

## SAWS INFORMATION SECURITY WORKGROUP

# SAWS INFORMATION SECURITY GUIDELINES

Revised: July 14, 1999

### Background

The SAWS Data Tracking Workgroup established the SAWS Information Security Workgroup (SAWS ISWG) to define and resolve issues related to security and confidentiality. This Workgroup was charged with developing the SAWS Information Security Guidelines. In the development of these Guidelines, it was recognized that there should be an appropriate balance between security needs and business needs. The SAWS ISWG consists of State, SAWS consortia, county, and consultant participants (see Attachment A).

The Statewide Automated Welfare System (SAWS) Data Tracking Workgroup recognized the need to address issues related to the security of the SAWS system. While networked systems allow organizations to efficiently meet their business needs, they also permit security vulnerabilities (system penetrations, viruses, etc.) to be easily shared across the network from user to user. Accordingly, it was agreed that appropriate information security guidelines should be developed to protect the confidentiality, integrity and availability of the information on the SAWS system in a cost-effective manner.

The following recommendations were identified as being essential to the security of the SAWS data:

### Recommendation Number 1:

*To adequately protect the security of the SAWS system and other connected systems, the SAWS ISWG recommends that State and county entities develop information security policies and procedures for their respective users. The SAWS Information Security Guidelines may be used in the development of these policies and procedures.* The Guidelines were developed as a base point from which comprehensive security policies and procedures can be developed. The variations in user sites will be a factor in the development of security policies and procedures. It should be noted that implementation of the Guidelines is voluntary and *not* mandatory; however, inadequate security at any level increases liability and places all connected systems and the information on these systems at risk for unauthorized access, modification, destruction or disclosure.

To assist organizations in the development of information security policies and procedures, samples of various State and county information security policies, procedures and guidelines are attached (see Attachment B). Information security references are also included (see Attachment C).

### **Recommendation Number 2:**

*The SAWS ISWG recommends that information security awareness training be provided for all levels of users.*

### **Recommendation Number 3:**

*The SAWS ISWG recommends that each SAWS Consortium designate an individual to act as the Information Security Officer (ISO). In addition, the ISO shall act as a point of contact for information security issues between the consortia, the counties and SAWS entities.* It should be noted that the ISO responsibilities may be assigned to an existing position. It need *not* be a new position. The ISO should be of a sufficiently high-level classification to execute his or her responsibilities in an effective and independent manner.

### **Scope**

It is recommended that all users of SAWS and other connected systems consider these Guidelines as a resource for the development of security policies and procedures. Users are defined as State and county employees and non-employees (contract employees and volunteers). This includes persons working in *any* location, including off-site work and work conducted at home.

### **SAWS Information Security Guidelines**

- I. Security Roles and Responsibilities** (identification of information security roles and responsibilities for personnel (employees, contractors, volunteers) within your organization)
  - a) Roles and responsibilities should be specific to function and/or classification of personnel and may include the following, as appropriate for your organization:
    1. Employees (general responsibilities)
    2. Managers/Supervisors
    3. Executive Management
    4. Information Security Officers
    5. Physical Security Officers
    6. System Administrators
    7. Technical Support Staff

8. Security Staff
9. Liaison Between Organizations
10. Public Information Officers
11. Public Response Staff
12. Backup Responsibilities

**II. Internet/Intranet** (The internet is a global network connecting millions of users whereas an intranet is a network that typically belongs to and is accessed by an organization.)

- a) Appropriate use and misuse
  1. Liability for misuse
- b) Web access (who obtains access and when)
- c) Virus prevention
- d) Firewall protection/proxy server (a server whose sole function is protecting the internal network from unauthorized intrusion)
- e) Downloading/uploading data and software
- f) E-mail use
- g) Video-mail (v-mail) use
- h) Data encryption (to minimize the risk when transmitting confidential SAWS data, encrypt when possible)
- i) Blocking/filtering sites
- j) Permissions/privileges

**III. System and Application Access Control/Authorization** (Access controls are the basic controls across applications, networks and systems. They determine if a task or user has the authority to access a computing resource, including networks, systems, applications and information. Authorization provides control for some level(s) of user permissions to access computing resources. Authorization allows for the approval and verification of a user's ability to perform a function.)

