Index

A
Accredited Standards Committee X9, 20, 82
Advanced Research Projects Agency, 19, 81
Algorithms. *See* Cryptographic algorithms
American Bar Association
  Science and Technology Section's Information Security Committee, 23, 87, 129
Arms Export Control Act, 12-13, 63, 117
ARPA. *See* Advanced Research Projects Agency
ASC X9. *See* Accredited Standards Committee X9
Association for Computing Machinery
  EES policy issues report, 21, 85
  U.S. Public Policy Committee of the ACM, 21-22, 85
Asymmetric cryptosystems. *See* Public-key cryptography
ATM machines, 117, 118
AT&T Corp.
  encryption microchip development, 20, 56, 82
AT&T CryptoBackup, 83
AT&T Surity Telephone Device, 20, 82
Authentication
  cryptography and, 47, 48
  definition, 6
Authenticity
  definition, 3

B
Background paper
  description, 2
  overview of chapters, 3-42
  purpose, 23
Bankers Trust International Corporate Key Escrow, 21, 83
Banking and financial services industries
  cryptography and, 20, 82, 117-118
Bell Atlantic Key Escrow, 83
"Best practices" of businesses, 68-71
Bill of Rights for privacy, 71
Branstad, Dennis, 82-83
Brickell, Ernest, 55
Brooks Act of 1965, 106-107
Bureau of Export Administration, 119
"Business Requirements for Encryption," 22, 86
Businesses. *See* Private sector; *specific businesses by name*

C
Canada
  privacy policy, 71
Cantwell, Rep. Maria, 13, 63
Capstone chip
  costs, 18, 35, 80, 98
  escrow locations, 17
  lack of market support for, 20, 82
  use by Defense Message System, 79
Cellular phones, 119-120
China
  liberalization of exports to, 120
Ciphertext
  description, 46, 48
Cleartext
  description, 46
Clinton Administration. *See also* Escrowed-encryption initiative; Escrowed Encryption Standard; Executive branch
  centralization of information security authorities, 8, 27, 53
  commitment to escrowing encryption keys, 17-18, 79
  creation of interagency working group on encryption and telecommunications, 56
  easing of export controls on cryptography without legislation, 14, 64
  exportability of EES encryption products, 54
  international market studies, 63
  liberalization of export controls, 120
  market study of cryptography and export controls, 97-98
  NIST funding, 81
  plans for making escrowed encryption mandatory, 37, 53, 125

Clipper chip. *See* Escrowed Encryption Standard
COCOMM. *See* Coordinating Committee for Multilateral Export Controls
Code of Fair Information Practices, 24, 89
Collins, Rep. Cardiss, 23, 88
Commerce Department. *See* Department of Commerce
Committee on Government Operations
    report on H.R. 145, 111-112
Competitiveness
    U.S. export policy and, 67
Computer crime, 72
Computer Security Act of 1987, 53
    agency responsibilities, 42, 109-110, 112-114
    controversies over, 910, 60, 92, 105-106, 114-115
    cost-effective safeguards, 41, 101
    description, 9, 60
    evolution of policy framework, 106-108
    frustration over implementation of, 74
    fulfilling intent of the act, 105, 115
    hearings on, 111
    implementation issues, 9-10, 15-16, 39, 42, 105, 114-115
    incentives for compliance and sanctions for noncompliance, 123
    mandates, 78
    NIST responsibilities, 9-10, 42, 113-114, 127-128
    NSA responsibilities, 9-10, 110-112, 113-114
    OMB Circular A-130 Appendix III proposed revision and, 29, 32, 126
    overlapping agency responsibilities before, 109-110
    oversight of, 16, 42, 68, 74, 98
    provisions, 10, 91, 105, 108-115
Computer System Security and Privacy Advisory Board, 10, 27, 60, 74, 105, 108-109, 114
    Resolution 95-3, 92
Computer Systems Laboratory, 107, 115
Computer Systems Policy Project
    GII recommendations, 21, 84-85
Confidentiality
    definition, 3
Congress. *See also* Government; Legislation; *specific committees, pieces of legislation, and members of Congress by name*
    cryptography policy review, 34-35, 123-124
    escrowed encryption initiatives responses, 36-37, 42, 125-126
    export administration legislation, 13, 63, 64, 121
    export controls and, 13, 14, 35-36, 63, 68, 73, 97-98, 121
    federal information security and privacy oversight, 37-38, 40-41, 98
    implications for action, 34-42, 97-101
    issues and options, 4, 34-42, 122-131
    letter of request to OTA, 2, 104
    locus of authority for information security, 39-42, 100-101
    OMB Circular A-130 Appendix III proposed revision oversight, 39, 40
    privacy protection legislation, 88-89
    workshop views on areas of action needed, 73-75
Cooperative research and development agreements
    for Westinghouse Savannah River Company to develop DSS software, 80
Coordinating Committee for Multilateral Export Controls, 120
Copyrighted materials
    digital signatures and, 47
    fee-for-use, 131
    options for protecting, 130-131
    workshop views, 71-72
Corporate privacy, 72, 75
Crackers, 2
CRADAs. *See* Cooperative research and development agreements
"Creating a New Order in U.S. Security Policy," 26-27, 91-92, 94
Credit reports, 24, 88
Crime
    computer crime, 72
    cryptography control and, 7
    organized crime, 78
Cryptanalysis
    description, 47
Cryptographic algorithms. *See also specific algorithms by name*
    description, 46
"Cryptographic Service Calls," 19, 81
Cryptography
    applications of, 56
    background, 5
    congressional review and open processes, 34-35, 123-124
    description, 3, 45, 46
    executive branch developments, 79-81
    history of, 46
    importance of, 57, 45-50
    misuse potential, 52
    nongovernmental markets, 6, 50
    policy debate over, 50, 52-53
    private sector developments, 82-84
    terminology, 46-47
    uses for, 46-47
Cryptography control
    Computer Security Act of 1987 and, 60
    as domestic security issue, 52-53
    export controls, 6, 7-8, 11-14, 35-36, 52-53, 61-64, 66-68, 116-121, 123, 124-125
    government marketplace influence, 60-61

