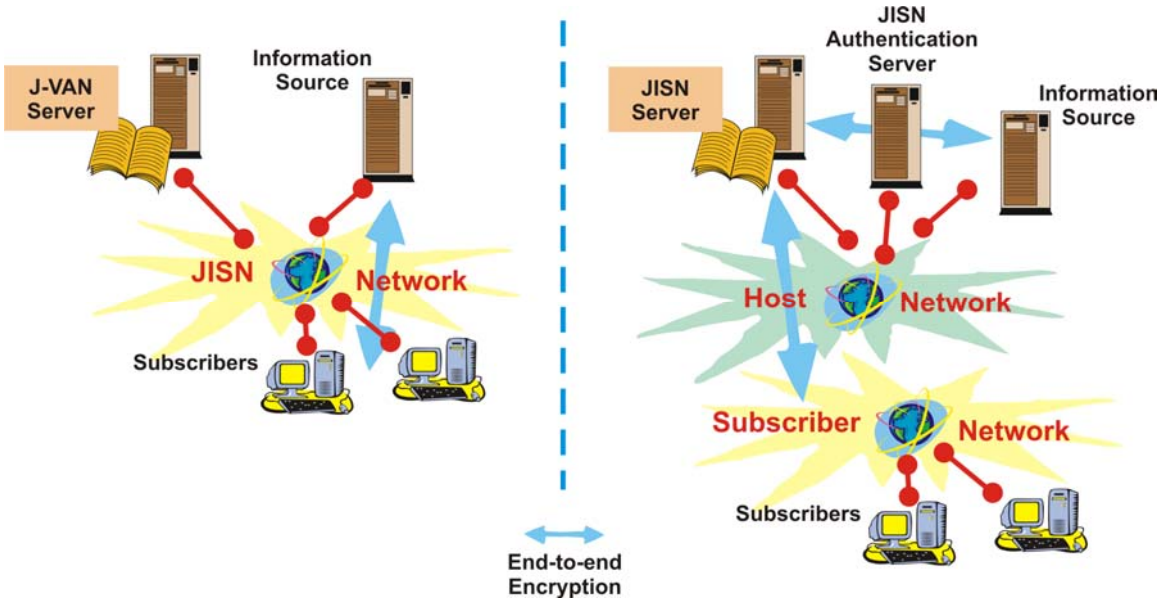
JISN. Reliable and secure messaging requires that each communicating party is certain who they are sending information to and guarantees that the contents of the message will not be compromised in transit.

As in all of the previous information sharing models, the JISN owners/managers must maintain written information security policies and practices with the objective of protecting these information flows. In addition, the data owners offering services on the network must be confident that the implementation of the JISN policies are sufficient to protect the information that they are providing to subscribers and the systems on which that information is stored.

Security Guidelines for Justice Interconnection Services Network (JISN) Model

The proper security approach for justice interconnection services network information sharing will depend upon the scope and nature of the value-added services provided. Figure 3-10: Security Practices to Support Brokered Information Flow Into the Justice Interconnection Services Network Model shows two possible levels of value-added service represented in side-by-side drawings. The drawing on the left side of the figure represents a JISN that serves primarily as a connectivity medium. On the right, the drawing represents a network that provides brokered connectivity to the information sources that are available through the JISN.

Figure 3-10: Security Practices to Support Brokered Information Flow Into the Justice Interconnection Services Network Model



In the left-hand drawing, the subscriber uses the JISN to identify and connect to an appropriate information source. Once that connection is made, the owner of the

information source has primary responsibility for the security procedures that govern the subscriber-to-information source session and information transfer. These procedures are similar to those that apply to the CIR model for subscriber-to-database information flow.

In the right-hand drawing, the JISN server takes a more active role in the subscriber-to-information source session. The JISN server brokers the session. The JISN server passes subscriber information requests on to the source database over a host-to-host connection. In this case, the security procedures that govern the subscriber-to-information source session are primarily set by the managers/owners of the JISN server. These procedures can be similar to those that apply to the CIR model for the subscriber-to-database information flow. The security procedures that govern the JISN server-to-information source session are agreed upon by the managers/owners of the JISN server and the information source. These procedures can be similar to those that apply to the CIR model for database-to-information source flow.

In both drawings, end-to-end encryption is included to protect the confidentiality of a subscriber's session. Since the JISN is likely to contain information sources with varying access requirements, it is important to ensure that traffic over the network is encrypted from endpoint to endpoint to reduce the risk that one user session can be intercepted by another user connected to the network. Protocols such as the secure socket layer protocol (SSL) can provide low-cost, low-overhead, end-to-end security and are particularly applicable in situations where the user-client software is a standard Internet browser.

The remainder of this section provides guidelines under each of the security disciplines.

Justice Interconnection Services Network (JISN) Model Disciplines

Firewalls, VPNs, and Other Network Safeguards

The JISN model arises from strategic alliances of law enforcement entities that have recognized commons goals and are looking to leverage data they may have or may hold for others by creating sharing initiatives among themselves. The connectivity in this model tends to involve groups of professionals from each participating organization that do formal analysis before any data can be exchanged. The policies for each organization are typically analyzed to determine acceptable sharing strategies that meet each entity's security needs. Each participant in this model must agree on how much to open their firewalls to allow the exchange of information, who is responsible for supporting the connections, and how vulnerabilities or breaches will be addressed. The use of a DMZ to isolate data sources to be shared from secure internal systems and from external networks would be typical in this firewall configuration. Logging becomes very important in this data sharing model, as there may be specific reporting requirements to the owners of data if a JISN provider is hosting information for another law enforcement agency. VPN technology may be employed depending on the sensitivity of the data. However, VPN-client access should be limited to the specific resources that are needed by the user to perform their authorized duties.

Critical Incident Response

Since there is a single management organization responsible for the JISN infrastructure, many of the guidelines for implementing a Computer Security Incident Response Capability (CSIRC) in the centralized sharing model apply. The difference is that the response team for the JISN must coordinate with the teams that serve each of the databases and information systems that the shared network interconnects.

Physical Security

The JISN model is similar to the other models in the necessity to establish physical security policies and procedures to protect the information. Each user organization has a responsibility to protect passwords, to restrict physical access, and to protect secure information obtained from the JISN model.

Identification and Authentication

The subscriber that gains access to the JISN will have access to many information sources. In general, the I&A procedure should be quite rigorous, as much as the most rigorous of I&A procedures of the native information source systems. As a minimum, strong passwords should be used, but as budget permits, the addition of a "something-you-have" factor, such as a hardware token or smart card, is recommended.

Figure 3-10 includes an authentication server. Authentication servers are a good way to implement "single logon" procedures (See Chapter 2, Objective 2: Prevention, Section Authentication Servers and Single Logon). Single logon allows JISN subscribers to gain access to all authorized information sources with a single password. In general, single logon systems provide higher assurance than systems that require subscribers to remember multiple passwords.

Authorization and Access Control

It is likely that the information sources connected to the JISN will carry varied levels of access privilege restrictions. Further, each individual information source system may have several levels of access privileges. In the left-hand drawing in Figure 3-10, authorization and access control is governed by the information source system in much the same way as the CIR model. In the right-hand drawing in Figure 3-10, authorization and access control is managed by the authentication server. The authentication server can implement an RBAC model for managing privileges of JISN subscribers. The JISN roles must be mapped into the levels of access privileges defined by each of the information source system managers/owners—there must be agreement and consistency between the JISN and information source managers on access roles.

Data Classification

The JISN model may have a security policy that creates consistent definitions that all information owners agree upon for each confidentiality, integrity, and/or availability level. For example, all open criminal investigation data might be labeled confidential, high-integrity, and high-availability. The policy should also include procedures for handling each of the different levels of sensitive or critical information. For example, confidential information might require encryption during storage and data transfer. However, the indices of open criminal investigation data might be public and may not require encryption. Information must be labeled to indicate the applicable levels. This method typically results in a memorandum of understanding, with each information provider specifying how the JISN owner will protect information resources and periodic security audits.

The JISN may alternatively choose to leave the security classifications to the specific database owners. Subscribers must adhere to unique security requirements for each database they access.