- a) Authorized/unauthorized access
  1. Liability for unauthorized access
- b) Documentation of requests for access (authorizations, changes, and/or terminations) and denials of access
  1. Develop access profiles (privileges/permissions for each user)
  2. Obtain signatures
  3. Immediately process terminations of system access

- c) Password issuance/resets
  - 1. Minimum frequency for changing passwords
  - 2. Maximum number of attempts before lockout
  - 3. Establish maximum limit on stored passwords (i.e., the system shall not allow the user to re-use a password until a minimum number of different passwords have been used)
  - 4. Authenticate identity of requestor for password resets
- d) Privileges/permissions (access profiles)
  - 1. Limit access privileges/permissions to a “need to know” basis
  - 2. Identify privileges/permissions by level of access (read, add, modify, delete)
- e) Adequate separation of duties

**IV. Data Sharing (controls to appropriately limit the sharing of data elements among different entities)**

- a) Authorized/unauthorized data sharing
  - 1. Limit data sharing to organizations/individuals that:
    - have an authorized business need.
    - have entered into a contractual agreement.
    - are legally authorized to receive the data.
- b) Data warehousing (a collection of data designed to support management decision making e.g., a centralized database that is accessed by multiple organizations would be data that is warehoused).

**V. Information Security (measures to protect and preserve the confidentiality, integrity, and availability of an organization’s information)**

- a) Care and storage procedures for confidential and sensitive system data
- b) Destruction procedures for confidential and sensitive materials (when salvaging out equipment, sending out equipment for repair, etc.)
- c) Confirmation of the identity of any individuals requesting confidential or sensitive data (over the counter, over the telephone, etc.)
- d) Disclosure procedures (e.g., disclosure permitted only if authorized by statute, regulations or policies)
- e) User log off procedures (e.g., log off from all networked systems that contain confidential or sensitive information whenever users leave their work area for an extended period of time)
- f) Automatic system log-off configuration (configure the system to terminate user’s

session after a specified period of inactivity)

- g) Precautions for sending confidential and sensitive information (ensure that e-mail addresses and fax numbers are correct prior to sending confidential and sensitive information)

**VI. Physical And Environmental Security** (measures to ensure that the physical environment contributes to the security of an organization's information)

- a) Building security controls (guards, locks, cameras, etc.)
- b) Building access controls (procedures for: (1) obtaining/returning keys, (2) obtaining/terminating building access cards, (3) obtaining and returning badges and (4) recording guest/visitor access)
- c) Environmental control systems (heating/cooling systems should function appropriately to ensure protection of information assets)
- d) Fire protection and suppression systems
- e) Separation of work areas (staff performing unrelated functions should be located in different physical areas, if feasible, to protect information)
- f) Access controls to the work site by the public and other persons not directly employed by the organization (balance the need to adequately serve customers with the need to protect information from unauthorized access, modification or destruction)

**VII. Personal Computer (PC) Security** (measures to protect the security of data stored on a PC or accessed via a PC)

- a) Use of personal computing equipment only for job-related duties
- b) Liability for misuse
- c) Authorization prior to installing software and hardware, altering PC and network configurations or connecting any computing equipment
- d) Reporting of stolen or missing equipment
- e) Installation and regular updating of anti-virus software
- f) Backup requirements and procedures for data stored on personal computers and laptops
- g) Storage of laptops in a secure area (e.g., in office, while traveling, etc.)
- h) Encryption of confidential and sensitive information
- i) Password protected screensavers (activation within a specified number of minutes)

**VIII. Auditing Controls And Trails** (measures to prevent and/or identify potential or actual vulnerabilities to an organization's systems)

