

Index

A

ABA. See American Bankers Association

Access control

- confidentiality and, 28
- copyrighted or proprietary information, 28
- definition, 28
- Orange Book and, 48
- subscription services and, 28

Accessibility and Integrity of Networked Information Collections, 6

Accreditation of systems, 50-51

Adleman, Leonard, 220

Administrative Procedures Act, 182

Advanced Research Projects Agency, 57,62,63

Advisory Council on the National Information Infrastructure

- input on national encryption policy, 172
- “Mega-Project” on privacy, security, and intellectual property, 172-173

Allen, Anita, 82,83

American Bankers Association, 47

American National Standards Institute, 47, 131, 136

American Society of Composers, Authors and Publishers, 108-109

Annual Authorization Service, 109

ANSI. See American National Standards Institute

Appendix 111 to OMB Circular A-130. See OMB Circular A-130

Arms Export Control Act, 151

ARPA. See Advanced Research Projects Agency

ASCAP. See American Society of Composers, Authors and Publishers

Association for Computing Machinery, 182

Asymmetric cryptosystems. See Public-key cryptography

AT&T Surety Telephone Device 3600,64-65

Auditing

- to prevent key misuse, 173
- of safeguard violations, 35

Australia

- data protection board, 22,95
- not included in work toward international product evaluation standard, 49

Austria

- data protection board, 22,95

Authentication, 20. See also Nonrepudiation

- authenticator, 32
- in banking, 121
- certificates, 77-78
- cryptographic keys for, 53
- cryptography and, 5-6, 35-37, 39, 53, 113, 124
- need for in electronic commerce, 20, 69, 76
- NIST activities relating to, 162
- product evaluations by Treasury Department, 48
- trusted entity role, 77-78
- U.C.C. requirements, 72-74
- using the DEA, 121

Authenticator, 32

Authorship and copyright, 104

Availability of services

- emphasis on by network providers, 28
- formal security models and, 31,32

B

Banking industry

- authentication using DEA, 121
- banks as certification authorities, 54-55,78
- emphasis on integrity and nonrepudiation, 28
- trusted third-party functions, 54-55,78
- U.C.C. and electronic funds transfers, 73
- use of DES-based encryption technology, 121, 131

Bell-LaPadula security model, 31

Berman, Jerry, 175-176, 180-181

Biham, Eli, 123

Biometric devices, 37

BMI. See Broadcast Music Inc.

Bok, Sissela, 83

Brandeis, Louis, 79,82

Brennan, William, 79

Brickell, Ernest, 118

Broadcast Music Inc., 108, 109

Brooks, Clinton, 14-15, 159, 169

Brooks, Rep, Jack, 122

Brooks Act of 1965, 121, 132, 133, 134-136

BSA. See Business Software Alliance

- Buckley Amendment, 80
- Bureau of Export Administration, 153
- Bureau of the Census, 133
- Business Software Alliance, 157
- C**
- Cable companies
 - emphasis on availability of services, 28
 - telephone and Internet services, 4
- CAIVRS. See Credit Alert Interactive Voice Response System
- Canada
 - data protection board, 22,95
 - role in developing an international product evaluation standard, 49
 - role in developing Generally Accepted System Security Principles, 51
 - role in developing information security certification, 52
- Canadian Information Processing Society
 - role in developing information security certification, 52
- Canadian Trusted Computer Product Evaluation Criteria, 49
- Cantwell, Rep. Maria, 12, 16, 160, 172
- Capstone chip, 65, 127, 167, 173, 174,216
- Carnegie Mellon University, 57
- CAS. See Certification authorities
- CCC. See Copyright Clearance Center
- CCITT. See Comité Consultatif Internationale de Télégraphique et Téléphonique
- CCL. See Commerce Control List
- Cellular phones, 154
- Cerf, Vinton, 41
- CERT. See Computer Emergency Response Team
- Certificates
 - authentication, 77-78, 162
 - in electronic key exchange, 53, 54
- Certification
 - of security professionals, 52
 - of systems, 50-51
- Certification authorities, 16,53-54,55-56,77, 162, 178. See *also* Trusted entity
- Challenge-response systems, 32
- Chemistry On-line Retrieval Experiment, 96-97
- China
 - export controls, 155
- Ciphertext
 - definition, 113
- Clark-Wilson security model, 31
- Clearinghouses for crisis response. See Emergency response
- Cleartext
 - definition, 113
- CLEF program. See Commercially-Licensed Evaluation Facilities program
- Clinton Administration
 - adoption of EES as voluntary standard, 10, 15, 17-18, 117-119, 173-174, 179
 - cost estimates for escrow system, 118, 163
 - encryption policy review, 119
 - escrowed-encryption initiative, 5, 17, 39,67, 161-163, 173-174, 176-177, 179-182
 - implementation of cryptography policy, 171-174
 - “Key Escrow Encryption Workshop,” 15-16, 172
 - liberalization of export controls, 155, 159-160
 - National Information Infrastructure program, 62-63
 - National Performance Review, 51,62,63
 - supports NIST’s efforts in GSSPS, 51
 - willingness to explore alternatives to key-escrow encryption, 11, 131, 172
 - Working Group on Encryption and Telecommunications, 171-172
- Clipper chip. See Escrowed Encryption Standard
- CNRI. See Corporation for National Research Initiatives
- COCOM. See Coordinating Committee for Multilateral Export Controls
- Code of Practice for Information Security Management, 51
- Colossus computing machines, 112
- Comité Consultatif Internationale de Télégraphique et Téléphonique, 47
- Commerce Control List
 - Commerce Department controls compared with State Department controls, 153-154
 - cryptography on, 153-154, 156
 - purpose, 153
- Commerce Department. See Department of Commerce
- Commerce-Net prototype, 54
- Commercially-Licensed Evaluation Facilities program, 49
- “Commercially reasonable” security measures, 73
- Committee on Government Operations, 147-148
- Common Information Technology Security Criteria, 49
- Competitiveness
 - EES standard and, 118, 181-182
 - export controls and, 154-160, 181
 - Green Book on, 92
 - tension between national security and competitiveness, 128
- Compuserve, 28
- Computer conferences, 98
- Computer Emergency Response Team, 3,57
- Computer Ethics Institute, 59