Public Access, Privacy, and Confidentiality

The JISN model must have a security policy that includes procedures for handling information subject to privacy laws. Information collected must be labeled as it is transmitted to indicate its privacy requirements, such as obtaining the subject's consent before disclosure outside the justice system. An authorization check must be performed to verify the subscriber meets requirements for use and dissemination of the information.

Intrusion Detection

Unlike the PG model that frequently involves allowing access to internal network resources, the CIR and JISN models are often configured to place data to be shared in locations outside of the firewalls that serve to protect sensitive internal resources. Data can be stored in locations separate from the core networks (DMZ), based upon its sensitivity. These areas are often protected by a second firewall that controls access to these shared resources. These models reduce the need to be concerned over the security profiles of subscriber agencies.

The size and scope of interconnectivity associated with the JISN model usually provides good rationale for implementing a comprehensive IDS. The focus of the IDS will be to monitor network resources, since each of the interconnected information system owners will generally be responsible for intrusion detection within their own systems.

Security Auditing

The guidelines provided in the disciplines area of Chapter 2, "Security Disciplines," apply to each of the organizations participating in JISN information sharing.

Disaster Recovery and Business Continuity

The guidelines provided in the disciplines area of Chapter 2, "Security Disciplines," Disaster Recovery and Business Continuity, apply to each of the organizations participating in the JISN model. Each JISN participant should have its own Disaster Recovery and Business Continuity plan. The plan may include having spare equipment in stock or signing agreements between organizations for hot- or warm-site support in the event of a disaster. The plan may also include alternate methods for transferring the information to subscribers, such as secure e-mail, couriers, registered mail, and phone support, depending on the time requirements.

Operational Examples of the Justice Interconnection Services Network (JISN) Model

National Law Enforcement Telecommunication System (NLETS)

Introduction

NLETS is a value-added network created, in its first form, in 1965 to meet the needs of law enforcement agencies for interstate communication. In 1965, the FBI had recently completed the central repository system called NCIC but had made a conscious decision not to facilitate interstate communication for the states.

The states collaborated to create NLETS so that databases held in each state could be shared for the benefit of law enforcement nationwide. This system was placed in Phoenix, Arizona, only because the Arizona Department of Public Safety (AZDPS) offered the space. NLETS was created and is owned and operated by a consortium of principal members (states, territories, and Washington, DC) that oversee a small paid staff.

Over the years, the system and network have been upgraded multiple times, increasing capacity and expanding services as customer demands increased. The NLETS network, which facilitates over 34 million transactions each month, is a "private" frame relay network, with networking services being purchased from a major network service provider. The NLETS business model fits well within the definition of a JISN model. All of the 50 states, U.S. territories, the District of Columbia, and over 20 federal agencies with a criminal justice component are connected via frame relay to each other. The hub of the system, or the "message switch," is located in Phoenix, as is the staff that operates NLETS.

NLETS inquiries can originate from any of the over 500,000 devices located in the United States and Canada. The inquiries may be made for any number of types of data accessed via the NLETS system. The formats that are used for the inquiries are standardized by NLETS to ensure compatibility for all users.

The following sections describe Security Practices that best exemplify the methods utilized by NLETS to operate within the JISN model. Topics include data integrity; physical security;

personnel security; identification, authentication, authorization, and access control; data classification and privacy; change management; and disaster recovery and business continuity.

Data Integrity

Data integrity, as it passes through the NLETS system, is very important to the officer on the street who is utilizing the information to make decisions that can result in the loss of freedom to citizens. The data must be protected as it leaves the state database where it is held until it arrives at the end user of the information. This is accomplished through security measures such as encryption, VPNs, and firewalls. NLETS utilizes VPNs within the private frame network to protect the data as it passes over NLETS. The data is encrypted at all times as it is carried via the VPN over the private network. The locations from where the data originates and terminates are secure criminal justice locations.

Physical Security

- **Network, Infrastructure, and Central Facilities**—The network and computing facilities maintained in NLETS space are leased from the AZDPS. These facilities are within the secure property, a walled and guarded complex providing excellent physical security for the central NLETS site. Entry to these areas is restricted to authorized NLETS staff and those escorted persons with a business need-to-access. These areas are controlled within the secured compound by computer-controlled badge access systems, physical locks, and cipher locks.

- **Customer Premises**—Since NLETS is a distributive system, each Control Terminal Agency (CTA) connected to the NLETS frame relay network must also be secure to ensure the overall security of the NLETS. In this model, the saying that a security system is only as strong as the weakest link is very true. Each CTA is required by policy to house its system within a physically secure location, allowing access to only those authorized persons with business needs for access.

Personnel Security

Access by authorized persons with a business need is an important component of physical security, but it is not the only criteria for access. Prior to allowing unescorted access to NLETS systems and networks, every person must successfully complete a background examination by the AZDPS for NLETS central-site employees or by the CTA at the customer site. This background check should include a name and date-of-birth check of state and federal criminal history files along with a fingerprint examination of state and federal automated fingerprint information systems. Checks that are recommended include employee reference checks along with credit checks of the employee or contractor wishing access. Unescorted access should not be allowed prior to the results of these checks being known. What constitutes a failure in these background checks is the responsibility of the

controlling agency, based upon severity of the crime for which a conviction has occurred, along with the amount of time that has elapsed since the offense.

Identification, Authentication, Authorization, and Access Control

The responsibilities related to these important functions fall to each of the over 70 CTAs that provide operational access to NLETS. These CTAs represent over 35,000 criminal justice agencies in the U.S. that have NLETS connectivity. Connectivity to NLETS is currently only available via a CTA connection. Individual practitioner access to NLETS is accomplished by accessing a distributed network access point controlled by the state or federal agency that is connected to NLETS. Each state or federal agency is responsible for ensuring that all practitioners accessing their network be identified and authenticated following NLETS- and NCIC-approved methods. For years, many CTA systems utilized terminal emulation with devices that were permanently "logged in" to the system. Anyone with physical access and knowledge of how to operate the system would have access to that CTA's information, and through that CTA, they would have access to NLETS and the NCIC systems as well.

Recent technical changes that have been occurring at varying speeds, based on resources within the CTAs, have been implementing robust identification and password systems to ensure appropriate access to the CTA and NLETS systems. Some jurisdictions have also added token devices ("something you have") to "something about yourself."

- **Physical Connectivity to NLETS**—Each request to connect to NLETS is evaluated on an individual basis by the NLETS Technical and Operations Committee (TOC), made up of technically competent managers from the membership (CTAs) of NLETS. Potential new customers wishing access to NLETS are required to submit a detailed network diagram and plan that demonstrates their adherence to the following NLETS security policies:

  - The NLETS router that is provided to the customer must be protected from the customer's Internet connection and Internet traffic by a customer-provided, firewall performing-packet inspection.

  - The NLETS router must be isolated from other external network connections coming into the customer site.

  - Any IP address routed across the NLETS network must be NLETS-assigned to the customer but not also routed on the Internet.

Data Classification and Privacy

All data exchanged via NLETS is considered to be for criminal justice purposes only. The data may bring with it the privacy classifications from where the data originated. Each state treats data differently. While some states may be open record states, others may have multiple layers of privacy protection on information that may be public elsewhere. Data classification being shared over a criminal justice system is generally controlled by the Code of Federal Regulations (CFR).

Change Management

All changes to the application are implemented according to NLETS standard methodology for system development. The revised specifications are reviewed by the TOC for appropriateness and impact to the CTAs. All systems are tested after changes are implemented and placed into production.

Disaster Recovery and Business Continuity

NLETS has a mirrored redundant set of hardware and network configurations located within the physically secure Meridian, Idaho, State Police compound. This site can be operational within 15 minutes should a disaster occur in the Phoenix area, taking down the central site. Testing of this facility takes place several times throughout the year, and the backup location is placed into operation for individual CTAs for varying local difficulties that occur throughout the year.

Conclusion

The need for criminal justice agencies to share information has never been more important than it is today. The day of large centralized databases holding hundreds of thousands of records no longer meets the business needs of the new millennium. NLETS is placed to meet these information sharing needs as a critical partner for criminal justice and as a JISN model that works for all who are connected.