- a) Track access by user, date, time, terminal, transaction, field, and case (to identify intrusions and assess system vulnerabilities)
- b) Track password resets
- c) Track invalid logon attempts, overwrites, purges, etc.
- d) General ad-hoc and automated reports
- e) Periodic audits
- f) Maintain separation of duties
- g) Fraud prevention indicators (flags for determining when potential fraud has occurred)

**IX. Identification and Authentication** (the process of identifying an individual, and verifying the individual's authorization for access to a computer system, usually by using both a user identifier and password)

- a) Develop secure passwords
  - 1. PC passwords (screen saver and power-on passwords)
  - 2. network passwords
  - 3. system passwords
  - 4. application passwords, where appropriate
  - 5. avoid duplication of passwords
- b) User identification should be independent of the operating system
- c) Callback (The user at a remote site uses a modem to dial-in to the system, connects with the system, identifies itself and then hangs up. The system then calls the modem after confirming that access through that modem is appropriate.)
- d) Router address verification
- e) Create unique ids (one id per user)
- f) Identify devices by names (to indicate that they are devices and not individuals)
- g) Use of digital certificates (digital certificates are used to verify a user's identification when encrypted files are shared)
- h) Secure cards for remote access
- i) Use of biometrics

**X. Information Security Incidents** (any event, intentional or unintentional, that causes the unauthorized access, modification, destruction, or disclosure of an organization's information. Incidents typically involve viruses, thefts, misuse, destruction, or intrusions.)

- a) Recognition (e.g., viruses, thefts, misuse, destruction, intrusions, etc.)
- b) Response
- c) Reporting (ad hoc reports)
- d) Investigations
- e) Security alerts (distribute to users)
- f) Prevention (i.e., monitoring, maintenance, and training)

**XI. Network Security** (measures to protect an organization's networking system from unauthorized access either within or outside of the organization)

- a) Identify roles and responsibilities related to the following:
  - 1. Firewall protections/proxy server
  - 2. Penetration testing/intrusion detection
  - 3. Remote access security (include documentation of users that have remote access)

**XII. System Change Management** (measures to ensure a complete and comprehensive audit trail of changes made to systems and their affects)

- a) Consider security requirements prior to initiating system modifications
- b) Documentation of application changes
- c) Installation of software
- d) County-level operational changes
- e) Configuration management
- f) Permanent copies of all builds (linked code)

**XIII. Risk Assessment** (a comprehensive evaluation of an organization's security posture related to information assets to identify vulnerabilities and identify cost-effective safeguard recommendations to mitigate risks associated with the vulnerabilities. Areas to be assessed would include software and data security, telecommunications security, personnel security, etc.)

- a) Conduct regular risk assessments of automated systems to identify vulnerabilities and safeguard recommendations to address those vulnerabilities. Risk assessments should be conducted biennially and whenever a significant change to a system is

made. The following criteria should be considered:

1. Criticality of system information
2. Probability that the vulnerabilities pose a threat
3. Cost-effectiveness of safeguard recommendations
4. Time frame for implementation of safeguard recommendations
5. Feasibility of implementation of safeguard recommendations
6. Prevention of physical or electronic intrusion by hackers or employees

**XIV. Penetration Testing** (tests conducted to identify network and system vulnerabilities for the risk analysis process)

- a) Testing within each entity (county, State, consortia, and interfacing systems)
- b) Due diligence (in implementation of recommended corrective actions)
- c) Independently conducted by a reputable organization
- d) Regularly conducted

**XV. Disaster Recovery Plan** (a plan developed to assist an organization in immediately responding to a disaster)

- a) Resources required (personnel, facilities, equipment, etc.)
- b) Priority/criticality of systems
- c) Levels of response and recovery
- d) Develop written backup schedules
- e) Updating the backup schedules
- f) Testing of completed backups
- g) Contact lists (individuals to be contacted following a disaster)
- h) Responsibility of personnel
- i) Contingency plans (a plan for emergency response, backup operations, and post-disaster recovery that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation)

