| **eb-2021-00898** |  |
| --- | --- |

|  |  |
| --- | --- |
| Document Date: | 12/01/2021 |
| To: | INCITS Members  |
| Reply To: | Deborah J. Spittle |
| Subject: | Public Review and Comments Register for the Adoption of: |
| **Due Date:** | **The public review is from December 10, 2021, to February 8, 2022.** |
| Action: | The InterNational Committee for Information Technology Standards ([INCITS](http://www.incits.org/)) announces that the subject-referenced document(s) is being circulated for a 60-day public review and comment period. Comments received during this period will be considered and answered. Commenters who have objections/suggestions to this document should so indicate and include their reasons. All comments should be forwarded not later than the date noted above to the following address: INCITS Secretariat/ITI1101 K Street NW - Suite 610 Washington DC 20005-3922Email: comments@standards.incits.org (preferred)*This public review also serves as a call for patents and any other pertinent issues (copyrights, trademarks). Correspondence regarding intellectual property rights may be emailed to the INCITS Secretariat at* *patents@itic.org**.* |

|  |  |
| --- | --- |
| ISO/IEC 10118-1:2016/AM1:2021[202x] | Information technology - Security techniques - Hash-functions - Part 1: General - Amendment 1: Padding methods for sponge functions |
| ISO/IEC 10118-2:2010/COR1:2011[202x] | Information technology - Security techniques - Hash-functions - Part 2: Hash-functions using an n-bit block cipher - Technical Corrigendum 1 |
| ISO/IEC 11770-3:2015/AM1:2017[202x] | Information technology - Security techniques - Key management - Part 3: Mechanisms using asymmetric techniques - Amendment 1: Blinded Diffie-Hellman key agreement |
| ISO/IEC 13888-2:2010/COR1:2012[202x] | Information technology - Security techniques - Non-repudiation - Part 2: Mechanisms using symmetric techniques - Technical Corrigendum 1 |
| ISO/IEC 18033-2:2006/AM1:2017[202x] | Information technology - Security techniques - Encryption algorithms - Part 2: Asymmetric ciphers - Amendment 1: FACE |
| ISO/IEC 18033-3:2010/AM1:2021[202x] | Information Technology - Security Techniques - Encryption Algorithms - Part 3: Block Ciphers - Amendment 1: SM4 |
| ISO/IEC 18367:2016[202x] | Information technology - Security techniques - Cryptographic algorithms and security mechanisms conformance testing |
| ISO/IEC 20009-2:2013[202x] | Information Technology - Security Techniques - Anonymous Entity Authentication - Part 2: Mechanisms Based On Signatures Using A Group Public Key |
| ISO/IEC 20009-4:2017[202x] | Information technology - Security techniques - Anonymous entity authentication - Part 4: Mechanisms based on weak secrets |
| ISO/IEC 20085-1:2019[202x] | IT Security techniques - Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules - Part 1: Test tools and techniques |
| ISO/IEC 20543:2019[202x] | Information technology - Security techniques - Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408 |
| ISO/IEC 21827:2008[202x] | Information technology - Security techniques - Systems Security Engineering - Capability Maturity Model® (SSE-CMM®) |
| ISO/IEC 21878:2018[202x] | Information technology - Security techniques - Security guidelines for design and implementation of virtualized servers |
| ISO/IEC 27021:2017[202x] | Information technology - Security techniques - Competence requirements for information security management systems professionals |
| ISO/IEC 27031:2011[202x] | Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity |
| ISO/IEC 27034-1:2011/COR1:2014[202x] | Information technology - Security techniques - Application security - Part 1: Overview and concepts - Technical Corrigendum 1 |
| ISO/IEC 27034-1:2011[202x] | Information technology - Security techniques - Application security - Part 1: Overview and concepts |
| ISO/IEC 29150:2011/COR1:2014[202x] | Information technology - Security techniques - Signcryption - Technical Corrigendum 1 |
| ISO/IEC 29192-1:2012[202x] | Information technology - Security techniques - Lightweight cryptography - Part 1: General |
| ISO/IEC 9797-3:2011/AM1:2020[202x] | Information technology - Security techniques - Message Authentication Codes (MACs) - Part 3: Mechanisms using a universal hash-function - Amendment 1 |
| ISO/IEC 9798-4:1999/COR1:2009[202x] | Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function - Technical Corrigendum 1 |
| ISO/IEC 9798-4:1999/COR2:2012[202x] | Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function - Technical Corrigendum 2 |