InterNational Committee for Information Technology Standards (INCITS)
Secretariat: Information Technology Industry Council (ITI)
1101 K Street NW, Suite 610, Washington, DC 20005
www.INCITS.org

eb-2014-00404

Document Date: 6/13/2014

To: INCITS Members

Reply To: Rachel Porter

Subject: Public Review and Comments Register for the Reaffirmation of:

INCITS/ISO/IEC 11770-2:2008[2009], Information technology - Security techniques - Key Management - Part 2: Mechanisms using symmetric techniques

INCITS/ISO/IEC 11770-3:2008[2009], Information technology - security techniques - Key Management - Part 3: Mechanisms using asymmetric techniques

INCITS/ISO/IEC 10116:2006/COR1:2008[2009], Information technology - Security Techniques - Modes of operation for an n-bit block cipher - CORRIGENDUM 1

INCITS/ISO/IEC 9798-3:1998[2009], Information technology - Security techniques _ Entity authentication - Part 3: Mechanisms using digital signature techniques

INCITS/ISO/IEC 9798-4:1999[R2009], Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function (2nd edition)

INCITS/ISO/IEC 13888-1:2009[2009], Information technology - Security techniques - Non-repudiation - Part 1: General

INCITS/ISO/IEC 14888-2:2008[2009], Information technology - Security techniques - Digital signatures with appendix - Part 2: Integer factorization based mechanisms

INCITS/ISO/IEC 14888-3:2006/COR 2:2009[2009], Information technology - Security Techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms -- CORRIGENDUM 2

INCITS/ISO/IEC 14888-3:2006/COR1:2007[2009], Information technology - Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms - CORRIGENDUM 1

INCITS/ISO/IEC 10118-1:2000[R2009], Information technology - Security techniques - Hash-functions - Part 1: General

INCITS/ISO/IEC 10118-3:2004[R2009], Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions

INCITS/ISO/IEC 10118-3:2004/AM1:2006[2009], Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-function 8 (SHA-224) AMENDMENT 1

INCITS/ISO/IEC 15946-1:2008/COR 1:2009[2009], Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 1: General - CORRIGENDUM 1

INCITS/ISO/IEC 18028-4:2005[R2009], Information technology - Security techniques - IT network security - Part 4: Securing Remote Access

INCITS/ISO/IEC 18032:2005[R2009], Information technology - Security techniques - Prime number generation

INCITS/ISO/IEC 18014-1:2009[2009], Information technology - Security techniques - Time stamping services - Part 1: Framework

INCITS/ISO/IEC 19772:2009[2009], Information technology - Security techniques - Authenticated encryption

Due Date: **The public review is from June 27, 2014 – August 11, 2014**

Action: The InterNational Committee for Information Technology Standards (INCITS) announces that the subject-referenced document(s) is being circulated for a 45-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/ITI
1101 K Street NW - Suite 610
Washington DC 20005-3922
Email: comments@itic.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.