**XVI. Business Continuity Plan** (a plan developed to assist an organization in continuing operations and resuming normal business operations following a disaster)

- a) Resources required (personnel, facilities, equipment, etc.)
- b) Documentation of infrastructure (inventory of current environment)

- c) Priority/criticality of business functions
- d) Operational impact analyses (analysis of the impact each disaster would have upon the operations of an organization)
- e) Responsibilities of personnel

**XVII. Termination and Transfer Procedures** (controls to ensure that an organization's equipment and materials are appropriately returned, and that physical and system access is appropriately terminated when employees terminate employment or transfer to another organization)

- a) Return of equipment, materials, key cards, keys, software, etc.
- b) Changing locks (for terminated employees that pose a threat)
- c) Immediately process terminations of system access (for employees that terminate employment)
  - 1. ID deletion after termination

**XVIII. E-Mail** (measures to protect the transmission of messages over any communication networks)

- a) Appropriate/inappropriate use
- b) Liability for misuse
- c) E-mail retention
- d) Message content guidelines
- e) Guidelines for sending/forwarding messages with confidential information
- f) Encryption
- g) Appropriate addressing
- h) Chain letters

**XIX. Information Security Policies, Procedures and Guidelines.** Attachment B includes a variety of policies, procedures and guidelines related to information security.

**XX. Information Security References.** Attachment C includes a variety of reference materials related to information security. **Note:** These references are presented without necessarily endorsing their content nor guaranteeing the accuracy of any information presented.

## Attachment A

### SAWS Information Security Workgroup Participants

<b>Name</b>	<b>Title</b>	<b>Organization</b>	<b>Entity</b>
Alexander, Diane	Business Analyst	SAWS TA	California Systems Consultant
Barr, Walt	Information Security Officer	Department of Health Services	State of California
Carr, Anna	Manager, Information Security Group	Department of Social Services	State of California
Christensen, Lori	Associate Governmental Program Analyst	Department of Social Services	State of California
Cox, David	Senior Security Administrator	SSA Information Systems Technology Branch	Orange County
Garcia, Daniel	Central Security Officer	Los Angeles County and LEADER	Los Angeles County
Hayes, Louise	Internal Security Officer	DPSS Human Resources	Riverside County
Hwu, Charles	Manager	SAWS TA - HWDC	CalServ
Jordan, Sherland	Information Security Officer	Department of Social Services	State of California
Khylyn, Rose	Security Consultant	Department of Social Services	State of California
Martinez, Peter	Program Specialist I	San Bernardino Social Services Group	San Bernardino County
Neitzel, Laura	Business Analyst	SAWS TA	California Systems Consultant
Obernesser, Bill	Independent Verification & Validation (IV&V) Consultant	SAWS - Consortia Strategy	Carrera Consulting
Reynolds, Patricia	SAWS Project Manager	DPSS Internal Review Branch	Riverside County
Rogers, Julie	ISAWS Consortia Manager	ISAWS	SAWS Consortia
Salmonsens, Carl	Information Security Officer	Health and Welfare Data Center	State of California
Swedlow, Jim	Deputy Director	LEADER	Los Angeles County
Tahara, Derrick	Data Security Administrator	SSA Information Systems Technology Branch	Orange County
Young, Beverly	Associate Governmental Program Analyst	Department of Social Services	State of California
Zuehlke, Carla	Information Systems Specialist	ISAWS Maintenance - HWDC	State of California

# **Attachment B**

## **SAWS Information Security Guidelines**

### **Table of Contents**

For questions related to the listed policies and procedures, you may contact the following:

Health and Welfare Data Center

Contact: Carl Salmonsén

Information Security Officer

(916) 739-7883

Salmonsén,Carl@HWMAIL

Riverside County

Contact: Louise Hayes

Internal Security Officer

(909) 358-3107

lhayes@riv.ca.usa

Department of Social Services

Contact: Sherland Jordan

Information Security Officer

(916) 657-3409

sjordan@dss.ca.gov

# **Attachment B**

## **SAWS Information Security Guidelines**

### **Table of Contents**

- I. CHHS/HWDC Network Access Policy
- II. Riverside County Software Usage Policy
- III. Riverside County DPSS Logon Request (RACF)
- IV. California Department of Social Services Internet and E-Mail Usage Policy
- V. California Department of Social Services Policy for Security of Confidential and Sensitive Data
- VI. California Department of Social Services Guidelines for Protection of Confidential and Sensitive Information
- VII. California Department of Social Services Guidelines for Destruction of Confidential and Sensitive Information
- VIII. California Department of Social Services Personal Computer Security Policy
- IX. California Department of Social Services Employee Password Controls Policy
- X. California Department of Social Services System Administrator Password Controls Policy
- XI. California Department of Social Services Guidelines for Password Protection and Security
- XII. California Department of Social Services Frequently Asked Questions About Passwords
- XIII. California Department of Social Services Incident Policy
- XIV. California Department of Social Services Procedures for Incident Response and Reporting
- XV. California Department of Social Services Network Security Controls Policy
- XVI. California Department of Social Services Information Security Roles and Responsibilities Policy

# **Attachment B**

## **SAWS Information Security Guidelines**

### **Table of Contents**

- XVII. California Department of Social Services Employee Separation and Transfer Policy
- XVIII. California Department of Social Services Employee Transfer Notice
- XIX. California Department of Social Services E-Mail Retention Policy
- XX. California Department of Social Services E-Mail Retention Policy Acknowledgement Form
- XXI. California Department of Social Services Frequently Asked Questions About the E-Mail Retention Policy
- XXII. California Department of Social Services System and Application Access Policy
- XXIII. California Department of Social Services Frequently Asked Questions About the System and Application Access Form
- XXIV. California Department of Social Services System and Application Access Form
- XXV. California Department of Social Services Information Security Policies Glossary

## Attachment C

# INFORMATION SECURITY REFERENCES

The following list of references include State and federal Statues, regulations, publications and additional reading selections that may be of assistance. It should be noted that this is not a comprehensive list of all references related to information security. These references are presented without necessarily endorsing their content nor guaranteeing the accuracy of any information presented.

### FEDERAL LEGISLATION

The following references contain many of the federally mandated requirements to protect sensitive automated information systems and the data they contain.

1. *Computer Security Act of 1987* (P.L. 100-235) - Requires agencies to conduct security training, identify sensitive systems, and implement system security plans.
2. *Privacy Act* (P.L. 93-579) of 1974 - Provides for the protection and accuracy of information about individuals.
3. *Electronic Communications Privacy Act* (P.L. 99-508) - Provides for the protection of transmissions of various communications technology.
4. *Computer Fraud and Abuse Act; Counterfeit Access Device Act* (P.L. 99-474; P.L. 98-473) - Established computer-related crime as an offense with specific penalties.
5. *Federal Managers Financial Integrity Act* (P.L. 97-225) - Requires the use of internal controls to reduce fraud, waste, and abuse.
6. *Trade Secrets Act* (18 USC) - Establishes penalties for improper disclosure of trade secrets.
7. *Copyright Act of 1980* (17 USC) - Protects copyrighted computer software.
8. *Paperwork Reduction Act of 1980 & 1986* (P.L. 96-511/P.L. 99-500) - Establishes the Federal Information Resources Management (IRM) Program.
9. *Computer Matching and Privacy Protection Act* (P.L. 100-503) - Establishes procedures to ensure the accuracy of computer matching programs.