Regional Information Sharing Systems (RISS)

Introduction

The Regional Information Sharing Systems (RISS) Program is a national program comprised of six regional intelligence centers operating in mutually exclusive geographic regions that include all 50 states, the District of Columbia, U.S. territories, Australia, Canada, and England. The six centers combined currently serve nearly 6,800 local, state, federal, and tribal law enforcement member agencies by facilitating and encouraging information sharing and communications to support their investigative and prosecution efforts. Typical targets of RISS activities are terrorism, drug trafficking, violent crime, cybercrime, gang activity, and organized criminal activities. Since September 11, 2001, increased emphasis has been placed on anti-terrorism activity, in addition to traditional activities.

RISS operates RISSNET™—the RISS nationwide secure criminal intelligence network for communications and information sharing by law enforcement member agencies. Using Internet technology, RISSNET is a secure private intranet that connects the six RISS centers and their participating law enforcement member agencies, as well as agency systems electronically connected as nodes. The participants may be either single computer

connections from a member agency user or node connections of an agency network. Node connections to RISSNET expand the resources and information available to law enforcement users. An important service provided on RISSNET is the availability of secure e-mail among participants. Other important services on RISSNET are the RISS Investigative Leads Bulletin Board (RISSLeads), the RISS Criminal Intelligence Databases (RISSIntel), the RISS National Gang Database (RISSGang), the RISS training Web site (RISSTraining), as well as access to each center's Web site for additional information and services, such as criminal activity bulletins and publications. RISS has developed a search capability, called RISSSearch, to assist users in locating information available on RISSNET. This search capability is currently implemented on all RISS-maintained resources and may be extended to help locate information on node-maintained information as well. Currently, RISS is in the process of implementing RISSLinks, a data visualization tool. RISSLinks will provide member agencies with the capability of retrieving data from the RISS criminal intelligence databases in the form of a link chart. The link chart will graphically show all associations of the result of an inquiry.

Firewalls, VPNs, and Other Network Safeguards

The RISS secure intranet (RISSNET) protects information through use of VPNs and multiple firewalls to prevent unauthorized access. A systematic layering of firewalls helps to compartmentalize security. This practice is employed to help contain breaches should they occur and provides an environment that allows the sharing of only necessary components to system users who are outside a firewall. The analogy most similar to this configuration is a bank. A bank may have locks on the external doors, a more sophisticated lock on the bank's vault, and locked safety deposit boxes within the safe. Even if a safety deposit box owner were to gain access within a bank vault, he would still only have access to the contents of his own box unless another box owner provided him access to another box.

The VPN technology that RISS employs allows access only after a user is satisfactorily authenticated. Once authentication has been successfully completed, a user is assigned a set of privileges to access resources that exist on RISSNET. The resources are unknown to the public Internet and may only be accessed using specific VPN-client software. The software maintains the resource list only in volatile memory, and a new set of privileges is sent to the user at the start of each VPN-access session. Communications between the client and the RISSNET resource are encrypted with triple Data Encryption Standard (DES) or Advanced Encryption Standard (AES). The key that is used to encrypt the communication is different for each session, as the key negotiation is based on a large key space that uses portions of the key to encrypt each session.

Authentication and Authorization

RISS currently requires a two-factor authentication to allow remote users to gain access to resources protected by firewalls on RISSNET. Authentication to RISSNET resources requires either a smart card or a software-based token along with a passcode required to enable the token. Authorization to RISSNET resources is provided by way of a list of entitlements that a user receives, which is based on a preconfigured account set up by RISS staff. The set of entitlements is sent to the user after authentication. The user's set of authorized entitlements is maintained on a secure server on RISSNET. The list of entitlements is sent in an encrypted

message to the user and is held in system memory until the client software is shut down. There are also time-out parameters, which control how a user must reauthenticate. RISS is currently evaluating allowing a user that has a trusted credential from another system to access RISS resources if the system issuing the credential has been vetted as trustworthy by RISS.

There is a feature of the RISS security systems that identifies all transmission control protocol/Internet protocol network transmissions after a user has been authenticated and received permissions to access resources. This feature is used to allow RISSNET users to access RISS database resources with no further login. The user-usage information is logged in multiple locations to ease the tracking of a user-usage pattern.

Disaster Recovery

RISS has created systems in several areas to ensure continued operation should catastrophic circumstances be experienced in areas where RISS facilities exist. RISS resources exist in a distributed environment. This makes the likelihood that all sites would be affected by a single disaster unlikely. However, there are certain critical areas where RISS has focused its efforts.

RISS performs tape backups of data and maintains them in an off-site secure location. The grandfather-father-son archive approach is used to ensure data integrity. Log files are routinely written to a CD-ROM media for potential future use. RISS has initiated a backup procedure where data is transmitted to a designated sister RISS center for storage and mounting for system access if required.

RISS has created a recovery site for its communications infrastructure to provide backup capability should a catastrophic disaster be experienced at its primary communications hub. RISS has an alternate Internet connection and the capacity to recreate the RISS secure intranet backbone via Integrated Services Digital Network backup.

RISS employs backup power sources to ensure that data is still available should electrical outages occur. All centers utilize UPS backup capability, and the central communications facility has an electrical generator for extended electrical outages.

Security Monitoring and Logging

There are a number of different services that are available on RISSNET, and each is monitored through several mechanisms. The initial logging of any user activity begins when the user attempts to access resources on RISSNET. The RISS gateway firewall records all user session information. Each subsequent firewall that a user traverses records information about what resources a user accessed. Another level of logging occurs at the application level. Detail logs are maintained regarding e-mail access, Web server access, and electronic bulletin board access. The highest-level detail logging of RISSNET resources occurs at the database access level. Information is captured regarding who is in the system and what information they are accessing. These logs are reviewed by various staff on a regular basis depending on the log to be reviewed. All logs are archived for future reference.

RISS staff reviews usage patterns of RISSNET to look for potential abuses. Traffic analyses are looked at regularly to help identify unusual usage. There are also regular reviews of the user database to help identify any unusual accounts that may exist.

Physical Security

All RISS resources are maintained in secure facilities with limited access and monitored alarm security. All visitors must sign in when entering a RISS facility and be escorted by a RISS staff member for the duration of the time they are there. Equipment is located in a climate-controlled room that has additional access controls. This includes the telephone equipment room for each center.

Intrusion Detection

RISS employs IDSs at multiple levels to help identify potential security threats on RISSNET. There is an initial IDS that scans for potential threats launched from the Internet and another set of IDS deployments that scan for potential threats that may be launched from the RISSNET frame relay cloud. RISS staff monitors the output from each IDS to determine the validity and severity of all potential security threats.

Data Classification/Privacy

The information maintained in RISS databases is contributed by participating law enforcement member agencies, and the contributing agency maintains ownership of information they contribute. Information may only be disseminated if an agency provides its approval to do so. When queries occur, notification of a hit is provided to the agency that contributed the information regarding who made the query. This allows agencies that have a common interest in an individual to contact each other, thus facilitating a more extensive exchange of information.

The data maintained in the system must meet the requirements set forth in 28 CFR Part 23, including reasonable suspicion of criminal activity. In addition, all information must relate to multijurisdictional criminal activity. Data is reviewed for compliance with this regulation by RISS staff. Additional data checks for 28 CFR Part 23 compliance are done randomly by the Office of Justice Programs, Office of General Counsel, and the Bureau of Justice Assistance. Data contributed to a RISS database by an agency may be retained in the system for a maximum five-year period. After five years, the data must be purged if there has not been a substantial update to it.

The RISS criminal intelligence databases may only be accessed by authorized member agency law enforcement personnel. Dissemination is based on a need-to-know and right-to-know the information in performance of law enforcement activities.

Critical Incident Response

RISS has a policy that centralizes responsibility of investigating all potential intrusions with a central group. Each RISS center or node agency connected to RISSNET has the responsibility of reporting potential intrusions to the central group. The policy has laid out procedures that make sure the correct staff is involved in an investigation of possible intrusions, define the scope of the response, determine the appropriate reporting mechanisms, and identify actions necessary to return the system to normal operations.

AAMVAnet Case Study

Introduction

The American Association for Motor Vehicle Administrators network (AAMVAnet) value-added network (VAN) was created in 1988, as a result of the Commercial Motor Vehicle Safety Act of 1986. The Act mandates that every Department of Motor Vehicles be able to exchange, electronically and in real time, information on commercial driver licenses (CDL). This is an effort to ensure that every commercial driver in the United States has one and only one CDL.