  issues and options, 4, 64
  lack of dialogue between government and private sector on, 15, 67-68, 73-74, 101
  leadership and responsibility issues, 78, 15, 53, 68
  mechanisms, 7, 50
  as national security issue, 50, 52
  policy objectives, 7
  tension between promoting and controlling information safeguards, 50
Cryptosystems. *See also specific system by name*
  description, 46-47
CSL. *See* Computer Systems Laboratory
CSPP. *See* Computer Systems Policy Project
CSSPAB. *See* Computer System Security and Privacy Advisory Board

D

Damages
  for misuse or unauthorized disclosure of escrowed key components, 37, 126
Data Encryption Standard
  EES algorithm comparison, 54
  export policy and, 67
  key length, 57
  reaffirmation of, 57
  as stable technology, 11, 61
  successors, 9, 57
  triple DES version, 9, 56, 57
"Data Encryption Standard" (FIPS Publication 46-2), 57
Databases
  key escrowing or trusteeship for, 18, 79
  national identification database, 23, 88
Decrypting, 117
Decryption keys, 6
Defense Information Systems Agency, 19, 81
  mock attacks, 78
Defense Message System, 9, 53, 80
Denning, Dorothy, 55, 82-83
Department of Commerce. *See also* Computer System Security and Privacy Advisory Board
  Commerce Control List, 118-119
  deposit of encryption keys in, 79
  economic impact of U.S. export controls on U.S. software industry, 13, 36, 125
  EES proposal, 8, 54
  export controls, 11-12, 13, 62, 63, 116, 118-121
  OMB Circular A-130 Appendix III proposed revision guidance, 33, 96
  responsibilities before Computer Security Act of 1987, 109
  traditional responsibilities for security standards, 100
Department of Defense, 53. *See also* Defense Information Systems Agency
  Defense Message System, 9, 53, 80
  export controls, 117
  Information Warfare activities, 24-25, 78, 89
  mock attacks on computers, 78
  OMB Circular A-130 Appendix III proposed revision guidance, 33, 96
Department of Energy
  UNIX flaw alert, 77
Department of Justice
  EES proposal, 54
  OMB Circular A-130 Appendix III proposed revision guidance, 33, 96
Department of State
  Arms Export Control Act amendment, 12-13, 63
  export controls, 11-13, 62, 82, 116-118, 119-121
  model law on electronic data interchange, 23, 87, 129
  Office of Defense Trade Controls, 117
Department of the Treasury
  deposit of encryption keys in, 79
  EES escrow agent, 55
DES. *See* Data Encryption Standard
Diffie-Hellman key exchange, 21, 58, 59
Digital libraries, 130-131
Digital Signature Act, 87-88, 129
Digital Signature Standard
  costs, 8081
  description, 49
  government-wide implementation, 80
  patent problems, 18, 79-80
  public-key algorithm specified in, 9, 57
  RSA and, 18, 20, 49, 80
Digital signatures
  acceptance and use of new FIPS for, 18
  alternatives to, 49
  description, 3, 6, 48-49
  electronic commerce and, 4, 128-129
  message authentication and, 47, 48
  public-key cryptography and, 47
  Utah statute, 87-88
DISA. *See* Defense Information Systems Agency
DOD. *See* Department of Defense
"Draft Principles for Providing and Using Personal Information and Commentary," 24, 89
Drug testing
  as privacy issue, 88
DSS. *See* Digital Signature Standard

