Appendix B

CS Legal and Regulatory References

Federal Laws

- **Freedom of Information Act**, P.L. 89-487 [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+5USC552]
- **Executive Order No. 12046 of March 27, 1978** [no electronic version available]
- **Executive Order No. 12472 of April 3, 1984** [no electronic version available]
- **Executive Order No. 13011 of July 16, 1996**  
  [http://www.nara.gov/fedreg/eo_clint.html]
- **Homeland Security Directive HSPD-7, Critical Infrastructure Identification, Prioritization and Protection**  

---

*Continued on next page*
### CS Legal and Regulatory References, Continued

**Office of Management & Budget (OMB) Circulars, Bulletins and Memoranda**

- [http://www.whitehouse.gov/omb](http://www.whitehouse.gov/omb)

- **OMB Circular No. A-11** Preparation and Submission of Budget Estimates (05/03)
- **OMB Circular No. A-123** Management Accountability and Control (06/95)
- **OMB Circular No. A-130** Security of Federal Automated Information Resources (Appendix III) (11/00)
- **OMB Bulletin No. 90-08** (Appendix A) [Security Plans]
- **M-97-16** Information Technology Architectures (06/18/97)
- **M-99-05** Instructions on Complying with President’s Memorandum of May 14, 1998 “Privacy and Personal Information in Federal Records” (01/07/99)
- **M-99-18** Privacy Policies on Federal Web Sites (06/02/99)
- **M-99-00** Security of Federal Automated Information Resources (06/23/99)
- **M-00-07** Incorporating and Funding Security in Information Systems Investments (02/28/00)
- **M-00-10** OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act (04/25/00)
- **M-00-13** Privacy Policies and Data Collection on Federal Web Sites (06/22/01)
- **M-00-15** OMB Guidance on Implementing the Electronic Signatures in Global and National Commerce Act (09/25/00)
- **M-01-05** Guidance on Inter-agency Sharing of Personal Data – Protecting Personal data (12/20/00)
- **M-03-19** Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (08/06/03)

*Continued on next page*
CS Legal and Regulatory References, Continued

- **FIPS PUB 31** Guidelines for Automatic Data Processing Physical Security and Risk Management (06/74)
- **FIPS PUB 46-3** Data Encryption Standard (DES); specifies the use of Triple DES (10/99)
- **FIPS PUB 48** Guidelines on Evaluation of Techniques for Automated Personal Identification (04/77)
- **FIPS PUB 73** Guidelines for Security of Computer Applications (06/80)
- **FIPS PUB 74** Guidelines for Implementing and Using the NBS Data Encryption Standard (04/81)
- **FIPS PUB 81** DES Modes of Operation (12/80)
- **FIPS PUB 83** Guideline on User Authentication Techniques for Computer Network Access Control (09/80)
- **FIPS PUB 87** Guidelines for ADP Contingency Planning (03/81)
- **FIPS PUB 102** Guideline for Computer Security Certification and Accreditation (09/83)
- **FIPS PUB 112** Password Usage (05/85)
- **FIPS PUB 113** Computer Data Authentication (05/85)
- **FIPS PUB 140-1** Security Requirements for Cryptographic Modules (01/94)
- **FIPS PUB 140-2** Security Requirements for Cryptographic Modules (06/01)
- **FIPS PUB 171** Key Management Using ANSI X9.71 (04/92)
- **FIPS PUB 180-2** Secure Hash Standard (04/95)
- **FIPS PUB 181** Automated Password Generator (10/93)
- **FIPS PUB 185** Escrowed Encryption Standard (02/94)
- **FIPS PUB 186-2** Digital Signature Standard (DSS) (01/00)
- **FIPS PUB 188** Standard Security Labels for Information Transfer (09/94)
- **FIPS PUB 190** Guideline for the Use of Advanced Authentication Technology Alternatives (09/94)
- **FIPS PUB 191** Guideline for the Analysis of Local Area Network Security (11/94)
- **FIPS PUB 196** Entity Authentication Using Public Key Cryptography (02/97)
- **FIPS PUB 199** Standards for Security Categorization of Federal Information and Information Systems (12/03)
- **FIPS PUB 201** Personal Identification Verification for Federal Employees and Contractors

CS Legal and Regulatory References, Continued

800 Series

- NIST Special Publication 800-2, Public-Key Cryptography
- NIST Special Publication 800-3, Establishing a Computer Security Incident Response Capability (CSIRC)
- NIST Special Publication 800-4A, Security Considerations in Federal Information Technology Procurements
- NIST Special Publication 800-5, A Guide to the Selection of Anti-Virus Tools and Techniques
- NIST Special Publication 800-6, Automated Tools for Testing Computer System Vulnerability
- NIST Special Publication 800-7, Security in Open Systems
- NIST Special Publication 800-8, Security Issues in the Database Language SQL
- NIST Special Publication 800-9, Good Security Practices for Electronic Commerce, Including Electronic Data Interchange
- NIST Special Publication 800-10, Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls
- NIST Special Publication 800-11, The Impact of the FCC’s Open Network Architecture on NS/EP Telecommunications Security
- NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook
- NIST Special Publication 800-13, Telecommunications Security Guidelines for Telecommunications Management Network
- NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems
- NIST Special Publication 800-15, Minimum Interoperability Specification for PKI components (MISPC), Version 1
- NIST Special Publication 800-17, Modes of Operation Validation System (MOVS): Requirements and Procedures
- NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems
- NIST Special Publication 800-19, Mobile Agent Security