The network is a private network managed by a leading network provider and is an example of the JISN model. All U.S. jurisdictions are attached to the network via a frame relay line, for the majority. They have access to a central database containing the key information (name, date of birth, social security number, and driver's license number with issuing state) of every U.S. commercial driver. Prior to issuing a new CDL, each state must query the central site to make sure that the person is not already licensed. It is also the state's responsibility to update the central site information, in real time, with the information of the new CDL when it is issued.

The following sections describe Security Practices that best exemplify the JISN model. Security topics include data integrity, physical security, identification, authentication, authorization, access control, data classification, privacy, change management, disaster recovery, and business continuity.

Data Integrity

Data integrity is of the utmost importance for maintaining, in real time, a distributed database of CDLs nationwide. To maintain a very high level of data integrity, AAMVA is certifying every jurisdiction's system through a stringent set of structured tests on a test network. Once they pass the certification, jurisdictions are promoted to the production network. Every jurisdiction must also be retested after any major system change.

Physical Security

- **Network Infrastructure and Central Database Facilities**—The network and computing facilities are maintained in AAMVA's network and system

providers' owned buildings, with controlled access areas separate from general office areas. Entry to these areas is restricted to only those authorized personnel with current business needs for access. Each controlled access area has a designated access custodian responsible for determining those individuals to be granted access. These areas are controlled via computer-controlled, badge-access systems, physical locks, cipher locks, or other locking mechanisms. The access custodian is also responsible for:

- Reviewing and approving access requests based on valid business requirements.
- Maintaining a visitor log of nonroutine accesses.
- Reviewing the approved access list on a periodic basis, at least every quarter, to remove persons who no longer need access. This does not preclude the requirement to immediately remove access for those whose need has expired (i.e., termination or transfer).

- **Customer Premises Equipment**—The network-provided, customer-premises equipment can be accessed either physically or remotely through a dial-up connection for maintenance and troubleshooting by authorized AAMVA network provider personnel. Physical access into the customer facilities housing the AAMVA network provider equipment is governed by customer policy and procedures. Access to the equipment is controlled at the most basic layer via password. Only authorized AAMVA network provider personnel have access to the passwords, which are required to be changed at regular intervals. Access via a dial-up connection to customer premises equipment is accessible only from specific network management hosts and only by authorized support personnel.

  Network support personnel access to these management hosts is controlled and revalidated on a regular basis, ensuring that only personnel managing the customer networks have access to these management hosts. In addition, access to the customer routers from the network management host is controlled by an authenticating server, which validates and verifies user accesses. "Telnet" and "SNMP" traffic to the customer router is allowed, but only from the Network Management server hosts.

Identification, Authentication, Authorization, and Access Control

- **Systems Network Architecture (SNA) Services and Hosts**—All access to SNA services and hosts is controlled by a network application known as the Service Manager, which:

  - Provides the initial connection point into the network for users, devices, and applications.

- Identifies and authenticates the user, device, or application.

- Validates the user, device, or application request for a session, based upon the authorizations profiled in the user, device, or application profile.

- Passes the session request to the destination network, application, or service.

Each resource, user, device, or application defined to the network has a profile in the Service Manager. The profile explicitly states what other network resources or services can be accessed and what type of access is allowed.

When an application or device requests a session through the network, the Service Manager first validates that the requesting application/device is authorized to access the network and is of the type described in its Service Manager resource profile. Then, the Service Manager checks the application profiles of both the origination and destination applications to ensure that the applications have been authorized to communicate with each other. Finally, the Service Manager will pass the session request to the destination application's network.

- **Internet Protocol (IP) Services and Hosts**—Access to IP services and hosts is controlled at the network layer via permanent virtual circuits (PVC). There must be a PVC definition between sites before they can have the potential to communicate, with each site providing written authorization for the creation of the PVC. Once the PVC is in place, further access is controlled through the use of access lists and router filters, which reside on each customer premises router and the AAMVAnet intermediate network routers. The general rule for access to IP host and services across AAMVAnet is that access is denied unless explicitly authorized.

- **AAMVA Applications**—In addition to the general identification, authorization, authentication, and access controls described above, there are additional levels of each within the AAMVA application message switch application, Network Control Software (NCS). Each entity communicates only with the NCS, and since there is no direct trading partner to trading partner communication, the NCS performs all trading partner identification, authorization, and authentication. Each site is known to the NCS by a site identifier, which is then hard-coded within the NCS to the site's SNA virtual telecommunication access-method application logical unit or their IP address and port. The combination of site identifier and logical network information create the unique identifier for a site.

  AAMVA has complete and sole control over allocating site identifiers and authorizing sites to be added to the NCS, as well as authorizing the necessary

Service Manager application profile changes required to enable the communication at the higher level.

- **Physical Connectivity to the VAN**—Each request to connect to the VAN is evaluated on an individual basis by several groups of highly qualified VAN network personnel, including network designers, security teams, and network technical support personnel. Potential customers are required to submit a detailed network diagram that demonstrates their adherence to the following VAN security policies.

  - The VAN-provided customer premises equipment must be protected from the customer's Internet connection and Internet traffic by a customer-provided firewall performing stateful packet inspection.

  - The VAN-provided customer premises equipment must be isolated from other external network connections coming into the customer site.

  - Any IP addresses routed across the VAN must be American Registry of Internet Numbers (ARIN)–registered to the customer and not also routed on the Internet.

- **Intrusion Detection Systems**—The VAN employs a combination of both host- and network-based tools to perform intrusion detection to determine whether any initiatives to penetrate network components have been attempted by nonauthorized personnel. The tools used are leading-edge scan tools from a widely recognized commercial software provider. Maintaining this information as confidential is, in itself, a facet of the VAN's security program that protects all customers.

  In addition to intrusion detection tools, the VAN employs "ethical hackers," who probe the VAN in an attempt to uncover weaknesses in security systems and processes.

  Upon occurrence of a security incident, the VAN identifies the level of the potential impact and notifies AAMVA. If specific customers are determined to be at risk, they will be notified.

- **Security Auditing**—The VAN regularly conducts security status checks to ensure that security controls are maintained in place and are functioning in accordance with plan. These initiatives include *health checking* and *vulnerability scanning*. Results from these activities are reviewed by each region for closure and for any required follow-up actions.

- **Health Checking**—Health checking is performed on a regular basis, involving the review and verification of system security settings, operating system resource security settings and status, and users having security administrative authority or system authority.

Health checking also includes the verification of network elements to ensure the proper level of security "fixes" are maintained, to ensure only those system processes required are active, to ensure the existence and retention of activity logs, and to verify support personnel accesses.

The local service providers and security personnel perform security status checking on an ongoing basis. During security reviews, the review team, as part of the review process, conducts status checking.

- **Vulnerability Scanning**—Vulnerability scanning is performed by authorized personnel to verify whether controls can be bypassed to obtain security administrative authority or system authority/access.

  Vulnerability scans to test the level of safeguards on network components are performed on a varying frequency based on the risk of compromise, utilizing authorized and leading-edge scanning tools. Vulnerability scans are performed quarterly.

Data Classification and Privacy

All data exchanged within the CDL application is classified and protected under the Commercial Vehicle Safety Act and the Driver Privacy Protection Act (DPPA). These two Acts specify who can access the data and under which conditions. In addition, most states have passed additional legislation to complement or reinforce the DPPA regulation. Therefore, individual jurisdictions have developed their own set of procedures to classify and protect drivers' data privacy.

Change Management

All changes to the application are implemented according to AAMVA standard methodology for system development. The revised specifications are reviewed and approved by ad hoc working groups composed of state and U.S. Department of Transportation representatives.

All systems (state and central site) are retested and certified after the changes have been implemented. The new programs are then promoted to the production environment after all the certifications have been passed.

Disaster Recovery and Business Continuity

Central-site disaster recovery drills are performed on a yearly basis at a different geographical location than the primary system's location.

A backup facility for the message switch is also hosted at a different geographical location than the primary facility and can be activated in less than 15 minutes. Testing of the backup facility is completed twice a year.