E

Eastern Europe. *See also* Europe
  liberalization of exports to, 120
Economic espionage, 78

EES. *See* Escrowed Encryption Standard
Electronic commerce
  digital signatures and, 4, 128-129
  nonrepudiation services, 128
Electronic Record Systems and Individual Privacy, 130
Employees
  Computer Security Act of 1987 training requirements, 112-113, 115
  errors due to lack of training in security, 70
Encryption
  definition, 3, 56
Escrowed encryption
  description, 45
Escrowed-encryption initiative, 6, 45
  congressional responses to, 36-37, 42, 125-126
  controversy over, 4, 123
  costs, 35, 98
Escrowed Encryption Standard. *See also* Skipjack algorithm
  ACM report, 85
  alternatives to, 17, 79
  Clinton Administration policy, 35, 53
  closed process for developing and implementing, 15, 41, 128
  DES algorithm comparison, 54
  description, 67, 89, 53, 54
  functions, 54-55
  history of, 55-56
  lack of market support for, 20, 82
  as mandatory, 8, 37, 124, 125
  private sector acceptance, 15, 61
  "spare keys" for, 7
  uses, 9, 45
  voluntary use of by private sector, 125
Europe. *See also* Eastern Europe
  need for consistency between U.S. privacy laws and European privacy laws, 75
  privacy policies, 71
European Union, 130
Exclusionary Rule Reform Act of 1995, 23-24, 88
Executive branch
  alternatives to EES and Skipjack, 79
  cryptography developments, 79-81
  digital signatures, 79-81
  reaction to ISSC, 27, 92
Executive Order 12333, 110
Executive orders
  agency responsibilities and, 110
Export Administration Act
  reauthorization, 36, 97-98
Export Administration Act of 1995, 14, 64
Export Administration Regulations, 118
Export controls
  Arms Export Control Act amendment, 12-13, 63
  on cryptography, 6, 7-8, 11-14, 35-36, 52-53, 61-64, 66-68, 116-121, 123, 124-125
  liberalization of, 120
  licensing requirements, 11-12, 62, 63, 116-121
  military and dual-use items, 11, 61-62, 116
  omnibus export administration legislation, 63, 121
  proliferation of cryptography to foreign adversaries and, 12, 62-63
  workshop views on congressional action needed, 14-15, 66-68, 73, 97

F
"Fair use" concept, 131
Family Privacy Bill, 24, 88-89
Federal Bureau of Investigation, 73
Federal information processing standards. *See also specific standards and titles by name*
  DES and, 8, 9
  DSS and, 8, 9
  EES promulgated as, 8-9, 45
  escrowed-encryption initiative and, 4
  for secure key exchange, 79
  Skipjack and, 8-9, 79
  users' needs and, 98
Federal Manager's Financial Accountability Act, 97
Federal Register
  online publication of, 130
Financial services. *See* Banking and financial services industry
Finding a Balance: Computer Software, Intellectual Property, and the Challenge of Technological Change, 131
FIPSs. *See* Federal information processing standards
Firewalls, 78
FORTEZZA PCMCIA cards
  costs, 18-19, 80-81, 98
  Defense Message System use, 79
  nondefense agency adoption of, 35
  number in use, 53, 56
Fortress KISS, 83

G
General Accounting Office
  export controls, 120
  OMB Transmittal Memorandum No. 1 and, 110
  study request, 127
General Services Administration
  government public-key infrastructure, 81
  OMB Circular A-130 Appendix III proposed revision guidance, 33, 96
  responsibilities before Computer Security Act of 1987, 109
GII. *See* Global information infrastructure

