AGENCY CONTACT MEMORANDUM #2022-0503

TO: **Agency IT Leadership, Technical Contacts**

FROM: **David Carter, Chief Information Security Officer**

DATE: **May 3, 2022**

SUBJECT: **Transport Layer Security 1.2 Sunset July 22, 2022**

Transport Layer Security (TLS) is an industry standard for secure communications based on security certificates. The current version of TLS is 1.3. TLS versions below 1.2 were deprecated in 2020 due to weakness in the encryption mechanisms that could allow data exposure.

The primary remaining concern with this deprecation is with the enterprise BigIP F5 appliances that all agencies leverage for load balancing, proxying and other purposes. While we have reviewed the usage reports to coordinate with impacted agencies, there may be other impacts that are not apparent on these point in time reports for things like periodic processing. Agencies will need to review all applications that rely on TLS for communications, especially those that rely on the enterprise F5 appliances, to ensure that they support the current standards. Due to the weaknesses in older TLS versions, it is important that agencies identify any dependence on the deprecated versions of TLS and bring these current to provide the best protection around the integrity and confidentiality of Commonwealth data.

Should agencies identify applications that are incapable of utilizing TLS 1.2 or higher by July 22, 2022, agencies may request an exemption through the established security exemption process in the COT ServiceNow ticketing system using the "F085 Other Requests" in the service catalogue. Otherwise as of July 22, 2022, we will no longer support these deprecated versions.

Should you need any additional information please contact David Carter via email at davidj.carter@ky.gov.