Appendix A: Glossary of Security Acronyms and Terminology

AAMVA	American Association of Motor Vehicle Administrators
Acceptable Risk	A concern that is acceptable to responsible management, due to the cost and magnitude of implementing controls
Access Control	Procedures and controls that limit or detect access to critical information resources. This can be accomplished through software, biometrics devices, or physical access to a controlled space.
Access Control Policy	The set of rules that define the conditions under which an access may take place
Access Level	The hierarchical security level used to identify the sensitivity of data and the clearance or authorization of users
Accountability	The security objective that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection, and after-action recovery and legal action.
ACL	Access Control List
ACLU	American Civil Liberties Union
AEA	Advanced Encryption Algorithm

AES	Advanced Encryption Standard
AFIS	Automated Fingerprint Identification System
AIS	Automated Information System
Algorithms	Complex mathematical formulae that are one component of encryption
Anonymizer	Anonymizer is a gateway to keep Web surfing anonymous and preserve privacy online when surfing the Web, sending e-mail, or posting to a newsgroup. By using the Anonymizer, any information and IP addresses that are collected will be false information. By hiding an IP address, one can eliminate the possibility of a DoS attack. See <http://www.anonymizer.com>.
ANSI	American National Standards Institute
Armored Virus	An armored virus tries to prevent analysts from examining its code. The virus may use methods to make tracing, disassembling, and reverse engineering its code more difficult.
APB	Advisory Policy Board
ASCII	American Standard Code for Information Interchange
Assurance	The grounds for confidence that an entity meets its security objectives
Audit	The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures and to recommend any indicated changes in controls, policy, or procedures

Audit Trail A chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to results

Authentication Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system

Authorization The granting or denying of access rights to a user, program, or process

Authorized A system entity or actor is granted the right, permission, or capability to access a system resource. See Authorization.

Availability Timely, reliable access to data and information services for authorized users; protection against intentional or accidental attempts to perform unauthorized deletion of data or otherwise cause a denial of service or data

Back door A feature built into a program by its designer which allows the designer special privileges that are denied to the normal users of the program. A back door in an EXE or COM program, for instance, could enable the designer to access special set-up functions.

Backup A duplicate copy of data made for archiving purposes or for protecting against data loss. A backup is considered secure only if it is stored away from the original.

BIA Business Impact Analysis

Binary A numbering system based on twos (2s) rather than tens (10s). Each element has a digit value of either one (1) or zero (0) and is known as a bit.

Biometrics	Biometrics is the science and technology of measuring and statistically analyzing biological data. In information technology, biometrics usually refers to automated technologies for authenticating and verifying human body characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements.
Bit	See Binary.
Brute Force Attack	An attack in which each possible key or password is attempted until the correct one is found
C&A	Certification and Accreditation
CA	Certification Authority—An authority that issues and manages security credentials for a PKI
CA Privacy Root Key	Cryptographic key known only to the CA. It is used to verify user or server certificate requests (digitally signed certificates).
CAPI	Cryptographic Application Programming Interface
Carnivore	The Internet surveillance system developed by the Federal Bureau of Investigation to monitor the electronic transmissions of criminal suspects
CCITSE	Common Criteria for Information Technology Security Evaluation
CDL	Commercial Driver License
CERT®/CC	CERT® Coordination Center
Certificate	In cryptography, an electronic document binding some pieces of information together, such as a user's identity and public key. Certifying Authorities (CAs) provide certificates.

Certificate Owner	The person that has access to use the certificate. This access could be protected by a password, a smart card, or other device.
CFR	Code of Federal Regulations
Chief Information Officer (CIO)	The highest-level person responsible for policy concerning information systems and telecommunications systems
CHRI	Criminal History Record Information
CIP	Critical Infrastructure Protection
Cipher	An alternative term for an encryption algorithm
Ciphertext	Encrypted data
CIR	Centralized Information Repository
CIS	Center for Internet Security
CJIS	Criminal Justice Information Services
CKMS	Centralized Key Management System
Compromise	To access or disclose information without authorization
Computer Emergency Response Team (CERT®)	(1) The people who are responsible for coordinating the response to computer security incidents in an organization. (2) CERT® is one of the main agencies for Internet security formed by the Defense Advanced Research Projects Agency (DARPA) in 1988 to aid the Internet community in responding to computer security events, raise awareness of computer security issues, and conduct research aimed at improving security systems. See <http://www.cert.org> for more information.

Computer Security Incident Response Capability (CSIRC)	A set of policies and procedures defining security incidents and governing the actions to be taken when they occur
Confidentiality	Assurance that information is not disclosed to unauthorized persons, processes, or devices. Confidentiality covers data in storage, during processing, and while in transit.
Contingency Plan	A plan maintained for emergency response, backup operations, and postdisaster recovery for an AIS, to ensure availability of critical resources and to facilitate the continuity of operations in an emergency
Cookies	Blocks of text placed in a file on a computer's hard disk. Web sites use cookies to identify users who revisit the site.
Countermeasure	Any action, device, procedure, technique, or other measure that reduces a system's vulnerability to a threat
CPO	Chief Privacy Officer
Cracker	One who breaks security on an automated system
Critical Security Perimeters (CSPs)	Security-related information (e.g., cryptographic keys, authentication data such as passwords and PINs) appearing in plaintext or an otherwise unprotected form and whose disclosure or modification can compromise the security of a cryptographic module or the security of the information protected by the module
CRL	Certificate Revocation List
CRT	Central Response Team
Cryptography	The art and science of using mathematics to secure information and create a high degree of trust in the electronic realm
CSA	Computer Security Act of 1987

CSD	Computer Security Division
CSS	Card Scanning Service
CSIRTs	Computer Security Incident Response Teams
CSMA/CD	Carrier Sense Multiple Access/Collision Detect
CSO	Central Security Officer
CSRC	Computer Security Resource Center
CTA	Control Terminal Agency
CTO	Control Terminal Officer
DAC	Discretionary Access Control
DAC	Data Authentication Code—also known as a Message Authentication Code (MAC) in ANSI standards
DBMS	Database Management System
Decryption	The process of changing ciphertext into plaintext
Denial-of-Service (DoS)	This is an indirect attack to a site. Hackers are not trying to get into the site itself, but they are trying to keep everyone else from getting into the site.
DES	Data Encryption Standard
Dictionary Attack	A password-cracking technique that uses words in a dictionary to crack passwords

DID	Distributed Intrusion Detection
Digital Fingerprint	A number that is unique to a digital certificate, used to verify if a signature is valid
Digital Signature	The result of a cryptographic transformation of data that, when properly implemented, provides the services of origin authentication, data integrity, and signer nonrepudiation
Digital Timestamp	A record mathematically linking a document to a time and a date
Distributed Denial-of-Service (DDoS) Attacks	Hackers launch attacks by using several smaller network connections, making it harder to detect. DDoS can inundate the largest ISPs and consume all their bandwidth.
DMS	Defense Messaging System
DMZ	Demilitarized Zone, a network inserted as a "buffer zone" between a company's private, or trusted, network and the outside, nontrusted network
DSA	Digital Signature Algorithm—used by a signatory to generate a digital signature on data and by a verifier to verify the authenticity of the signature
DSO	District Security Officer
DSS	Digital Signature Standard
DSSV	Digital Signature Storage and Verification
EAL	Evaluation Assurance Level 4 as defined by the Common Criteria for Information Technology Security Evaluation (CCITSE). EALs provide a uniformly increasing scale which balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. There are seven hierarchically ordered EALs. The higher the EAL, the greater the degree of assurance.