- Computer Incident Advisory Capability, 57
- Computer Matching Act, 84
- Computer Professionals for Social Responsibility, 219-220
- Computer programs copyright, 100
- Computer records admissibility, 74-76
- Computer Security Act of 1987
 - background, 139-145
 - cost-effectiveness requirement, 219
 - federal agency responsibilities under, 145-150
 - implementation of, 8, 13-16, 20, 114, 132, 133-134, 149-150, 164-171
 - legislative history, 140-142
 - purpose, 8, 138-139
 - significance of, 8, 133, 138-139
 - text of, 190-196
- Computer Security Division. *See also* National Institute of Standards and Technology
 - activities related to computer and information security, 162-163
 - authentication-related activities, 162
- Computer Security Institute
 - role in developing information security certification, 52
- Computer System Security and Privacy Advisory Board
 - call for a broad review of cryptography policy, 176-177, 218-219
 - endorses NRC study of national cryptography policy, 177, 218, 220
 - establishment of, 13, 139, 148
 - purpose of, 148
 - questions cost of DSS under PKP licensing arrangement, 221
 - role in encryption policy review, 172
- Computer Systems Laboratory, 136, 161, 164
- Computers, Health Records and Citizens Rights*, 83
- Computers and the Rights of Citizens*, 80-81
- Confidentiality
 - cryptography and, 5-6, 35-37, 39, 113
 - definition, 28, 82-83
 - distinguished from privacy, 28, 82-83
 - Orange Book and, 48
- Congress
 - policy issues and options, 18-23, 85, 95, 105-106, 108, 110; 174-183
 - response to escrowed-encryption initiatives, 17-18, 179-182
 - review of cryptography policy, 16-17, 177-179
 - role in defining objectives and organizational security policy, 27
 - strategic and tactical roles, 174-183
- Congressional Budget Office, 179
- Congressional Research Service, 180
- Contracts, 71-74. *See also* Electronic commerce
- Convention of the Council of Europe for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 88
- Coordinating Committee for Multilateral Export Controls, 154, 155
- Copyright. *See also* Royalties
 - authorship and compilations, 104
 - computer programs, 100
 - copyright collectives, 108-110
 - cryptography and access controls for protection, 28
 - defining a work, 98
 - digital libraries and, 22-23, 98-104, 105
 - electronic information, 4, 6, 23
 - fair use, 102-103, 105-106
 - first-sale doctrine, 104, 105, 107
 - history of U.S. copyright law, 99-100
 - multimedia works, 23, 97, 106-108
 - OTA's 1992 study of software and intellectual property, 97-106
 - policy options, 23, 97, 105-106, 108, 110
 - purpose of, 99
 - rights under U.S. law, 99-101
 - unauthorized copying, 105
- Copyright Act, 106
- Copyright Act of 1976, 100-101, 102, 103, 104, 109
- Copyright Clearance Center, 109, 110
- Copyright collectives
 - legal issues, 108-110
- Cornell University, 96-97
- Corporation for National Research Initiatives
 - proposed electronic copyright management system, 110
- Corporations
 - cryptography and access controls, 28
- Cost-justifying safeguards, 30-31, 52, 134
- costs
 - effects of lower costs on computing, 4
- Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 90-95
- CPSR. *See* Computer Professionals for Social Responsibility
- "Crackers," *See also* Hackers
 - exaggeration of threats from, 42, 60
 - threats to networked information, 26
- Credit Alert Interactive Voice Response System, 84, 85
- Criminal and civil penalties, 8, 18, 60-61, 180-181
- CRS. *See* Congressional Research Service
- Cryptanalysts
 - definition, 112
 - differential cryptanalysts, 123
- Cryptographic algorithms. *See also* specific algorithms

- classified 181
- definition, 113
- export controls, 157
- symmetric or asymmetric, 39
- Cryptography
 - congressional policy review, 16-17
 - description, 112-113
 - history of, 112
 - how it protects information, 39
 - importance of, 115-128
 - policy issues and options, 8-23, 174-183
 - terminology, 113
- Cryptosystem**
 - definition, 113
- CSL. See Computer Systems Laboratory
- CSSPAB. See Computer System Security and Privacy Advisory Board
- D**
- Damages, 18, 180-181
- Data Encryption Algorithm, 39, 120, 121
- Data Encryption Standard
 - compared with **EES**, 118, 120
 - description, 10, 39, 121-123
 - export controls on products using, 156, 157, 158
 - history of, 120, 121, 129-130, 136
 - NIST** evaluation of products using, 48, 121
 - RSA for key exchange, 126
 - technological stability and, 129-130
 - triple encryption, 121, 122-123, 171
 - U.S. sales figures for DES hardware and software products, 130
- Data Encryption Standard Message Authentication Code, 77
- Data integrity boards, 84, 85
- Data processing
 - notification requirement of Council Directive, 93
- Data Processing Management Association, 52
- Data protection boards
 - foreign countries, 95
 - proposed responsibilities and functions, 95
- DDN. See Defense Data Network
- DEA. See Data Encryption Algorithm
- Decryption
 - definition, 113
 - real-time decryption, 119
- Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information*, 6, 136
- Defense Authorization Bill for FY 1994, 220
- Defense Communications Agency, 57
- Defense Data Network Security Coordination Center, 57
- Defense Information Systems Agency, 3
- Degaussers**
 - NSA list of, 48
- Delphi, 28
- Denmark
 - availability of DES-based products, 158
- Deming, Dorothy, 118, 126-127
- Department of Agriculture, 85
- Department of Commerce. See *also* National Institute of Standards and Technology
 - assigning of resources to **NIST**, 20, 183
 - Brooks Act requirements, 133, 135-136, 142
 - Computer Security Act requirements, 20, 137-138, 139, 148, 166, 168, 183
 - Computer System Security and Privacy Advisory Board, 13, 139
 - congressional policy option, 20, 183
 - DES issued as a **FIPS**, 121
 - DSS issued as a **FIPS**, 47, 168, 218-219, 221-222
 - EES** issued as a **FIPS**, 47, 117, 118
 - export controls, 11-12, 150, 151, 153-154
- Department of Defense. See *also* National Security Agency
 - Advanced Research Projects Agency, 57, 62, 63
 - certification and accreditation of systems, 50
 - formal security models and, 31
 - Orange Book and, 48
 - role in establishing Munitions List, 151, 155-156
 - role in federal information systems safeguards, 137-138, 143, 145, 146
 - role in NCS management, 61
 - role in standards appeal process, 166
 - security breaches, 2, 3
- Department of Education, 85
- Department of Energy, 57, 146
- Department of Health, Education, and Welfare, 80
- Department of Housing and Urban Development, 8, 5
- Department of Justice, 118, 173
- Department of State
 - export controls, 11-12, 45, 117, 150-152, 155-156, 157, 160
 - export controls compared with Commerce Department controls, 153-154
- Department of the Treasury
 - Automated Systems Division as **EES** escrow agent, 118, 173
 - evaluation of authentication products for financial transactions, 48
- Department of Veterans Affairs, 85
- DES. See Data Encryption Standard
- DES MAC. See Data Encryption Standard Message Authentication Code
- Differential cryptanalysts, 123
- Diffie**, Whitfield, 126, 170, 179-180, 220
- Diffie-Hellman** public-key technique, 54, 64

