WORLD TRADE ORGANIZATION

G/TBT/N/VNM/239

25 October 2022

(22-7997)

Page: 1/2

Committee on Technical Barriers to Trade

Original: English

NOTIFICATION

The following notification is being circulated in accordance with Article 10.6

1.	**Notifying Member:** VIET NAM **If applicable, name of local government involved (Article 3.2 and 7.2):**
2.	**Agency responsible:** Viet Nam Government Information Security Committee (VGISC) Add: 105 Nguyen Chi Thanh street – Dong Da district - Hanoi, Vietnam Tel: (+84) 24.38344382 **Name and address (including telephone and fax numbers, email and website addresses, if available) of agency or authority designated to handle comments regarding the notification shall be indicated if different from above:** National Agency of Cryptography and Information Security (NACIS) Add: 23 Nguy Nhu Kon Tum street - Thanh Xuan district - Hanoi, Vietnam Tel: (+84) 24.37756896 Fax: (+84) 24. 37756896 Email: info@nacis.gov.vn Website: http://nacis.gov.vn
3.	**Notified under Article 2.9.2 [X], 2.10.1 [ ], 5.6.2 [ ], 5.7.1 [ ], 3.2 [ ], 7.2 [ ], other:**
4.	**Products covered (HS or CCCN where applicable, otherwise national tariff heading. ICS numbers may be provided in addition, where applicable):** 8471 - Automatic data processing machines and units thereof; magnetic or optical readers, machines for transcribing data onto data media in coded form and machines for processing such data, not elsewhere specified or included.
5.	**Title, number of pages and language(s) of the notified document:** The draft National technical regulation on cryptographic technical specifications used in civil cryptography products under data storage security products group (18 pages, in Vietnamese); (18 page(s), in Vietnamese)
6.	**Description of content:** This draft national technical regulation prescribes the limits of cryptographic technical characteristics of civil cryptographic products using in secutiry of non-state-secrets information. This draft technical regulation applies to organizations and individuals involve in trading and using civil cryptographic products to protect non-state-secrets information.
7.	**Objective and rationale, including the nature of urgent problems where applicable:** Quality requirements

8.	**Relevant documents:** QCVN 12:2022/BQP "*National technical regulation on cryptographic technical specifications used in civil cryptography products under IP security products group with IPsec and TLS*". TCVN 11367-3:2016 (ISO/IEC 18033-3:2010) "*Information technology – Security techniques – Encryption algorithms – Part 2: Block ciphers"*. TCVN 12213:2018 (ISO/IEC 10116:2017) "*Information technology – Security techniques – Modes of operation for an n-bit block ciphers*". TCVN 12853:2020 (ISO/IEC 18031:2011 With amendment 1:2017) "*Information technology - Security techniques - Random bit generation*". TCVN 11816 (ISO/IEC 10118) "*Information technology - Security techniques – Hash-functions – Part 3: Dedicated hash-functions*". TCVN 11495-1:2016 (ISO/IEC 9797-1:2011) "*Information technology - Security techniques – Message Authentication Codes*". ISO/IEC 27040:2015 "*Information technology – Security techniques – Storage security*". National Institute of Standards and Technology, FIPS 186-4 "*Digital Signature Standard (DSS)*", July 2013. National Institute of Standards and Technology, FIPS 180-4 "*Secure Hash Standard (SHS)"*, August 2015. National Institute of Standards and Technology, FIPS 202 *"SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions",* August 2015. National Institute of Standards and Technology, Special Publication 800-38E "*Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices*", January 2010. Internet Engineering Task Force, "*IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices"*, October 2018. [RFC7801]: "*GOST R 34.12-2015: Block Cipher "Kuznyechik""*, Internet Engineering Task Force (IETF), March 2016. [RFC 5832]: "*GOST R 34.10-2001: Digital Signature Algorithm"*, Internet Engineering Task Force (IETF), March 2010. [RFC 7091]: "*GOST R 34.10-2012: Digital Signature Algorithm"*, Internet Engineering Task Force (IETF), December 2013. [RFC 4868]: "*Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec*", Internet Engineering Task Force (IETF), May 2007. [RFC 9106]: "*Argon2 Memory-Hard Function for Password Hashing and Proof-of-Work Applications*", Internet Engineering Task Force (IETF), September 2021.
9.	**Proposed date of adoption:** 1 June 2023 **Proposed date of entry into force:** 1 July 2023
10.	**Final date for comments:** 60 days from notification
11.	**Texts available from: National enquiry point [ ] or address, telephone and fax numbers and email and website addresses, if available, of other body:** https://members.wto.org/crnattachments/2022/TBT/VNM/22_7197_00_x.pdf