Glenn, Sen. John
  letter of request, 2, 104
"Global Digital Signature Guidelines," 23, 87
Global information infrastructure, 21, 84-86
Gore, Albert. *See also* Vice President's National Performance Review
  encryption market and export controls study, 36, 125
  letter to Representative Cantwell, 13, 63
Government. *See also* Clinton Administration; Congress; Executive branch; Executive orders; Private sector; Reagan Administration; *specific agencies by name*
  agency downsizing and restructuring effects on information security, 98-99
  cryptography control efforts, 4, 6, 7-8, 50, 52-53, 56-64
  dialogue between government and private sector, 15, 67-68, 73-74, 97-98
  export controls, 6, 52-53, 61-64, 97-98
  federal agency head responsibilities under Paperwork Reduction Act of 1995, 95
  information security in federal agencies, 74-75, 98-101
  information security regarded as "expensive overhead" by agency managers, 98-99
  key-escrow encryption alternatives, 83-84
  locus of authority for information security, 39-42, 100-101
  management commitment to security, 4, 17, 38, 74, 94, 97, 98-99, 123
  marketplace influence attempts, 60-61, 69
  OMB Circular A-130 Appendix III proposed revisions, 95-97, 99-100
  proposals for centralizing security responsibilities, 8, 100-101
  safeguarding information in federal agencies, 126-128
  safeguarding unclassified information, 98-101
  tension between promoting and controlling information safeguards, 50
Government Information Technology Services Public-Key Infrastructure Federal Steering Committee, 19, 81

H

Hackers, 109
Hashing algorithms, 49
Hashing functions, 48-49
Horn, Rep. Steve, 24, 88
House Committee on Foreign Affairs, 13, 63
House Permanent Select Committee on Intelligence, 13, 63
House Subcommittee on Telecommunications and Finance, 2

I

ICC. *See* International Chamber of Commerce
"ICC Position Paper on International Encryption Policy," 22, 85-86
IEEE P1363
  working group on public-key cryptography, 20-21, 82
Immigration concerns, 23, 88
Individual Privacy Protection Act of 1995, 23, 88
Information infrastructure
  global information infrastructure, 21, 71, 84-86
Information Infrastructure Task Force
  Working Group on Privacy, 24, 89
Information security
  definition, 3
"Information Security and Privacy in Network Environments: What Next?." *See* Workshop
Information-security policy initiatives and legislation
  Joint Security Commission, 25-90, 100-101
  locus of authority for, 39-42, 100-101
  OMB Circular A-130 Appendix III proposed revision, 29, 32-34, 95-97
  Paperwork Reduction Act of 1995, 28-29, 94-95
  Security Policy Board, 25-28, 90-94
Information Systems Security Committee, 26-27, 39, 91-92, 100
Information Systems Security Research Joint Technology Office, 19-20, 24, 81, 89
Integrity of information
  cryptography and, 46-47
  definition, 3, 6
Intellectual property. *See also* Copyrighted materials
  options for protecting, 4, 130-131
  workshop views, 71-73
"Internal Control Systems," 107
International Chamber of Commerce
  cryptography position paper, 22, 85-86
  model law on electronic data interchange, 23, 87, 129
International issues. *See also* Export controls; *specific countries and regions by name*
  cryptography markets, 6
  DES-based encryption and authentication methods use, 20, 82
  personal data transfer, 130
  privacy policies, 71
  USCIB recommendations, 86
International Traffic in Arms Regulations, 117, 118
Internet, 122

lack of built-in security, 69
unauthorized intrusions, 2
ISSC. *See* Information Systems Security Committee
ITAR. *See* International Traffic in Arms Regulations

J

Joint Security Commission
efficiency arguments, 100-101
information security recommendations, 89-90
JTO. *See* Information Systems Security Research Joint Technology Office

K

Katzen, Sally
letter from Steering Committee of the Federal Computer Security Program Manager's Forum, 27, 92-93
Privacy Protection Commission statement, 88
Kent, Stephen, 55
Key-escrow encryption. *See also* Escrowed encryption; Public-key cryptography
alternatives to, 17, 21, 82-84
damages for misuse or unauthorized disclosure of escrowed key components, 37, 126
export controls and, 52-53
market appeal, 11
rationale for, 6
Key management, 47
Keys
commercial depositories, 79
decryption keys, 6
deposit in Commerce and Treasury departments, 79
description, 46-47
EES "spare keys," 7
key escrowing or trusteeship for large databases, 18, 79
optional deposit with registries, 17-18, 79
size and encryption scheme strength, 47