10. *45 CFR 95 Subpart F* - Requires that state systems include assurances that information in the computer systems as well as access, use, and disposal of data will be safeguarded.
11. *42 U.S.C. 654* - Requires that state systems ensure the integrity and security of data contained within its systems.
12. *Federal Copyright Act, 17 U.S.C. 101 et. seq.* - Protects “intellectual property” rights and prohibits misuse of all original works of authorship in any tangible medium of expression.
13. Office of Management and Budget (OMB) CIRCULARS AND BULLETINS
14. OMB Circular No. A-130, Appendix III, *Security of Federal Automated Information Systems*, February, 1996
15. OMB Circular No. A-123 Revised, *Internal Control Systems*, August 4, 1986
16. OMB Circular No. A-127, *Financial Management Systems*, December 19, 1984
17. OMB Bulletin No. 90-08, *Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information*, July 9, 1990

#### **OFFICE OF PERSONNEL (OPM) MANUALS AND REGULATIONS**

1. *5 CFR PART 930, Subpart C--Employees Responsible for the Management or Use of Federal Computer Systems*, January 1992
2. *Federal Personnel Manual*, Chapter 731, *Personnel Suitability*, September 29, 1988

#### **GENERAL SERVICES ADMINISTRATION (GSA) REGULATIONS AND BULLETINS**

1. *Federal Information Resources Management Regulation (FIRMR)*, Subpart 201-21.3, *Security and Privacy*, October 1990
2. *Federal Information Resources Management Regulation (FIRMR)*, Part 201-23, *Disposition*
3. FIRMR Bulletin C-19, *Information System Security (INFOSEC)*, January 30, 1991
4. FIRMR Bulletin C-28, *Computer Viruses*, November 6, 1991
5. FIRMR Bulletin C-2, *Disposition and Reuse of Federal information Processing Equipment*,

6. *Federal Property Management Regulations (FPMR)*, Subchapter H, Part 101-43, *Utilization of Personal Property*, Part 101-44, *Donation of Personal Property*, Part 101-45, *Sale, Abandonment, or Destruction of Personal Property*, and Part 101-46, *Utilization and Disposal of Personal Property Pursuant to Exchange/Sale Authority*.

**NIST: FEDERAL INFORMATION PROCESSING STANDARDS (FIPS)**

1. FIPS PUB 31, *Guidelines for Automatic Data Processing Physical Security and Risk Management*, June 1974
2. FIPS PUB 41, *Computer Security Guidelines for Implementing the Privacy Act of 1974*, May 30, 1975
3. FIPS PUB 46-2, *Data Encryption Standard (DES)*, December 30, 1993 (Reaffirmed until 1998)
4. FIPS PUB 48, *Guidelines on Evaluation of Techniques for Automated Personnel Identification*, April 1, 1977
5. FIPS PUB 65, *Guideline for Automatic Data Processing Risk Analysis*, August 1, 1979
6. FIPS PUB 73, *Guidelines for Security of Computer Applications*, June 30, 1980
7. FIPS PUB 74, *Guidelines for Implementing and Using the NBS Data Encryption Standard*, April 1, 1981
8. FIPS PUB 81, *DES Modes of Operation*, December 2, 1980
9. FIPS PUB 83, *Guideline on User Authentication Techniques for Computer Network Access Control*, September 29, 1980
10. FIPS PUB 87, *Guidelines for ADP Contingency Planning*, March 27, 1981
11. FIPS PUB 88, *Guideline on Integrity Assurance and Control in Database Administration*, August 14, 1981
12. FIPS PUB 102, *Guideline for Computer Security Certification and Accreditation*, September 27, 1983
13. FIPS PUB 112, *Standard on Password Usage*, May 30, 1985
14. FIPS PUB 113, *Standard on Computer Data Authentication*, May 30, 1985
15. FIPS PUB 140-1, *Security Requirements for Cryptographic Modules*, January 11, 1994
16. FIPS PUB 171, *Key Management Using ANSI X.9.17*, April 27, 1992
17. FIPS PUB 180, *Secure Hash Standards (SHS)*, May 11, 1993