E-mail Bombing	Flooding a site with enough mail to overwhelm its e-mail system. Used to hide or prevent receipt of e-mail during an attack or as retaliation against a site.
EAM	Extranet Access Management
ECC	Elliptic Curve Cryptosystem
EDI	Electronic Data Interchange
Encryption	The process of cryptographically converting plaintext electronic data to a form unintelligible to anyone except the intended recipient
EPIC	Electronic Privacy Information Center
ERB	Engineering Review Board
Expiration Date IEEE	All digital certificates should have an expiration date (Institute of Electrical and Electronics Engineers). A body that creates some cryptographic standards.
FAR	False Acceptance Rate
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
File Viruses	Usually replace or attach themselves to COM and EXE files. They can also be files with the extensions SYS, DRV, BIN, OVL, DOC, VBS, SCR, and OVY.
FIPs	Fair Information Practices
FIPS	Federal Information Processing Standard

FIPS PUB	Federal Information Processing Standard Publication
Firewall	A system designed to prevent unauthorized accesses to or from a private network. Often used to prevent Internet users from accessing private networks connected to the Internet.
Firewall Boundary	A commonly used term referring to a security perimeter that is largely defined by the presence of one or more firewalls
FIRST	Forum of Incident Response and Security Teams. See <http://www.first.org>.
Footprinting	Also known as profiling, the process of obtaining data about a particular individual or company
FRR	False Rejection Rate
FTC	Federal Trade Commission
FTP	File Transfer Protocol, a means to exchange files across a network
GASSP	Generally Accepted System Security Principles
Gopher Protocol	Designed to allow a user to transfer text or binary files among computer hosts across networks
Hacking	Unauthorized use or attempts to circumvent or bypass the security mechanisms of an information system or network
"Hactivism"	Politically motivated attacks on publicly accessible Web pages or e-mail servers
HIDS	Host computer Intrusion Detection Systems
HTML	HyperText Markup Language, the mechanism used to create Web pages

I&A	Identification and Authentication
IAFIS	Integrated Automated Fingerprint Identification System
ICDAG	Interagency Confidentiality and Data Access Group
ICMP	Internet Control Message Protocol
IDIP	Intruder Detection and Isolation Protocol
IDWG	Intrusion Detection Working Group
IDXP	Intrusion Detection Exchange Protocol
IETF	Internet Engineering Task Force
III	Interstate Identification Index
IJIS	Integrated Justice Information Systems. See <http://www.ijis.org>.
IMAP	Internet Message Access Protocol
Insider Threat	A disgruntled insider with knowledge of the victim's system
Integrity	Preservation of the original quality and accuracy of data in written or electronic form
Intermediary	A program or set of programs that in some way evaluate, filter, modify, or otherwise interject some function between two end users or end-use programs such as a client/server. An example is the proxy server that most companies place between their internal Web users and the public Internet.

Intrusion Detection Systems (IDS)	Techniques that try to detect intrusion or unauthorized entry into a computer or network by observation of actions, security logs, or audit data. Intrusion detection is the discovery of break-ins or attempted break-ins either manually or via specific software systems that operate on logs or other information available on the network.
IP	Internet Protocol
IP Security (IPsec)	IPsec adds security features to the standard IP protocol to provide confidentiality and integrity services.
IP Spoofing	An attack where a hacker outside the network attempts to impersonate a computer from the trusted network
ISO	Information Security Officer
ISO	International Standards Organization
ISPs	Internet Service Providers
IT	Information Technology
ITMS	Information Technology Management Section
ITN	Identification Tasking and Networking
IWG	IJIS Industry Working Group. See <http://www.ijis.org>.
JISN	Justice Interconnection Services Network
JTF	Joint Task Force
KEA	Key Exchange Algorithm

Key	A series of numbers used by an encryption algorithm to transform plaintext data into encrypted data
Key Encrypting Key (KEK)	A cryptographic key that is used for the encryption or decryption of other keys
Key Escrow	The system of giving a piece of a key to each of a certain number of trustees such that the key can be recovered with the collaboration of all the trustees
Key Recovery	A secure means for backup and recovery of encryption key pairs
Key Serial Number	A 128-bit number associated with a certificate
Keyring File	A file that can house the certificate
Killer Packets	A method of disabling a system by sending Ethernet or IP packets that exploit bugs in the networking code to crash the system. See SYN Floods.
KMF	Key Management Facility
KTC	Key Translation Center
LAN	Local Area Network
LEIF	Law Enforcement Interconnecting Facilities
Lightweight Directory Access Protocol (LDAP)	A standardized way to connect with a directory that might hold passwords, addresses, public encryption keys, and other exchange-facilitating data
Local Registration Authority (LRA)	A person who evaluates and approves or rejects certificate applications on behalf of a CA
MAC	Mandatory Access Control or Message Authentication Code

MIME	Multipurpose Internet Mail Extensions
MISPC	Minimum Interoperability Specification for PKI Components
Misuse	Illicit activity that exploits system vulnerabilities or file access privileges
MIT	Massachusetts Institution of Technology
NAPs	Network Access Points
NASCIO	National Association of State Chief Information Officers
NAT	Network Address Translation
NCIC	National Crime Information Center
NCS	Network Control Software
NCSC	National Center for State Courts
NIAP	National Information Assurance Partnership
NIDS	Network Intrusion Detection System
NIPC	National Infrastructure Protection Center
NIST	National Institute of Standards and Technology. See <http://www.nist.gov>.
NLETS	National Law Enforcement Telecommunication System

NNTP	Network News Transfer Protocol, protocol for Usenet news distribution
Nonrepudiation	The cryptographic assurance that a message sender cannot later deny sending a message or that the recipient cannot deny receipt
NSA	National Security Agency. See <http://www.nsa.gov>.
NTIS	National Technical Information Service
OECD	Organization for Economic Cooperation and Development
OMB	Office of Management and Budget
Open Systems Interconnection (OSI)	Also known as the OSI reference model. This describes a standard for how messages should be transmitted between any two points in a network. The reference model defines seven layers that take place at each end of a communication.
ORI	Originating Agency Identifier
OSCA	Office of State Court Administrators
P3P	Platform for Privacy Preferences
Packet	A unit of data that is routed between an origin and a destination on the Internet
Password	A string of characters used to authenticate an identity or to verify access authorization
PDP	Privacy Design Principle

Personal/Person-Identifiable Information	Information about the characteristics or activities of an identifiable natural person, including information about individuals who may not be explicitly identified, but whose identity could be inferred from elements of the data. Sensitive data elements in existing databases can include name, address, social security number, ID numbers, and birth date.
Physical Security Policy	A document specifying the steps to take to protect the actual machines used to store and process sensitive or valuable data
PIA	Privacy Impact Assessment
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	See Public Key Infrastructure.
Plaintext	Unencrypted (unenciphered) data
POC	Point-of-Contact
PP	Protection Profile
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
Pretty Good Privacy (PGP)	This set of standardized security procedures and algorithms provides authentication and privacy services and is most frequently used for secure e-mail. More information about PGP is available at <http://www.pgp.com>.
Privacy	The right of an entity (normally a person), acting on its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others

Privacy Seals	The seals of approval granted by organizations such as TRUSTe, BBBOnline, and WebTrust. The seals intend to demonstrate that a Web site has adopted appropriate policies to protect personal information and to assure individuals that they are visiting a Web site they can trust. Disclaimer—keep in mind that these seals are not monitored, and anyone can "stick" a seal on their Web site.
Private Key	The key of the public key pair that is not shared by its owner
PRNG	PseudoRandom Number Generator
Protected Resource	A target, access to which is restricted by an access control policy
Protocol	A set of rules (i.e., formats and procedures) for communications that computers use when sending signals between themselves
Public Key	The key of the public key pair that is widely shared, generally through a digital certificate
Public Key Cryptography	Cryptography based on methods involving a public key and a private key
Public Key Infrastructure (PKI)	An architecture which is used to bind public keys to entities, enable other entities to verify public key bindings, revoke such bindings, and provide other services critical to managing public keys
PVC	Permanent Virtual Circuits
RACF	Resource Access Control Facility
RBAC	Role-Based Access Control
RC2, RC4	Specific standardized block ciphers algorithms (Rivest Cipher or Ron's Code)

"Recreational Hackers"	Persons who crack into networks for the thrill of the challenge or for bragging rights in the hacker community
Registration Authority	A mechanism or person that, as part of a PKI, is involved in verifying and enrolling users
Release	Disclosure of documents (records) containing personal information to a third-party requester
Remote Access	Potential entry point for an attack that uses a war dialer and a password hacking tool to make login attempts
RFC	Request for Comments
Risk	An expectation of loss or threat that can be expressed as the probability that a particular threat (or set of threats) will exploit a particular vulnerability with particularly harmful results
Risk Analysis/Risk Assessment	The process of examining all risks, then ranking those risks by level of severity. Risk analysis involves determining what you need to protect, what you need to protect it from, and how to protect it.
Risk Management	The total process of identifying, controlling, and mitigating information technology-related risks; cost-benefit analysis; and the selection, implementation, testing, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission/business and constraints due to policy, regulations, and laws.
RISS	Regional Information Sharing Systems
Router	A device or, in some cases, software in a computer that determines the next network point to which a packet should be forwarded toward its destination
RSA	Rivest-Shamir-Adelman public key encryption algorithm

Rules of Behavior	The rules that have been established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of federal government equipment, assignment and limitation of system privileges, and individual accountability.
S-HTTP	Secure HyperText Transfer Protocol
S/MIME	Secure Multipurpose Internet Mail Extensions
S/WAN	Secure Wide Area Network
SAML	Security Assertion Markup Language
Security Assertion Markup Language (SAML)	An XML security standard for exchanging authentication and authorization information
Security Discipline	A set of subjects, their information objects, and a common security policy
Security Goal	To enable an organization to meet all mission/business objectives by implementing systems with due care and consideration of information technology-related risks to the organization, its partners, and its customers
Security Objectives	The five security objectives are integrity, availability, confidentiality, accountability, and assurance.
Security Policy	The statement of required protection of the information objects
Secure Socket Layer Protocol (SSL)	Invented by Netscape Communications, Inc. This protocol provides end-to-end encryption of application layer network traffic.

