CYBERSECURITY SITUATIONAL AWARENESS ADVISORY

February 22, 2022

Stakeholders:

All Texas Counties, County IT staff, and their related technology and service providers

Summary:

Recent and ongoing developments between the United States and Russia, regarding Ukraine, has the potential to create new and heightened cyber attacks against U.S. government, U.S. agencies, local governments, and other critical targets. Russian state-sponsored cyber actors have been actively targeting U.S. contractors from at least January 2020 through February 2022 (US-CERT Alert AA22-047A). An increased cyber threat could result in local governments coming into the crosshairs of these cyber threat actors.

We highly encourage all Texas counties, IT staff and their partners to review their current cyber posture, evaluate their cyber detection and response readiness, be mindful of suspicious activity, and review your cyber incident response plan.

Resources:

- U.S. National Cyber Awareness System – alerts, analysis reports, current activity, bulletins and more
- Joint Cybersecurity Advisory, February 16, 2022: Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology
- Cybersecurity and Infrastructure Security Agency (CISA): Russia Cyber Threat Overview and Advisories
- US-CERT National Cyber Awareness System – mailing lists and feeds for timely information about security topics and threats

TAC Risk Management Pool Cyber Liability Members:

If you suspect that your county may have been impacted by a cyber attack, please remember to reach out to us to report this is as soon as possible. Please call Andrea Beard at 512-745-0253 or report a claim via email at U.S.SpecialtyComplexClaims@sedgwick.com

Texas Association of Counties
County Information Resources Agency

Texas Association of Counties
Risk Management Pool