18. FIPS PUB 181, *Automated Password Generator*, October 5, 1993
19. FIPS PUB 185, *Escrowed Encryption Standard (EES)*, February 9, 1994
20. FIPS PUB 186, *Digital Signature Standard (DSS)*, May 19, 1994
21. FIPS PUB 191, *Specifications for Guidelines for the Analysis Local Area Network Security*, November 9, 1994

#### **NIST: SPECIAL PUBLICATIONS (SPEC PUBS) AND OTHER REPORTS**

1. NIST SPEC PUB 500-74, *Guide for Selecting Automated Risk Analysis Tools*, October 1989
2. NBS SPEC PUB 500-120, *Security of Personal Computer Systems: A Management Guide*, January 1985
3. NBS SPEC PUB 500-137, *Security for Dial-Up Lines*, May 1986
4. NBS SPEC PUB 500-153, *Guide to Auditing for Controls and Security: A System Development Life Cycle Approach*, April 1988
3. NBS SPEC PUB 500-156, *Message Authentication Code (MAC) Validation System: Requirements and Procedures*, May 1988
6. NIST SPEC PUB 500-157, *Smart Card Technology: New Methods for Computer Access Control*, September 1988
7. NIST SPEC PUB 500-160, *Report of the Invitational Workshop on Integrity Policy in Computer Information Systems*, January 1989
8. NIST SPEC PUB 500-166, *Computer Viruses and Related Threats: A Management Guide*, August 1989
9. NIST SPEC PUB 500-169, *Executive Guide to the Protection of Information Resources*, October 1989
10. NIST SPEC PUB 500-170, *Management Guide to the Protection of Information*, October 1989
11. NIST SPEC PUB 500-171, *Computer User's Guide to the Protection of Information Resources*, October 1989
12. NIST SPEC PUB 500-172, *Computer Security Training Guidelines*, November 1989
13. NIST SPEC PUB 800-2, *Public-Key Cryptography*, April, 1991
14. NIST SPEC PUB 800-3, *Establishing a Computer Security Incident Response Capability (CSIRC)*, November, 1991

15. NIST SPEC PUB 800-4, *Computer Security Considerations in Federal Procurements, A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials*, March 1992
16. NISTIR 4659, *Glossary of Computer Security Terminology*, September 1991
17. NISTIR 4667, *Computer Security Bulletin Board System User's Guide*, September 1991
18. NISTIR 4749, *Sample Statements of Work for Federal Computer Security Services: For Use In-House or Contracting Out*, December 1991
19. NIST NCSL *Bulletin*, Data Encryption Standard, June 1990

#### CALIFORNIA STATE LEGISLATION

1. *Government Code Section 11770* - Requires each California State agency to notify the Department of Information Technology of all information security incidents.
2. *Government Code Section 11771* - Requires each California State agency to implement policies and standards regarding the confidentiality and security of information.
3. *California Public Records Act: Government Code Sections 6250 - 6270* - Allows individuals to obtain information about the actions of Government.
4. *Information Practices Act of 1977: Civil Code Section 1798 et seq.* - Places specific requirements on State agencies in the collection, use, maintenance, and dissemination of information relating to individuals.
5. *Penal Code Section 502* - Affords protection to individuals, businesses, and governmental agencies from tampering, interference, damage and unauthorized access to lawfully created computer data and computer systems.

#### OTHER GOVERNMENT PUBLICATIONS

1. *Model Framework for Management Control Over Automated Information Systems*, President's Council on Management Improvement and the President's Council on Integrity and Efficiency, January 1988
2. *Information Technology Installation Security*, Federal Systems Integration and Management Center (FEDSIM), GSA, December 1988
3. *California State Administrative Manual (SAM)*- Requires that all State agencies establish controls to ensure that information contained within systems is protected and to develop policies to protect these systems against unauthorized access, modification, and deletion.

4. *Information Technology Security and Risk Management Guidelines, Office of Information Technology, April 1989 (Revised 4/10/92)* - This guideline has been prepared to assist State agencies in establishing effective security and risk management programs in compliance with State policy. It is intended to provide practical advice to agency management and to the security practitioner.

