Wednesday, September 19, 2018 at 8:59 AM

From: ICANN Global Support <noreply-globalsupport@icann.org>
Date: Wednesday, September 19, 2018 at 8:59 AM
Subject: Notice to TMDB Users - Upcoming TMDB Maintenance

Dear ICANN Trademark Database User,

As part of ICANN's commitment to security and stability, ICANN will be enhancing the security configuration on the Trademark Database (TMDB) interfaces. These changes will be effective in the production environment for the TMDB as of **10 December 2018**. To ensure contracted parties can prepare for these changes, the TMDB Operational Testing & Evaluation (OT&E) systems will be available for validation and testing beginning on **10 October 2018**. We strongly recommend that contracted parties begin testing their systems as soon as possible.

The new settings for the OT&E systems are provided below:

The Transport Layer Security (TLS) implementation on the following URLs: https://ry.marksdb.org and https://tmcnis.org will be updated as follows:

- Only TLS v1.2 will be supported.
- Only the following ciphers will be permitted:
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

If you have questions, please contact ICANN's Global Support Center by email.

Best regards,

ICANN Global Support Center