Secret Key	In secret-key cryptography, this is the key used both for encryption and decryption.
Sensitive Information	Information whose loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of federal programs or the privacy to which individuals are entitled
SHA-1	Cryptographic hash algorithm that is optimized for high-end processors and produces a 160-bit digest
Shoulder Surfing	Stealing passwords or PINs by looking over someone's shoulder
SLA	Service Level Agreement
Smart Card	A small plastic card with a microprocessor that can store information
SMTP	Simple Mail Transfer Protocol
Smurfing	The attacking of a network by exploiting Internet Protocol broadcast addressing and certain other aspects of Internet operations. Smurfing uses a program called Smurf and similar programs to cause the attacked part of a network to become inoperable.
SNA	Systems Network Architecture
Sniffer	A program to capture data across a computer network. Used by hackers to capture user names and passwords. Software tool that audits and identifies network traffic packets. It is also used legitimately by network operations and maintenance personnel to troubleshoot network problems.
Social Engineering	Subverting information system security by using nontechnical, social means
Spamming	Sending unsolicited e-mail

Standards	Conditions and protocols set forth to allow uniformity within communications and virtually all computer activity
SYN Floods	A method of disabling a system by sending more TCP SYN packets than its networking code can handle. See Killer Packets.
TOC	Technical and Operations Committee
Target of Evaluation	An information technology (IT) product or system and its associated administrator and user guidance documentation that is the subject of an evaluation
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol and Internet Protocol
Telnet Protocol	A communication protocol used to (possibly remote) log on to a computer host
Threat	An event or activity, deliberate or unintentional, with the potential for causing harm to an information technology (IT) system or activity
TRB	Technical Review Board
Trinoo	A Trojan horse used by hackers to launch a Distributed Denial-of-Service (DDoS) attack
Triple DES	A technique used to make Data Encryption Standard encryption stronger by applying the algorithm three times
Tripwires	A mechanism or tool that detects hack attacks and alerts someone, such as an administrator, about the attack

Trojan Horse	A computer program that appears to have a useful function but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program
UPS	Uninterruptible Power Source
USENET	An e-mail-based discussion system, originally supported by dial-up connections, now usually accessed via TCP/IP
VAN	Value-Added Network
VIN	Vehicle Identification Number
Virtual Private Network (VPN)	A collection of technologies that creates secure connections via nonsecure networks (such as the Internet)
Virus	A small program that inserts itself into another program when executed and generally produces a detrimental result
Vulnerability	A weakness in system security procedures, hardware, design, implementation, internal controls, technical controls, physical controls, or other controls that could be accidentally triggered or intentionally exploited and result in a violation of the system's security policy
WAN	Wide Area Network
War Dialer	A simple database and an automated modem script that dials every phone number in a group designated by the user. After it successfully connects with a modem tone, the war dialer will record the phone number in a database. The hacker can then review the database and select a likely target for a hack attempt.

Wireless Access Protocol (WAP)

A specification for a set of communication protocols to standardize the way that wireless devices, such as cellular telephones and radio transceivers, can be used for Internet access, including e-mail, the World Wide Web, newsgroups, and Internet Relay Chat (IRC). For more information on the following terms, see the links provided.

Protocol:
<http://searchNetworking.techtarget.com/sDefinition/0,,sid7_gci212839,00.html>

Wireless:
<http://searchNetworking.techtarget.com/sDefinition/0,,sid7_gci213380,00.html>

Internet Relay Chat:
<http://searchWin2000.techtarget.com/sDefinition/0,,sid1_gci214040,00.html>

Worm

A program that copies itself from system to system via the network

XML

Extensible Markup Language

Zeroization

A method of erasing electronically stored data by altering the contents of the data storage in order to prevent the recovery of the data

Appendix B: Bibliography

- Allen, Julia & Stoner, Ed. *Detecting Signs of Intrusion*. (CMU/SEI-SIM-009). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2000, <http://www.cert.org/security-improvement/modules/m09.html>.

- *The Biometric Consortium* <http://www.biometrics.org/html/standards.html>.

- *Biometrics Standards and Current Standard-Related Activities*, The Biometrics Resource Center Web site, National Institute of Standards and Technology, <http://www.itl.nist.gov/div895/biometrics/standards.html>.

- *Center for Internet Security (CIS)*, Hershey, PA, <http://www.cisecurity.org/>.

- *CERT® Coordination Center (CERT/CC)*, Carnegie Mellon Software Engineering Institute, <http://www.cert.org>.

- *The Computer Security Act of 1987*, Title 40, Section 1441, Responsibilities Regarding Efficiency, Security, and Privacy of Federal Computer Systems, <http://uscode.house.gov/usc.htm>.

- *Computer Security Resource Center (CSRC)*, National Institute of Standards and Technology (NIST), Computer Security Division (CSD), compilation of computer- related security best practices, <http://csrc.nist.gov/>.

- *Confidential Information*, United States Code, Title XI, Rule 81: Papers Filed Conformity, Section (h), <http://www4.law.cornell.edu/uscode/28/appendix-rule81PapersFiled Conformity.html>.

- *Criminal Justice Information Systems*, U.S. Code of Federal Regulations (CFR), 28 CFR 20.1, Judiciary and Judicial Procedure, U.S. Department of Justice.

- *Data Encryption Standard* (DES) was, until recently, used by the United States government for protecting sensitive but unclassified data. This standard has since been superseded by Triple DES due to increases in computer power which have allowed DES encryption to be broken. Advanced Encryption Standard (AES) has now become recognized by NIST CSD CSRC and has been officially approved for use by the United States government under Federal Information Processing Standard (FIPS) 197.

- *Data Security and Classification Guidelines*, Section IX: Data and Computing Policy Guidelines, The University of Massachusetts, <http://www.umassp.edu/policy/data/itcdatasec.html>.

- *Directive 96/46/EC on Data Protection* (the Directive), European Union (EU), <http://www.privacyinternational.org/agreements.html>.

- *Domestic Disaster Recovery Plan for PCs, OIS, and Small VS Systems*, National Institute of Standards and Technology (NIST), Gaithersburg, MD, U.S. Department of State, Washington, DC, National Technical Information Service (NTIS), U.S. Department of Commerce, <http://www.ntis.gov/search/product.asp?ABBR=PB90265240&starDB=GRAHIST>.

- *The Electronic Communications Privacy Act of 1986 (ECPA),* United States Code, Title 18, Part 1, Chapter 119, Section 2511: Interception and disclosure of wire, oral, or electronic communications prohibited <http://www4.law.cornell.edu/uscode/18/2511.html>.

- Engineering Principles for Information Technology Security (A Base Line for Achieving Security), NIST Special Publication 800-27, June 2001, <http://csrc.nist.gov/publications/nistpubs/800-27/sp800-27.pdf>.

- *Evaluation Assurance Level 4 (EAL4), Common Criteria for Information Technology Security Evaluation (CCITSE)*, The Trust Technology Assessment Program (TTAP), National Security Agency (NSA) and National Institute of Standards and Technology (NIST), Radium Customer Information Provider. EALs provide a uniformly increasing scale which balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. There are seven hierarchically ordered EALs. The higher the EAL, the greater the degree of assurance. <http://www.radium.ncsc.mil/tpep/process/faq-sect3.html>.