## NON-GOVERNMENT PUBLICATIONS

1. Baker, Richard H., *Computer Security Handbook*, McGraw-Hill, Blue Ridge Summit, PA, 1991
2. Baker, Richard H., *Network Security: How to Plan for it and Achieve it*, McGraw-Hill, Blue Ridge Summit, PA, 1995
3. Baskerville, Richard, *Designing Information Systems Security*, John Wiley & Sons, New York, NY, 1988
4. Brazier, F.M.T., and Johanson, D., *Distributed Open Systems*, IEEE Computer Society Press, Los Almitos, CA, 1994
5. Cohen, Frederick B., *Protection and Security on the Information Superhighway*, John Wiley & Sons, New York, NY, 1995
6. *Computers at Risk*, National Research Council, National Academy Press, 1991
7. Cheswick, William R., and Bellovin, Steven M., *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison-Wesley, Reading MA, 1994
8. Curry, David A., *UNIX System Security: A Guide for Users and System Administrators*, Addison-Wesley, Reading, MA, 1992
9. Dutton, Ellen, *LAN Security Handbook*, M&T Books, New York, NY, 1994
10. Fites, Philip, and Kratz, Martin P.J., *Information Systems Security: A Practitioner's Reference*, Van Nostrand Reinhold, New York, NY, 1993
11. Garfinkel, Simson, and Spafford, Gene, *Practical Unix Security*, O'Reilly & Associates, Inc., Sebastopol, CA, 1991
12. Gahan, Chris, *LAN Security: The Business Threat from Within*, 3COM Corporation, Santa Clara, CA, 1991
13. Heywood, Drew, et al., *LAN Connectivity*, New Riders Publishing, Carmel, IN, 1992
14. Madron, Thomas, W., *Network Security in the 90s, Issues and Solutions for Managers*, John Wiley & Sons, Inc., 1992
15. Michael, Wendy, H., et al., *Fiber Distributed Data Interface: An Introduction*, Digital Press, Burlington, MA, 1993

16. Miller, Mark A., *Internetworking: A Guide to Network Communications*, M&T Books, San Mateo, CA, 1991
17. Motorola Codex, *The Basics Book of Information Networking*, Addison-Wesley, Reading, MA, 1992
18. Novell NetWare 3.12, *Concepts*, Novell Inc., Provo, UT, 1993
19. Novell NetWare 3.12, *System Administration*, Novell Inc., Provo, UT, 1993
20. Novell NetWare 3.12, *Utilities Reference*, Novell Inc., Provo, UT, 1993
21. Nowsgadi, Farshad, *Managing Netware*, Addison-Wesley, Reading, MA, 1994
22. Russell, Deborah, and Gangemi, G.T., *Computer Security Basics*, O'Reilly & Associates, Inc., Sebastopol, CA, 1991
23. Sandler, Corey, et al., *VAX Security: Protecting the System & the Data*, John Wiley & Sons, New York, NY, 1991
24. Sawicki, Ed, *LAN Desktop Guide to Security*, SAMS, Carmel, IN, 1992
25. Stallings, William, *Network and Internetwork Security, Principles and Practice*, ISBN 0-02-415483-0, Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1995
26. Stallings, William, *Networking Standards: A Guide to OSI, ISDN, LAN, and MAN Standards*, Addison-Wesley, Reading, MA, 1993
27. Stallings, William, *SNMP, SNMPv2, and CMIP: The Practical Guide to Network Management Standards*, Addison-Wesley, Reading, MA, 1993
28. Stang, David J., and Moon, Sylvia, *Network Security Secrets*, IDG Books Worldwide, Inc., San Mateo, CA, 1993
29. Steen, William, *NetWare Security*, New Riders Publishing, Indianapolis, IN, 1996
30. Stern, Hal, *Managing NFS and NIS*, O'Reilly & Associates, Inc., Sebastopol, CA, 1991