Continued on next page
<table>
<thead>
<tr>
<th>NIST Special Publications (continued)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NIST Special Publication 800-20</strong>, Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures</td>
<td></td>
</tr>
<tr>
<td><strong>NIST Special Publication 800-21</strong>, Guideline for Implementing Cryptography in the Federal Government</td>
<td></td>
</tr>
<tr>
<td><strong>NIST Special Publication 800-22</strong>, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications</td>
<td></td>
</tr>
<tr>
<td><strong>NIST Special Publication 800-23</strong>, Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products</td>
<td></td>
</tr>
<tr>
<td><strong>NIST Special Publication 800-25</strong>, Federal Agency Use of Public Key Technology for Digital Signatures and Authentication</td>
<td></td>
</tr>
<tr>
<td><strong>NIST Special Publication 800-26</strong>, Security Self Assessment Guide for Information Technology Systems</td>
<td></td>
</tr>
<tr>
<td><strong>NIST Special Publication 800-27</strong>, Engineering Principles for IT Security</td>
<td></td>
</tr>
<tr>
<td><strong>NIST Special Publication 800-28</strong>, Guidelines on Active Content and Mobile Code</td>
<td></td>
</tr>
<tr>
<td><strong>NIST Special Publication 800-29</strong>, A Comparison of the Security Requirements of Cryptographic Modules in FIPS 140-1 and 140-2</td>
<td></td>
</tr>
<tr>
<td><strong>NIST Special Publication 800-30</strong>, Risk Management Guide for Information Technology Systems</td>
<td></td>
</tr>
<tr>
<td><strong>NIST Special Publication 800-31</strong>, Intrusion Detection Systems (IDS)</td>
<td></td>
</tr>
<tr>
<td><strong>NIST Special Publication 800-32</strong>, Introduction to Public Key Technology and the Federal PKI Infrastructure</td>
<td></td>
</tr>
<tr>
<td><strong>NIST Special Publication 800-33</strong>, Underlying Technical Models for Information Technology Security</td>
<td></td>
</tr>
<tr>
<td><strong>NIST Special Publication 800-34</strong>, Contingency Planning Guide for Information Technology Systems</td>
<td></td>
</tr>
<tr>
<td><strong>NIST Special Publication 800-35</strong>, Guide to IT Security Services (Draft)</td>
<td></td>
</tr>
<tr>
<td><strong>NIST Special Publication 800-36</strong>, Guide to Selecting IT Security Products</td>
<td></td>
</tr>
<tr>
<td><strong>NIST Special Publication 800-38A</strong>, Recommendation for Block Cipher Modes of Operation - Methods and Techniques</td>
<td></td>
</tr>
<tr>
<td><strong>NIST Special Publication, 800-38B</strong>, Recommendation for Block Cipher Modes of Operation: the RMAC Authentication Mode</td>
<td></td>
</tr>
</tbody>
</table>

*Continued on next page*
CS Legal and Regulatory References, Continued

- NIST Special Publication, 800-38C, Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality
- NIST Special Publication 800-40, Procedures for Handling Security Patches
- NIST Special Publication 800-41, Guidelines on Firewalls and Firewall Policy
- NIST Special Publication 800-42, Guideline on Network Security Testing
- NIST Special Publication 800-44, Guidelines on Securing Public Web Servers
- NIST Special Publication 800-45, Guidelines on Electronic Mail Security
- NIST Special Publication 800-46, Security for Telecommuting and Broadband Communications
- NIST Special Publication 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Devices
- NIST Special Publication 800-50, Building an Information Technology Security Awareness and Training Program
- NIST Special Publication 800-51, Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme
- NIST Special Publication 800-53, Security Controls for Federal Information Systems
- NIST Special Publication 800-53A, Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems
- NIST Special Publication 800-55, Security Metrics Guide for Information Technology Systems
- NIST Special Publication 800-60, Guide for Mapping Information and Information Types to Security Objectives and Risk Levels
- NIST Special Publication 800-61, Computer Security Incident Handling Guide
- NIST Special Publication 800-63, Recommendation for Electronic Authentication

Continued on next page
CS Legal and Regulatory References, Continued

USDA Policies & Regulations

- DR 3140-2, USDA Internet Security Policy
- DR 3300-1, Telecommunications & Internet Services & Use
- DR 3410-1, Information Collection Activity
- DR 3080-1, Records Disposition
- DM 3500, USDA Cyber Security Manual
- OCIO Web Farm Physical Security Standards, Policies & Procedures
- Director Central Intelligence Directive (DCID) 1/21; DCID 6/3, Secure Compartmented Information Facility Construction Specifications

Miscellaneous

- DOD Directive 8500.1 Information Assurance (10/02) [http://www.dtic.mil/whs/directives/]
- Common Criteria for Information Technology Security Evaluation (Ver. 2.1) (08/99) [http://csrc.nist.gov/cc/ccv20/ccv2list.htm]
- Federal CIO Council, Securing Electronic Government (01/01) [http://www.cio.gov]