- Digital information. See *also* Information;
 Networked information
 copyright and, 98-104, 105
 differences from information in traditional forms,
 97
 trend toward, 4
- Digital libraries
 description, 96-97
 intellectual property protection, 22-23, 97-110
 legal issues, 22-23,70,96-110
 privacy, 66-68
- Digital powers of attorney, 171, 178
- Digital Signature Algorithm, 65,215-216,222
- Digital Signature Standard
 criticisms and NIST response, 167-168,222
 effect on technology control, 126, 129
 evolution of, 11, 215-222
 issuance of, 11, 47, 221-222
 NIST activities relating to, 162
 not a public key encryption algorithm, 10, 127
 patent problems, 220-221
 public-key algorithm in, 123
 resistance to, 131, 132, 176
- Digital signatures. See *also* Digital Signature
 Standard
 DES and, 121, 124
 description, 124-125
 Green Book proposals, 91,92
 limitation of, 77
 public-key cryptography and, 6, 10,39, 113, 127
 purpose of, 6,20,21,35-37,39,74, 76, 113,215
 RSA system-based products, 11, 124-125, 139
- Digital Telephony and Communications Privacy Act
 of 1994, 66
- Disaster recovery services, 43-44
- Distributed computing, 3-4,5, 134
- DOD. See Department of Defense
- Douglas, William O., 79
- DSA. See Digital Signature Algorithm
- DSS. See Digital Signature Standard
- Dual-use items export controls, 150, 151, 153, 155
- Due care approach to safeguarding information, 7,
 8,30-31,44,52
- E**
- E-mail. See Electronic mail
- EAA. See Export Administration Act
- Eastern Europe
 export control policy, 155
- EC MA. See European Computer Manufacturers
 Association
- EDI. See Electronic Data interchange
- Education/training
 computer security management training, 145, 163
 ethical principles, 59
 professional development, 52-53
- EES. See Escrowed Encryption Standard
- EFF. See Electronic Frontier Foundation
- Efficiency, 4-5,29
- Eisenstadt v. Baird*, 79
- Electric utilities
 information services, 4
- Electronic commerce
 legal issues, 20-21,69,70-78
 networked society and, 4, 6
 public-key infrastructure and, 68
 rules of evidence: data integrity and
 nonrepudiation, 74-78
 Statute of Frauds writing and signature
 requirement, 71-74
- Electronic Data Interchange, 71
- Electronic Data Interchange value-added services
 emphasis on integrity and nonrepudiation, 28
- Electronic Data Processing Auditors Association
 Control Principles, 51
 role in developing information security
 certification, 52
- Electronic Frontier Foundation, 175, 180
- Electronic mail
 copyright issues, 98
 description, 36
 Privacy-Enhanced Mail, 36-37
Electronic Record Systems and Individual Privacy,
 95
- Electronic surveillance
 cryptography and, 116, 117-118, 119, 123, 159,
 179-180
 EES and, 117-118, 179-180
 separation of duties principle, 37-39
- Electronic Text Center, 96
- ElGamal signature scheme, 217
- Emergency response, 8, 57
- Employee misuse of information, 3,26,60
- Employee monitoring, 60-61
- Encryption. See Cryptography
- Encryption algorithms. See Cryptographic
 algorithms
- End-use regulations, 157
- Energy Science Network, 57
- Enigma cipher machines, 112
- ES-net. See Energy Science Network
- Escrow agents, 118, 173, 180, 181
- Escrowed-encryption initiative, 5, 17,39,67,
 161-163, 173-174, 176-177, 179-182
- Escrowed Encryption Standard
 classified encryption algorithm, 120-123
 Clinton Administration policy, 11, 131, 172
 compared with fair cryptosystems, 67

- CSSPAB hearings cm, 176, 177
 - debate over, 9,47, 116
 - description, 117-119
 - development process, 18, 175
 - effect on technology control, 126, 129, 130
 - effects of introduction as new federal standard, 127-128
 - future of, 131
 - key escrowing for, 118, 171, 173-174, 180, 181
 - policy options, 17, 179-182
 - public-key Key Exchange Algorithm and, 127, 216
 - resistance to, 11,131, 132
 - telephone systems security, 11, 16, 172
 - Escrowed keys, 60-61
 - Ethics, 8,58-60, 135
 - ETSI. See European Telecommunications Standards Institute
 - European Community
 - cryptography export controls, 155
 - Information Technology Security Evaluation Criteria, 49
 - role in development of Generally Accepted System Security Principles, 51
 - working toward international product evaluation standard, 49
 - European Computer Manufacturers Association, 47
 - European Economic Community Commission
 - Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 90-95
 - draft directive for protection of personal data, 88
 - Green Book on the Security of Information Systems*, 91-92
 - European Telecommunications Standards Institute, 47
 - European Union
 - protection of personal data, 21,70,88,90-95
 - Executive Agent of the Government for National Security Telecommunications and Information Systems, 143, 145
 - Executive branch implementation of cryptography policy, 171-174
 - Executive Order 12333, 143
 - Export Administration Act, 153, 156
 - Export controls
 - Commerce Department controls, 153-154
 - competitiveness and, 45-46, 154-160, 181
 - contentious items, 155-156
 - cryptographic items excepted from control, 154
 - on cryptography, 7,9, 10, 11-13, 17,61, 115, 128, 132, 150-160, 181, 182
 - DES, 129
 - DSS, 221
 - effects on development of safeguards, 132
 - federal agency concerns, 134
 - policy options, 178-179
 - regulatory regimes, 150-151
 - State Department controls, 151-152
 - Export Controls and Nonproliferation Policy*, 159
- F**
- Fair Credit Reporting Act, 80
 - Fair cryptosystems, 67
 - Fair use
 - concept of, 102-103
 - criteria, 100, 101, 102-102
 - digital libraries and, 22,97
 - and fee-for-use copyright protection, 110
 - policy options, 23, 105-106
 - size of the work and, 98
 - Family Educational Rights and Privacy Act of 1974, 80
 - Farber, David, 175
 - FB [. See Federal Bureau of Investigation
 - FCC. See Federal Communications Commission
 - Federal agencies. See *also* Government; *specific agencies*
 - developing an organizational security policy, 29-30
 - formal security models, 31-32
 - future directions in safeguarding information, 148-150
 - guidance on safeguarding information, 132-150
 - information security and privacy concerns, 134-135
 - interagency linkages and privacy, 21-22, 29, 84, 85
 - national security and, 111-114
 - Privacy Act requirements,81 -85
 - responsibilities prior to Computer Security Act, 139-143
 - responsibilities under the Computer Security Act, 145-148
 - safeguarding information, 18-20, 182-183
 - security plans, 19
 - Federal Bureau of Investigation, 2-3, 116, 169, 173
 - Federal Communications Commission, 61
 - “Federal Criteria” for product evaluation, 49
 - Federal Information Processing Standards. See *also specific standards*
 - based on cryptography, 10-11
 - Commerce Department role, 142
 - development of, 5,47, 142
 - NIST role, 47, 168
 - significance of, 9, 129, 174
 - and technological stability, 129