L

Lab document confidentiality, 72
Law enforcement, 52
Law Enforcement Access Field, 54, 55
LEAF. *See* Law Enforcement Access Field
Legal issues
confidentiality of corporate information, 72
copyrighted materials, 4, 47, 71-72, 130-131
digital signatures, 23, 87
electronic commerce, 128-129
intellectual property protection, 130-131
personal privacy protection, 129-130
Legislation. *See also* Congress; *specific pieces of legislation by name*
privacy protection, 23-24, 88-89
Letter of request from Roth and Glenn, 2, 104
Liability issues
business uncertainty about U.S. government's position on, 86-87
importance to electronic commerce development, 22-23, 87
personal data and, 72-73, 129-130
"Liability Issues and the U.S. Administration's Encryption Initiatives," 22, 86
Licensing requirements. *See* Export controls
Locus of authority for information security, 39-42, 100-101

M

Maher, David, 55
Mailing lists
sale of by communication carriers or U.S. Postal Service, 24, 88
Management
federal agency security responsibilities, 4, 17, 38, 74, 94, 97, 98-99, 123
private sector security responsibilities, 4, 16, 17, 68, 70-71, 123
"Management of Federal Information Resources," 107, 110
Marketing. *See also* Export controls
government efforts to control, 11, 60-61, 69
security problems in, 69
technology stability and, 10-11, 61
Medical privacy rights, 88
Memorandum of Agreement establishing JTO, 81
Memorandum of Understanding between NIST and NSA, 74, 109, 114
Message authentication
definition, 3
digital signatures and, 47, 48
Micali Fair Cryptosystems, 83
MOU. *See* Memorandum of Understanding between NIST and NSA
Multimedia works
copyright for, 131
Munitions List, 63, 117, 118, 119, 120
Murray, Sen. Patty, 13, 63
Mykotronx, 20, 54, 82

N

National Bureau of Standards. *See* National Institute of Standards and Technology
National identification database, 23, 88
National Institute of Standards and Technology, 73
DSS product validation system, 19, 81

EES escrow agent, 55
funding, 15-16, 19, 41, 42, 74-75, 81, 115, 127-128
Memorandum of Understanding with NSA, 74, 109, 114
redirection of activities, 39, 68, 98
responsibilities under Computer Security Act of 1987, 9-10, 42, 60, 105, 106, 112-113
"National Policy on Telecommunications and Automated Information Systems Security," 110
National Research Council
cryptography study, 13-14, 35, 64, 123-124
National Security Agency
absolute effectiveness standard versus cost-effectiveness, 41, 101
assessment of economic impact of U.S. export controls on U.S. software industry, 13, 36, 125
expanded responsibilities under NSDD-145, 110-112
foreign availability of encryption products study, 63-64
frustration over role of, 73-74
JTO establishment, 19
Memorandum of Understanding with NIST, 74, 109, 114
responsibilities under Computer Security Act of 1987, 9-10, 106, 113-114
Skipjack development, 8
Trusted Computer System Evaluation Criteria, 117, 119
National Security Council, 13, 54, 125
National Security Decision Directive 145, 92, 110-112
National Security Directive 42, 108
National Telecommunications and Information Administration, 109
National Telecommunications and Information Systems Security Committee, 110
"National Telecommunications and Information Systems Security Policy Directive No. 2," 110-111
NBS. *See* National Institute of Standards and Technology
Network information
decentralization, 5, 44
focus on safeguarding the information itself, 5, 44, 97
1994 OTA report
background, 44-45
cryptography importance, 45-50
current report and, 2
government efforts to control cryptography, 50, 52-53, 56-64
issues and options, 64, 122-131
motivation for, 122
need for products that integrate security features with other functions, 123
overview, 43-64
preparation request, 2
summary, 4
workshop participants and, 65
NIST. *See* National Institute of Standards and Technology
Nonrepudiation services for electronic transactions, 128
NSA. *See* National Security Agency
NSD 42. *See* National Security Directive 42
NSDD-145. *See* National Security Decision Directive 145
NTIA. *See* National Telecommunications and Information Administration
NTISSP No. 2. *See* "National Telecommunications and Information Systems Security Policy Directive No. 2"