- *Federal Agency Security Practices*, National Institute of Standards and Technology (NIST), <http://csrc.nist.gov/fasp/>.

- *Federal Information Security Management Act of 2002 (FISMA),* Public Law 107-347, December 17, 2002.

- Ford, Gary, et al. *Securing Network Servers*. (CMU/SEI-SIM-007). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1999, <http://www.cert.org/security-improvement/modules/m10.html>.

- *The Freedom of Information Reform Act* (1986), United States Code, Title 5, Part I, Chapter 5, Subchapter II, Section 552: Public information; agency rules, opinions, orders, records, and proceedings, <http://www4.law.cornell.edu/uscode/5/552.html>.

- *F-Secure, Symantec, and McAfee* (antivirus software providers), <http://www.fsecure.com>; <http://www.symantec.com>; <http://www.mcafee.com>.

- *Generally Accepted System Security Principles (GASSP)* as defined by the International Information Security Foundation, <http://web.mit.edu/security/www/GASSP/gassp11.html>.

- *Global Security Working Group* (authentication policy samples), Global Justice Information Sharing Initiative, <http://www.it.ojp.gov/topic.jsp?topic_id=58>.

- *Government Information Technology Agency* (sample working, multiagency program, with Central Response Team membership application), <http://gita.state.az.us/policies_procedures/p800_s855_incident_resp.htm>.

- *Guide for the Security Certification and Accreditation of Federal Information Systems*, NIST Special Publication 800-37, June 2003 (second public draft), <http://csrs.nist.gov/sec-cert/>.

- *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* Organization for Economic Cooperation and Development (OECD), <http://oecdpublications.gfi-nb.com/cgi-bin/OECDBookShop.storefront/EN/product/932002011P1>.

- *Health Insurance Portability and Accountability Act (HIPAA) of 1996*, Centers for Medicare and Medicaid Services, <http://www.cms.gov/hipaa/>.

- *Health Insurance Portability and Accountability Act (HIPAA) of 1996*, Fact Sheet, Administrative Simplification Under HIPAA: National Standards for Transactions, Security, and Privacy, U.S. Department of Health and Human Services, <http://www.hhs.gov/news/press/2002pres/hipaa.html>.

- *IEEE/EIA STD 12207*. Software Lifecycle Processes, <http://standards.ieee.org/reading/ieee/std_public/description/se/12207.0-1996_desc.html>, <http://standards.ieee.org/reading/ieee/std_public/description/se/12207.1-1997_desc.html>, and <http://standards.ieee.org/reading/ieee/std_public/description/se/12207.2-1997_desc.html>.

- *Industry Working Group (IWG)*, Integrated Justice Information Systems (IJIS), <http://www.ijis.org>.

- *Information Technology Security Training Requirements: A Role and Performance-Based Model*, NIST Special Publication 800-16, April 1998, <http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf>.

- The Internet Engineering Task Force, four documents under current review:
  - *Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML) Document Type Definition*, David Curry, Hervé Debar, 31-Jan-03.
  - *The Intrusion Detection Exchange Protocol (IDXP),* Benjamin Feinstein, Gregory Matthews, John White, 23-Oct-02.
  - *The TUNNEL Profile*, Darren New, 06-Dec-02.
  - *Intrusion Detection Message Exchange Requirements*, Mark Wood, Michael Erlinger, 23-Oct-02, <www.ietf.org/ids.by.wg/idwg.html>.

- *Internet Storm Center,* (DID) Systems, <http://www.incidents.org/isw/iswp.php>.

- *IP Security Protocol (IPsec),* Internet Engineering Task Force (IETF), <http://www.ietf.org/html.charters/ipsec-charter.html>.

- *The ISO 17799 Service and Software Directory*. ISO 17799 is a comprehensive set of controls comprising best practices in information security. It is essentially an internationally recognized generic information security standard, International Organization for Standardization, <http://www.iso17799software.com/>.

- *Justice Information Privacy Guideline - Developing, Drafting, and Assessing Privacy Policy for Justice Information Systems,* National Criminal Justice Association, September 2002, <http://www.ncja.org/publications.html#>.

- Kossakowski, Klaus-Peter, et al. *Responding to Intrusions*. (CMU/SEI-SIM-006). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1999, <http://www.cert.org/security-improvement/modules/m06.html>.

- *Lightweight Directory Access Protocol (LDAP),* The Internet Engineering Task Force, Network Working Group, <http://www.ietf.org/rfc/rfc1777.txt>.

- *MIT Business Continuity Plan,* Massachusetts Institute of Technology (MIT), 1995, <http://web.mit.edu/security/www/pubplan.htm>.

- *MIT Emergency Response System*, Massachusetts Institute of Technology (MIT), <http://web.mit.edu/emergency/ers/index.html>.

- *National Association of State Chief Information Officers (NASCIO)*, Lexington, KY, <http://www.nascio.org>.

- *Omnibus Crime Control and Safe Streets Act of 1968*, Pub. L. No. 90-351, 82 Stat. 197, 1968 U.S.C.C.A.N. 237, as amended.

- *Personnel Security Standard*, Treasury Board of Canada, <http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/CHAPT2-4_e.asp>.

- *Preservation and Exchange of Identification Records and Information*, U.S. Code of Federal Regulations, Title 28, Part II, Chapter 33, Sec. 534, Judiciary and Judicial Procedure, U.S. Department of Justice, Federal Bureau of Investigation, Acquisition, <http://www.access.gpo.gov/uscode/uscmain.html>.

- *Privacy Act of 1974,* United States Code, Title 5, Part 1, Chapter 5, Subchapter 11, Section 552a, <http://www.4.law.cornell.edu./uscode/5/pich5schll.html>.

- *Recommendation for Electronic Authentication*, NIST Special Publication 800-63, <http://fasp.nist.gov/publications/drafts.html#draft-sp80063>.

- *Safe Harbor Act*, U.S. Department of Commerce, Export Portal, <http://www.export.gov/safeharbor/>.

- *Sample Operating Policies and Procedures*, Institute for Intergovernmental Research (IIR), <http://www.iir.com/28cfr/sample_operating_Policies_procedures.htm>.

- *The SANS Security Policy Project*, The SANS Institute <http://www.sans.org/resources/policies/>.

- *Security Assertion Markup Language (SAML),* Organization for the Advancement of Structured Information Standards (OASIS), Security Services Technical Committee, <http://www.oasis-open.org/committees/security/>.

- *Security Classification of Information*, Classification Levels, Chapter 7, Vol. 2. Principles for Classification of Information, Oak Ridge National Laboratory, U.S. Department of Energy, Department of Energy Federation of American Scientists Web site, <http://www.fas.org/sgp/library/quist2/chap_7.html>.

- *Secure Hash Standard*, Federal Information Processing Standard Publication 180-1, 1995 April 17, <http://www.itl.nist.gov/fipspubs/fip180-1.htm>.

- *Summary of the Intrusion Detection and Isolation Protocol (IDIP) Project*, Intrusion Detection and Isolation Protocol, University of California, Davis, <http://seclab.cs.ucdavis.edu/projects/idip.html>.

- Swanson, Marianne. *Security Self-Assessment Guide for Information Technology Systems*, National Institute of Standards and Technology, Publication 800-26, <http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf>.

- *Underlying Technical Models for Information Security*, Stoneburner, G., NIST Special Publication 800-33. December 2001, <http://csrc.nist.gov/>.

- *Washington State Information Technology Security Policy Audit Standards*, Washington State Auditor's Office, September 2001, <http://www.sao.wa.gov/StateGovernment/ITSecurity/ITStandards.htm>.

- *Washington State Privacy Policy*, Access Washington, Department of Information Services, <http://www.wa.gov/dis/aboutdis/pdpnotice.htm>.

- *<http://www.leo.gov/lesig/cjis/cjis_pub/information/poly2002_feb/POLY2002_Feb.htm>.
  *Note: Only LEO members may access the www.leo.gov Web site.

Note: Those who are interested in computer and information systems security are encouraged to consult the Web site of the National Institute for Standards and Technology (NIST) at <http://csrc.nist.gov/index.html>. At this site, the Computer Security Resource Center (CSRC) at NIST offers a series of publications on security terminology, issues, and policies for justice information specialists to use as guidance.