- Federal Information Systems Security Educators' Association, 59
- Federal Internetworking Requirements Panel, 131-132
- Federal Privacy Commission
 proposed creation of, 22,95
 suggested responsibilities and functions, 22, 95
- Federal Register*
 online publication, 21, 85
- Federal Reserve System
 use of DES-based encryption technology, 131
- Federal Telephone System, 135
- Federal Videotape Privacy Protection Act, 80
- Financial Privacy Act of 1978,80
- Financial transactions. See *also* Banking industry;
 Electronic commerce
 authentication product evaluation by Treasury Department, 48
 authentication using DES, 121, 131
 need for safeguards, 68
 via information networks, 1-2
- Finding a Balance: Computer Software, Intellectual Property and the Challenge of Technological Change*, 6,97-106
- Finland
 data protection board, 22,95
- FIPS. See Federal Information Processing Standards
- Firewalls, 34-35
- FIRST. See Forum of Incident Response and Security Teams
- First-sale doctrine, 104, 105, 107
- Formal security models, 7-8,31-32
- Forum of Incident Response and Security Teams, 57
- France
 data protection board, 22,95
 Information Technology Security Evaluation Criteria, 49
- Fried, Charles, 82,83
- G**
- GAO. See General Accounting Office
- Gavison, Ruth, 83
- General Accounting Office, 2, 19,86, 133, 146, 156, 166, 167, 182-183,217,219
- General Services Administration
 information security services and documents, 137
 procurement, 135
 role in computer security, 139, 142
- Generally accepted principles, 31,44,51-52
- Generally Accepted System Security Principles, 8, 51,52
- Georgetown University, 118
- Germany
 availability of DES-based products, 158
 data protection board, 22,95
 Enigma machines, 112
 Information Technology Security Evaluation Criteria, 49
- Glenn, Sen. John
 letter of request to OTA, 5, 187
- Glickman, Rep. Dan, 140
- Goal Security Architecture, 163
- Goldberg, Arthur, 79
- Gore, Al, 11, 13, 16, 131, 172, 173
- GOSIP. See Government Open Systems Interconnection Profile
- Government. See *also* Congress; Federal agencies
 congressional role, 174-183
 export controls, 150-160
 importance of cryptography policy, 115-128
 management role, 7
 need for more open processes, 15, 16, 18, 170, 175-177, 178, 179, 182, 183
 NIST/NSA role, 160-174
 procurement policies effects, 131-132, 135
 public visibility and accountability for technology impacts, 17
 role in providing direction for information safeguards, 63-68, 179
 security problem examples, 2-3
 statutory guidance of safeguarding information, 132-150
 tension between promoting and controlling information safeguards, 8-9, 111, 115-128
 trusted product evaluation process, 8
 use of networks, 2-3
- Government Open Systems Interconnection Profile, 131
- Green Book, 91-92
- Griswold v. Connecticut*, 79
- GSA. See General Services Administration
- GSSPs. See Generally Accepted System Security Principles
- Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 88-90
- H**
- Hackers. See *also* "Crackers"
 DOD penetration, 2,3
 publicized incidents, 139
 threats to networked information, 26
- Hardware and Software Information Products
 GSSPs, 51
- Harris, Jo Ann, 130-131
- Hashing
 algorithms, 39, 124-125, 174, 222
 functions, 39
 standard, 65, 125, 174,219, 222

- Hellman, Martin, 126,220
- High Performance Computing and Communications/National Information Infrastructure Programs, 161
- HPCC/NII. See High Performance Computing and Communications/National Information Infrastructure Programs
- Human error and design faults, 25-26
- I
- IBM, 122, 123
- ICC. See International Chamber of Commerce
- ICC Position Paper on International Encryption Policy*, 181
- ICCP. See Institute of Computer Professionals
- Iceland
 - data protection board, 22,95
- Idaho State University
 - role in developing information security certification, 52
- IEEE. See Institute of Electrical and Electronics Engineers
- Incident reporting
 - Green Book proposals, 92
- Industrial List, 155
- Industry-government working groups, 172
- Information. See *also* Digital information; Networked information
 - as an asset, 42, 43
 - boundaries blurring, 4
 - integrity of, 28, 31, 32, 35-37, 76
 - ownership rights, 4
 - responsibility for, 4, 5, 182
- Information infrastructure
 - definition, 41
 - institutions that facilitate safeguards for, 40-63
- Information Infrastructure Task Force, 171
- Information network
 - definition, 27
- Information Policy Committee, 171
- Information Security Professional GSSPS, 51
- Information Systems Security Association
 - role in developing Generally Accepted System Security Principles, 51
 - role in developing information security certification, 52
- Information Technology Laboratory, 20, 136, 183
- Information Technology Security Evaluation Criteria, 49
- Insiders
 - auditing systems, 35
 - monitoring employees, 60-61
 - threat to networked information, 26
- Institute of Computer Professionals, 52
- Institute of Electrical and Electronics Engineers, 47
- Institute of Internal Auditors,51
- Insurance, 43-44
- Integrated Data Retrieval System, 3
- Integrity of information
 - contracts, 76
 - cryptography and, 35-37, 113
 - definition, 28
 - emphasis on by value-added services, 28
 - formal models and, 31,32
- Intellectual property, 4, 22-23, 46,70,97. See *also* Copyright; Patent issues
- Intelligence activities. See Electronic surveillance; National security; Signals intelligence
- Interactivity, 4
- Internal Revenue Service
 - electronic access to data, 84
 - information protection, 86, 133, 178, 179
 - misuse of data, 3
 - Tax Systems Modernization Program, 86
- International Chamber of Commerce, 181-182
- International data flow
 - DES and, 129-130
 - European Council Directive effects on U. S., 94-95
 - Green Book proposals, 92
 - ICC recommendations on international encryption, 181-182
 - personal information protections and, 21,22,70, 87-88,90-95
 - policy, 95, 181-182
 - privacy concerns, 87-95
- International Federation for Information Processing
 - role in developing information security certification, 52
- International Information Systems Security Certification Consortium, 52
- International Organization for Standardization, 47, 136
- International Traffic in Arms Regulations, 151, 152, 155, 156, 157, 158
- Internet
 - acceptable use, 58-59
 - advertising on, 58
 - decentralized nature of, 134
 - differing user objectives, 41
 - firewalls and, 35
 - growth of, 1
 - information network, 27
 - information services, 4
 - NIST activities relating to, 162
 - number of users, 1
 - as part of information infrastructure, 42
 - Privacy-Enhanced Mail, 36-37,54