O

OECD. *See* Organization for Economic Cooperation and Development
Office of Management and Budget, 53, 88. *See also specific OMB circulars by number*
effectiveness of guidance, 126-128
notice of "Draft Principles for Providing and using Personal Information and Commentary," 24, 89
Paperwork Reduction Act responsibilities, 94-95
responsibilities before Computer Security Act of 1987, 109
security policy guidance, 4, 123
Office of Personnel Management
OMB Circular A-130 Appendix III proposed revision guidance, 33, 96
Office of Strategic Trade and Foreign Policy Controls, 119
OMB. *See* Office of Management and Budget
OMB Circular A-71
Transmittal Memorandum No. 1, 110
OMB Circular A-123, 107
OMB Circular A-130, 107, 110
OMB Circular A-130 Appendix III, 107-108
OMB Circular A-130 Appendix III proposed revision, 78, 93
active risk acceptance and accountability by management, 33, 97
cost-effective safeguards, 41-42, 101
free information flow and public accessibility and, 27
guidance provisions, 29, 32, 33-34, 38-39, 40, 95-96

intention, 95, 126-127
shift in emphasis to safeguarding information itself, 5, 97
Omnibus Export Administration Act of 1994, 13, 63
Open Systems Interconnection protocols for networking, 60
Open User Recommended Solutions, 69-70
Organization for Economic Cooperation and Development, 130
Organized crime, 78
OSI protocols. *See* Open Systems Interconnection protocols for networking
OURS. *See* Open User Recommended Solutions

P

Paperwork Reduction Act of 1980, 107
Paperwork Reduction Act of 1995, 92
agency responsibilities, 28-29, 78
cost-effective safeguards, 29, 41, 101
provisions, 28-29, 94-95, 97
reaffirmation of OMB responsibilities, 29, 126
Passwords
employees' posting of passwords on computers, 70
password sniffers, 2, 77
Patents, 18, 72
Digital Signature Standard and, 79-80
PCMCIA cards. *See* FORTEZZA PCMCIA cards
PDD-29. *See* Presidential Decision Directive 29
Personal Computer Memory Card Industry Association cards. *See* FORTEZZA PCMCIA cards
Personal data
liability standards, 72-73, 75, 129-130
potential for abuse of information, 71
"Perspectives on the Global Information Infrastructure," 21
PKI. *See* Public-Key Infrastructure Federal Steering Committee
Plaintext
description, 46, 48
Poindexter, John, 110-111
Point of sale terminals, 117, 118
Presidential Decision Directive 29
items it was not intended to cover, 26, 91
Security Policy Board and Security Policy Advisory Board creation, 25, 26, 90-91
Privacy
definition, 3
medical privacy rights, 88
need for consistency between U.S. laws and European laws, 75
privacy protection legislation, 23-24, 88-89
workshop view, 71
Privacy Act
OMB Circular A-130 Appendix III proposed revision and, 29, 126
Privacy Act of 1974
provisions, 106
Privacy Bill of Rights, 71
Privacy Commission, 71, 75, 130
Privacy Protection Commission, 23, 88
Private sector. *See also* Government; *specific businesses by name*
availability of secure products, 69-70
common checklist for security officers, 70-71
cost concerns, 15, 69-70
cryptography developments, 20-21, 82-84
dialogue between government and, 15, 67-68, 73-74, 97-98
domestic and international privacy issues, 14-15, 71
global information infrastructure, 21, 84-86
information-security policies and "best practices," 68-71
large business and small business ability to purchase product incorporating security, 69
management responsibility for information security, 4, 16, 17, 68, 70-71, 123
preference for RSA over DSS, 80
technology-neutral security policies, 16, 68-69, 99
training issues, 70
voluntary use of EES, 11, 125
Proprietary information
workshop views, 71-73
Public-key cryptography. *See also* Digital Signature Standard
description, 6, 46-47, 48, 51
digital signatures and, 47, 48-49
secret-key distribution using, 58
Public-Key Infrastructure Federal Steering Committee, 81

R

RC2 algorithm, 20, 120
RC4 algorithm, 120
RC5 algorithm, 82
Reagan Administration
role of NSA, 109
Reno, Janet, 55
Rivest-Shamir-Adleman algorithm
description, 9, 48
DSS and, 18, 49, 80, 82
export policy and, 67
for secure key exchange, 58
signature creation, 49
Roth, Rep. Toby, 14, 64