- providers' emphasis on availability of services, 28
 - security problems, 2
 - Transmission Control Protocol/Internet Protocol, 46, 131
 - viruses, 2
 - worm, 149
 - Internet Architecture Board, 47
 - Internet Engineering Task Force, 47
 - Internet Society, 1,41
 - Interoperability
 - open systems and, 4
 - standards development, 165, 181
 - Iran
 - export controls, 154
 - Iraq
 - export controls, 154
 - Ireland
 - data protection board, 22,95
 - IRS. *See* Internal Revenue Service
 - ISC². *See* International Information Systems Security Certification Consortium
 - ISO. *See* International Organization for Standardization
 - Israel
 - data protection board, 22,95
 - ISSA. *See* information Systems Security Association
 - ITAR. *See* International Traffic in Arms Regulations
 - ITSEC. *See* Information Technology Security Evaluation Criteria
- J**
- Japan
 - cryptography export controls, 155
 - not included in work toward international product evaluation standard, 49
 - role in development of Generally Accepted System Security Principles, 51
 - Joint R&D Technology Exchange Program, 165
- K**
- Kallstrom, James, 116, 119
 - Kammer, Raymond G.
 - comments on cryptographic standards, 120, 126
 - letter of clarification of NIST/NSA memorandum of understanding, 201-209
 - NIST/NSA memorandum of understanding, 197-200
 - Katz v. United States*, 79
 - KEA. *See* Key Exchange Algorithm
 - Kent, Stephen, 118
 - Key
 - definition, 39, 113
 - size and encryption scheme strength, 113, 122-123
 - Key-escrow agents
 - policy options, 17, 18, 173
 - Key-escrow encryption. *See also* Escrowed-Encryption Standard; Public-key cryptography
 - Clinton Administration will ingness to explore industry alternatives for key-escrow encryption, 11, 131, 172
 - congressional policy review, 16-17
 - for the EES, 173-174
 - escrowed-encryption initiative, 5, 17, 39, 67, 161-163, 173-174, 176-177, 179-182
 - export controls, 159
 - law enforcement and, 9, 10,65, 117-118
 - policy options, 16, 178
 - separation of powers and, 18, 180
 - Key Escrow Encryption Working Group, 163
 - Key Escrow Encryption Workshop, 15-16, 172
 - Key exchange
 - Diffie-Hellman technique, 126
 - public-key, 10, 11,39,53,54, 125-126, 127
 - RSA techniques, 125-126
 - Key Exchange Algorithm, 65, 127,216
 - Key management
 - auditing and accountability controls, 173
 - deposit with trusted entity, 17, 171
 - exchanging keys, 10, 11, 38, 53, 54, 125-126, 127,216
 - functions, 113
 - Green Book proposals, 92
 - key-escrow agents, 17, 18, 173
 - MITRE study on, 219
 - public-key infrastructure, 53-56
 - Kravitz, David, 217
- L**
- Laptop computers, 157, 158
 - Law enforcement. *See also* Electronic surveillance
 - cryptography and, 8-9, 17, 111, 116-120, 126, 128, 129
 - monitoring financial transactions, 68
 - safeguarding networked information, 60
 - Law Enforcement Access Field, 65, 117, 118, 173
 - Lawrence Livermore Laboratory, 57
 - LEAF. *See* Law Enforcement Access Field
 - Leahy, Sen. Patrick, 141
 - "Least privilege" principle, 37
 - Legal issues
 - digital libraries, 22-23,70,96-110
 - electronic commerce, 20-21, 69, 70-78
 - legal sanctions, 8, 18,60-61, 180-181
 - privacy protection, 21-22,70,78-95

Letter of request to OTA from Rep. Edward J. **Markey**, 188
Letter of request to OTA from **Sen. John Glenn**, 187
Letter of request to OTA from **Sen. William V. Roth, Jr.**, 185-186
Letters of clarification of **NIST/NSA** memorandum of understanding, 201-209,210-214
Libraries. *See also* Digital libraries
digital information copyright issues, 98-104
Libya
export controls, 154
Licensing. *See* Export controls
Logic bombs, 36
Lou **Harris/Equifax** survey on privacy, 87
Luxembourg
data protection board, 22,95

M

Maher, David, 118
Malicious software. *See also* Viruses; Worms
threats to networked information, 26
Management
cost-justifying safeguards, 30-31,52, 134
NIST activities related to, 163
role in developing organizational security policy, 7, 18,27,29
role in establishing or inhibiting safeguards, 42-43, 148, 149, 150
Management of Federal Information Resources. See OMB Circular A-130
Markey, Rep. Edward J.
letter of request to OTA, 5, 188
Massachusetts Institute of Technology, 220
McConnell, J. M., 159
McNulty, F. Lynn, 218
Memorandum of Understanding, 13-14,20, 148, 164-171, 183, 197-200,201-209
Merkle, Ralph, 220
Merkle's "tree-signature" technique, 121
Message digest, 39, 124-125,219,222
Mexico
role in development of Generally Accepted System Security Principles, 51
Miller, Jim, 141
MILNET, 57
MIT. *See* Massachusetts Institute of Technology
MITRE Corp., 219
Money laundering, 68
Mosbacher, Robert A.
letter of clarification of **NIST/NSA** memorandum of understanding, 210-214
Multimedia works
copyright issues, 23,97, 106-108
policy options, 23, 106, 108

Multiple encryption, 122-123
Munitions List
Commerce Department export controls compared with State Department controls, 153-154
cryptography on, 151-152, 155, 156
establishment of, 151
robust encryption, 154
Murray, Sen. Patty, 12, 160
MYK78. *See* Clipper chip
MYK80. *See* Capstone chip
Mykotronx, 64,65, 117

N

National Communications System, 61
National Computer Ethics and Responsibilities Campaign, 59-60
National Computer Security Center, 48
National Computer Security Conference, 164, 165
National Conference of Commissioners on Uniform State Laws, 74
National Crime Information Network, 2-3
National Information Infrastructure program
NIST activities relating to, 162, 163
NRC report on, 63
research and development, 62-63
royalty collection agencies, 109
National Institute of Standards and Technology
activities in support of security and privacy, 161-164
Computer Security Division, 162-163
emergency response, 57
funding for computer-security activities, 20, 163-164, 183
as key-escrow agent, 118, 163, 173
Key Escrow Encryption Workshop, 172
laboratories, 136
letter of clarification of **NIST/NSA** memorandum of understanding, 210-214
NIST/NSA memorandum of understanding, 13-14,20, 148, 164-171, 183, 197-200,201-209
overview of joint **NIST/NSA** activities, 165
policy option, 16, 178
product evaluation, 48, 121
proposed "Federal Criteria" for product evaluation, 49
research and development, 62
role in developing information safeguards, 160-174
role in developing information security certification, 52
role in developing standards, 9, 10,47, 121, 122, 132, 139, 145-145, 147, 148, 160-174,215, 216-217
role in standards-setting, 47

- Trusted Technology Assessment Program, 48-49, 50
- National Manager for Telecommunications and Automated Information Systems Security, 143, 145
- National Performance Review, 51,62,63
- National Policy on Telecommunications and Automated Information Systems Security (NSDD-145)*, 141, 143-145
- National Research Council
 - comments on system certification, 50-51,62
 - report on computer security, 63-65
 - report on information networking and the National Information Infrastructure program, 63
 - study of IRS implementation of TSM initiative, 86
 - study of national cryptography policy, 16, 17, 177, 178,220
 - suggests areas for research, 62
 - suggests establishment of generally accepted principles, 51
- National Science Foundation, 58,62,63
- National security. *See also* National Security Agency; Signals intelligence
 - cryptography control and, 115-116, 126,127, 128, 137, 166-167, 170, 176, 177, 183
 - export controls and, 12, 45, 115
 - federal agencies and, 111-114
 - terrorism, 9, 116, 118
- National Security Agency
 - development of SKIPJACK, 117
 - education on ethical computer use, 59
 - emergency response, 57
 - expanded responsibilities under NSDD-145, 143-145
 - export controls, 45, 154, 155-156, 157
 - joint NIST/NSA activities, 164
 - letter of clarification of NIST/NSA memorandum of understanding, 210-214
 - NIST/NSA memorandum of understanding, 13-14,20, 148, 164-171, 183, 197-200,201-209
 - overview of joint NIST/NSA activities, 165
 - policy option, 16, 178
 - product evaluation, 48, 121
 - proposed "Federal Criteria" for product evaluation, 49
 - research and development, 62
 - role in computer security, 140
 - role in developing information safeguards, 160-174
 - role in developing information security certification, 52
 - role in developing standards, 121, 122, 123, 132, 139, 141, 145, 146, 147-148, 148, 160-174, 216-217
 - SKIPJACK, 64
 - working toward international product evaluation standard, 49
- National Security Council, 15,61, 118, 119, 166, 170, 171
- National Security Decision Directive 145, 141, 143-145
- National Security Directive 42, 137-138
- National Security Telecommunications Advisory Committee, 172
- National Security Telecommunications Advisory Council, 61
- National Security Telecommunications and Information Systems Security Committee, 145
- National Telecommunications and Information Administration, 139-142
- National Telecommunications and Information Systems Security Committee, 143
- National Telecommunications and Information Systems Security Policy Directive No. 2*, 140, 144-145
- Natural disasters and environmental damage threats to networked information, 26
- NCS. *See* National Communications System
- NCSC. *See* National Computer Security Center
- Netherlands
 - data protection board, 22,95
 - Information Technology Security Evaluation Criteria, 49
- Network
 - definition, 27
- Network Reliability Council, 61
- Networked information. *See also* Information government's role, 63-68
 - institutions that facilitate safeguards for, 40-63
 - organizational objectives and security policy, 7
 - policy issues and options, 8-23
 - safeguards for, 6-8, 26-40
 - system certification and accreditation, 50-51
 - threats to networked information, 25-26
 - trends affecting information security, 3-5
- NII Security Issues Forum, 173
- NJ ST. *See* National Institute of Standards and Technology
- Nonrepudiation
 - definition, 28
 - emphasis on by value-added services, 28
 - encryption and, 35-37
 - Green Book proposals, 91
 - need for, 69, 76
 - services, 20-21, 76
- North Korea
 - export controls, 154
- Norway
 - data protection board, 22,95
- NRC. *See* National Research Council

- NSA. See National Security Agency
- NSDD- 145. See National Security Decision Directive 145
- NSFNET, 62
- NSTAC. See National Security Telecommunications Advisory Council
- NSTISSC. See National Security Telecommunications and Information Systems Security Committee
- NTIA. See National Telecommunications and Information Administration
- NTISSC. See National Telecommunications and Information Systems Security Committee
- O**
- Objectives
- differing objectives in large networks, 41
 - federal agencies, 27, 135
 - organizational objectives and information safeguards, 7, 27-28, 32
- OECD. See Organization for Economic Cooperation and Development
- Office of Export Licensing, 153
- Office of Management and Budget
- responsibility for computer security policy, 43, 39, 142, 143, 146, 161, 182
 - responsibility for information resource management, 18, 133, 150
 - role in defining objectives and organizational security policy, 7, 27
 - role in emergency response, 57
- Office of Science and Technology Policy, 119, 171
- Office of Technology and Policy Analysis, 153
- Office of Technology Assessment
- letters of request, 185-188
 - scope and background of OTA report, 5-6
- OMB. See Office of Management and Budget
- OMB Bulletin 90-08, 138
- OMB Circular A-71, 143
- OMB Circular A-123, 137
- OMB Circular A-130, 18-19, 133, 137-138, 143-144, 150, 182-183
- OMB Transmittal Memorandum No. 1, 143
- Omnibus Export Administration Act, 12, 160
- Online Computer Library Center, 96-97
- Online publishers
- cryptography and access controls, 28
- Open systems, 4,5
- Open Systems Interconnection protocols, 46, 131
- Open Systems Security
- NIST activities relating to, 163
- “Opportunity to Join a Cooperative Research and Development Consortium to Develop Software Encryption with Integrated Cryptographic Key Escrowing Techniques,” 161-163
- Orange Book, 48
- Organization for Economic Cooperation and Development
- Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 88-90
 - information-security guidelines, 51
 - personal data controls, 21
- Organizational security policy
- cost-justifying safeguards, 30-31
 - developing, 29-30
 - formal models, 31-32
 - organizational objectives and, 27-28
- OSI. See Open Systems Interconnection
- OSTP. See Office of Science and Technology Policy
- Ownership of electronic information, 4,6
- P**
- Paperwork Reduction Act of 1980, 133, 137-138
- Parent, W. A., 83
- Passwords
- challenge-response systems, 32
 - guidance for users, 33
 - sniffer network monitoring incidents, 3, 149
 - weak vs. strong, 33
 - weaknesses of, 32, 33
- Patent issues, 127, 128, 167, 168,217,220-221
- Paul v. Davis*, 80
- PCMCIA cards, 34,65, 129
- PEM. See Privacy-Enhanced Mail
- Penalties, 8, 18,60-61, 180-181
- Personal data
- access to, 21, 81, 85, 93, 130, 135
 - amendment right under Council Directive, 93
 - amendment right under OMB Circular A-130, 138
 - amendment right under Privacy Act, 81
 - collection of, 138
 - European Community protection of, 21,22, 87-88,90-95
 - policy options, 21-22,85,95, 182-183
 - Privacy Act rights, 80-87
 - privacy issues, 21-22,85,87, 135
 - protection of, 20-21,70,87, 138
- Plaintext**
- definition, 113
- Pohlig, Stephen, 220
- Poindexter, John, 144
- Policy issues and options, 8-23,85,95, 105-106, 108, 110, 174-183
- President
- role in standards appeal-mechanism, 166, 168