Roth, Sen. William V., Jr.
letter of request, 2, 104
Royalties, 130-131
RSA algorithm. *See* Rivest-Shamir-Adleman algorithm
RSA Data Security, Inc.
RC5 algorithm, 20, 82
RC2 and RC4 algorithms, 120
Russia
liberalization of exports to, 120

S
Safeguard
definition, 3
Search and seizure issues, 23, 88
Secret-key cryptography
description, 46-47, 48, 50
"Security of Federal Automated Information." *See* OMB Circular A-130 Appendix III proposed revision
Security Policy Advisory Board, 26, 90-91
Security Policy Board
creation, 25, 90
Information Systems Security Committee, 25-27, 39, 91-92, 100
membership, 25, 90
OMB Circular A-130 Appendix III proposed revision guidance, 33, 96
opposition to recommendations, 92-93
Security Policy Forum, 90
staff comments on OTA draft text, 28, 94
staff report, 8, 26-27, 30-32, 91-92, 94, 100
"Security Policy Coordination," 25
Security Policy Forum, 25-26, 90
"Security Requirements for Cryptographic Modules" (FIPS 140-1), 19, 81
Senate Committee on Governmental Affairs, 2
Senate Committee on the Judiciary
Title V of S.3 hearing, 24, 88
Signature digitalization. *See* Digital signatures
Simon, Sen. Paul, 88
Single-key systems. *See* Secret-key cryptography
Skipjack algorithm
alternatives to, 17, 79
as DES successor, 57
description, 89, 54, 56-57
evaluation by outside experts, 55
key length, 56
uses, 8, 9, 18, 53
Smart cards, 117, 119
Sniffers, 2, 77
Social security cards
tamper proofing, 23, 88
Software
Commerce Department and NSA assessment of economic impact of U.S. export controls on U.S. software industry, 13, 36, 125
copyright for multimedia works, 131
export controls, 12, 62, 63, 118, 120
ITAR restrictions, 120-121
Software Publishers Association, 62*n*
SPB. *See* Security Policy Board
Spoofing, 77
State Department. *See* Department of State
Steering Committee of the Federal Computer Security Program Manager's Forum
letter to Sally Katzen, 27, 92-93
Subscriber list sale, 24, 88
Symmetric encryption. *See* Secret-key cryptography
Systems Security Steering Group, 110

T
TCP/IP protocols. *See* Transmission Control Protocol/Internet Protocol
Technology-neutral information-security policies, 16, 68-69, 99
TECSEC VEIL, 83
Terminology, 4
Terrorism, 7, 52, 78
TESSERA cards. *See* FORTEZZA PCMCIA cards
TIS. *See* Trusted Information Systems, Inc.
TIS Commercial Software Key Escrow System, 83
TIS Software Key Escrow System, 83
Training
Computer Security Act of 1987 requirements, 112-113, 115
employee errors and security systems, 70
materials for, 70
private sector problems, 17, 70
Transmission Control Protocol/Internet Protocol, 60-61
Trusted Computer System Evaluation Criteria, 117, 119
Trusted Information Systems, Inc.
key-escrow encryption alternative, 21, 83-84
key-escrow system description, 56
Tuchman, Walter, 55

U
United Nations Commission on International Trade Law
model law on electronic data interchange, 23, 87, 129
United States Council for International Business
position papers, 22-23, 86-87
UNIX operating system, 69
DOE's alert to flaw in, 77

U.S. Postal Service
government public-key infrastructure, 81
sale of mailing lists, 24, 88
U.S. Public Policy Committee of the ACM
recommendations, 21-22, 85
USACM. *See* U.S. Public Policy Committee of the ACM
USCIB. *See* United States Council for International Business
Utah
Digital Signature Act, 87-88, 129

V

Vice President's National Performance Review, 88
VLSI Logic, 54
VLSI Technology, Inc.
encryption microchip development, 20, 56, 82

W

Warner Amendment, 10, 60, 106
Westinghouse Savannah River Company, 80
Workshop
discussion topics, 14-17, 35-36, 66, 67, 97
objectives, 14, 66
participant demographics, 14, 65-66
private sector information-security policies, 68-75
purpose, 65
World Wide Web
home page flaw, 77
products under development, 77-78