- Privacy. See *also* Privacy Act of 1974
 computerization and, 85-87
 constitutional right to, 78-80
 definition, 82-83
 distinguished from confidentiality, 28,82-83
 federal agency concerns, 134, 135
 interactivity and, 4
 international data flow, 87-95
 legal issues, 21-22,70,78-95
 “Mega-Project” on privacy, security, and intellectual property, 172-173
 NIST activities in support of, 161-164
 policy options, 21-22,85,95, 182-183
 problem examples, 2-3
 statutory requirements, 80-85, 133
 streamlined operations and, 4-5, 29
 Privacy Act of 1974, 19,21,80-85,88, 133, 182
Privacy and Freedom, 82-83
 Privacy-Enhanced Mail, 36-37,54
 Privacy Protection Act
 proposes establishment of Privacy Protection Commission, 22,95
 Privacy Protection Commission
 proposed creation of, 22,95
 suggested responsibilities and functions, 22, 95
 Procurement, 131-132, 135
 Prodigy, 28
 Product
 definition, 50
 Product evaluation
 delegation to third parties certified by the U.S. government, 49
 in the European Community, 49
 Green Book proposals, 92
 international standard proposal, 49-50
 joint NIST/NSA activities relating to, 49, 165
 purpose of, 47-48
 trusted product evaluation process, 8
 in the U. S., 48-50
 Professional development, 52-53
 Professional organizations and examinations, 52-53
Protecting Privacy in Computerized Medical Information, 6
 Protocols
 definition, 46
 Public access
 need for more open processes, 15, 16, 18, 170, 175-177, 178, 179, 182, 183
 to personal data, 21, 81,93, 135, 138
 Public-key cryptography. See *also* Digital Signature Standard
 choice of a signature technique for the standard, 10,217-220
 CNRI-proposed electronic copyright management system, 110
 definition, 113
 description, 39
 for digital signatures, 6, 10,39, 113, 124-125, 215,216,217-220
 electronic commerce and, 6,7, 16, 53-56, 68, 1 13
 infrastructure, 7, 16, 53-56, 68, 216
 key exchange, 10, 11,39,53,54, 125-126, 127
 royalty issue, 220
 standard development efforts, 167, 216
 uses of, 10, 127
 Public Key Partners, 220-221,222
 Publishing under copyright law, 98
- R**
 Rainbow Series books, 48,49,51
 Reagan Administration, 139, 141
 Regulatory bodies, 61-62
 Reno, Janet, 118, 173
 Research and development
 joint NIST/NSA activities relating to, 165
 National Information Infrastructure Program, 62-63
 Responsibility for information, 4,5, 182
 Risk analysis, 7,30,31,44
 Rivest, Ronald, 220
 Rivest-Shamir-Adleman system, 11,39, 124-126, 217,220
 Robust encryption, 10, 127, 132, j54
Roe v. Wade, 79
 “Rogue countries” export controls, 154
 Roth, Sen. William V., Jr.
 letter of request to OTA, 5, 185-186
 Royalties
 copyright collectives, 108-110
 current performance plan, 109
 for electronic information, 23,68,97, 105
 fee-for-use plan, 110
 four-fund system, 109
 policy options, 23, 110
 RSA Data Security, Inc., 157,216,220
 RSA system. See Rivest-Shamir-Adleman system
 Rules of evidence
 electronic commerce and, 74-78
 Russia
 availability of DES-based products, 158
 export control policy, 155
- S**
 Safeguarding networked information
 government’s role, 63-68
 institutions facilitating safeguards, 40-63
 organizational objectives and policy, 27-32
 techniques and tools, 32-40
 threats to networked information, 25-26

- Sandia National Laboratories, 118
 - Satellite networks
 - emphasis on availability of services, 28
 - information infrastructure, 41
 - Schnorr, Claus, 220
 - Secret-key systems. See *Symmetric cryptosystems*
 - Secure Hash Standard, 65, 125, 174,219,222
 - Secure tokens, 34, 129
 - Security. See *also* Safeguarding networked information
 - definition, 26-27
 - problem examples, 2-3
 - Security Coordination Center, 57
 - Security practitioners
 - professional development, 52-53
 - Sensitive information
 - definition in Computer Security Act of 1987, 140-141, 143-144
 - Sensitive items
 - export controls, 153, 154-155
 - Separation of duties principle, 37-39
 - Separation of powers and key escrow, 18, 180
 - Service providers
 - Green Book self-evaluation proposal, 92
 - organizational objectives and security aspect emphasis, 27-28
 - trends, 4
 - Shamir, Adi, 123,220
 - Shils, Edward, 82
 - Signals intelligence. See *also* Electronic surveillance; National security
 - cryptography and, 8-9, 17, 111, 116-120, 128, 129, 166
 - NSA role, 112, 122, 169,219
 - Signature. See *also* Digital signatures
 - requirement of U. C. C., 73,74
 - Signature standard. See Digital signature standard
 - SKIPJACK, 64,65, 117, 118-119, 170, 174
 - Small Business Administration, 85
 - Smart cards, 34, 128-129, 154
 - SmartDisks, 34
 - Sniffer programs, 3
 - Social Security Administration
 - electronic data access, 84
 - Socular, Milton J.,]64-165
 - Software
 - developer responsibilities for safeguards, 44-46
 - export controls, 11-12, 154, 155, 156-157
 - implementation of cryptography, 67, 182
 - Software Engineering Institute, 57
 - Software Publishers Association
 - study identifying encryption products using DES, 130
 - study of foreign availability of encryption products, 157-158
 - “Solicitation for Public Key Cryptographic Algorithms,” 167, 216
 - SPA. See Software Publishers Association
 - SRI International, 57
 - SSA. See Social Security Administration
 - Standards. See *also specific standards*
 - appeal mechanism, 166, 168-170
 - definition, 46
 - development of, 46-47, 115, 134
 - effects on information safeguards, 46-47, 147
 - international, 181, 182
 - joint NIST/NSA activities relating to, 148, 164-171
 - NIST activities relating to, 136, 145, 147, 162, 164-171
 - standards-setting bodies, 46-47
 - and technological stability, 129
 - Stanford University, 220
 - Statute of Frauds, 71-74
 - Studeman, W.O.
 - letter of clarification of NIST/NSA memorandum of understanding, 201-209
 - NIST/NSA memorandum of understanding, 197-200
 - Subscription services
 - emphasis on access control, 28
 - Sweden
 - data protection board, 22,95
 - Symmetric cryptosystems, 39, 113
 - System
 - certifications and accreditations, 50-51
 - definition, 50
 - Systems Security Examination, 52
 - Systems Steering Group, 143
- T**
- Tax Systems Modernization Program, 86
 - Taxpayer data
 - misuse by IRS employees, 3
 - protection of, 86, 133, 178, 179
 - TCP/IP. See Transmission Control Protocol/Internet Protocol
 - TCSEC. See Trusted Computer Security Evaluation Criteria
 - Technical harmonization
 - Green Book proposals, 92
 - Technical Working Group (NIST/NSA), 14, 166, 167,]69, 217,219
 - Telephone systems
 - EES and, 11, 16,64, 172
 - emphasis on availability of services, 28
 - Federal Telephone System, 135
 - information infrastructure, 41
 - information services, 4
 - regulatory bodies, 61

- TEMPEST equipment, 48
Terrorism, 9, 116, 118
TESSERA card, 127, 167, 216
Third-party trustees. See Trusted entity
Threats to networked information
 “crackers” and other intruders, 26
 human errors and design faults, 25-26
 insiders, 26
 natural disasters and environmental damage, 26
 viruses and other malicious software, 26
Time stamping
 in electronic commerce, 76-78
 Green Book proposals, 92
Tokens, 34, 129
Trading partner agreements, 74
Training. See Education/training
Transactional Reporting Service, 109
Transmission Control Protocol/Internet Protocol, 46, 131
Treasury Department. See Department of the Treasury
Trivial File Transfer Protocol, 2
Trojan horses, 36
Trust level assignment, 48
Trusted Computer Security Evaluation Criteria, 48
Trusted entity. See *also* Certification authorities
 attributes of, 77
 functions, 77-78
 Green Book proposals, 91-92
 key management, 67, 171, 178
 Postal Service as, 55-56, 78
 time stamping, 77
Trusted product evaluation process, 8
Trusted Technology Assessment Program, 8, 49, 50, 165
Trustees. See Trusted entity
TSM. See Tax Systems Modernization Program
TTAP. See Trusted Technology Assessment Program
Tuchman, Walter, 118
- U**
U.C.C. See Uniform Commercial Code
Unauthorized copying, 105
Unauthorized use, 58-60
Uniform Commercial Code
 electronic funds transfers security procedures, 72-73
 proposed legislative modifications, 74
 Statue of Frauds, 71-74
United Kingdom
 availability of DES-based products, 158
 Code of Practice for Information Security Management, 51
 Commercially-Licensed Evaluation Facilities program, 49
 data protection board, 22, 95
 United States v. Miller, 80
 University of Virginia, 96
 UNIX trusted-host feature, 2
 U.S. Postal Service
 as certification authority, 55-56
 trusted third-party functions, 78
 U.S. Privacy Protection Study Commission, 85-86
 U.S. Public Policy Committee of the Association for Computing Machinery, 182
 USACM. See Association for Computing Machinery
 Users
 definition, 27
 emphasis on confidentiality, 28
 ethics, 8, 58-60, 135
 responsibility for security, 134, 135
- V**
Value-added network providers
 as certification authorities, 54
 emphasis on integrity and nonrepudiation, 28
 trusted entity functions, 78
Vendors
 government regulation, 61, 62
 Green Book self-evaluation proposal, 92
 licensing vs. selling, 98
 responsibilities for safeguards, 44-46
 self-validation of product claims, 49
Virus checkers, 35, 36
Viruses
 affecting Internet, 2
 protection practices, 36
 threats to networked information, 26
VLSI Logic, 117
Vulnerabilities. See *also* Threats to networked information
 shared information policies, 57
- W**
Walker, Stephen, 132, 157-158
Warren, Earl, 79
Warren, Samuel, 79, 82
Westin, Alan, 82-83
White Book, 49
Williams & Wilkins Co. v. United States, 103
Wireless networks
 emphasis on availability of services, 28
 information infrastructures, 41
Wiretapping. See Electronic surveillance
Working Group on Encryption and Telecommunications, 171-172

Worms. See also Viruses
definition, 36
protection practices, 36
Wright v. Warner Books, 103

Writing
copyright law, 100
U.C.C. requirement, 71 -74

Superintendent of Documents **Publications** Order Form

Order Processing Code:

***7515**

YES, please send me the following:

Telephone orders (202) 512-18;3
(The best time to call is between 8-9am. EST.)
To fax your orders (202)512-2250

Charge your order. It's Easy!

_____ copies of **Information Security and Privacy in Network Environments** (252 pages),
S/N 052-003 -01387-8 at \$16.00 each.

The total cost of my order is \$_____. International customers please add 2570. Prices include regular domestic postage and handling and are subject to change.

(Company or Personal Name) (Please type or print)

(Additional address/attention line)

(Street address)

(City, State, ZIP Code)

(Daytime phone including area code)

(Purchase Order No.)

Please Choose Method of Payment:

Check Payable to the Superintendent of Documents

GPO Deposit Account -

VISA or MasterCard Account

(Credit card expiration date)

**Thank you for
your order!**

(Authorizing Signature)

(9/94)

YES NO
May we make your **name/address** available to other mailers?

Mail To: New Orders, Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250-7954