KEN PAXTON
ATTORNEY GENERAL OF TEXAS

January 3, 2022

Ms. Kathryn Thiel
Counsel for the North Texas Municipal Water District
Lloyd Gosselink Rochelle & Townsend, P.C.
816 Congress Avenue, Suite 1900
Austin, Texas 78701

OR2022-00104

Dear Ms. Thiel:

You ask whether certain information is subject to required public disclosure under the Public Information Act (the "Act"), chapter 552 of the Government Code. Your request was assigned ID# 923336.

The North Texas Municipal Water District (the "district"), which you represent, received a request for five points of information related to cybersecurity and ransomware during a stated time period. You state the district will release some information to the requestor. You claim the submitted information is excepted from disclosure under sections 552.101 and 552.139 of the Government Code. We have considered the claimed exceptions and reviewed the submitted information.

Initially, we note the requestor seeks only five points of information related to cybersecurity and ransomware during the stated time period. The district has submitted information that contains information beyond the requested information. Thus, the portions of the submitted documents that contain information beyond the requested information are not responsive to the present request. This ruling does not address the public availability of any information that is not responsive to the request, and the district is not required to release such information in response to this request.

Section 552.139 of the Government Code provides, in relevant part:

> (a) Information is excepted from [required public disclosure] if it is information that relates to computer network security, to restricted information under Section 2059.055 [of the Government Code], or to the design, operation, or defense of a computer network.

> (b) The following information is confidential:
>
> > (1) a computer network vulnerability report;
> >
> > (2) any other assessment of the extent to which data processing operations, a computer, a computer program, network, system, or system interface, or software of a governmental body or of a contractor of a governmental body is vulnerable to unauthorized access or harm, including an assessment of the extent to which the governmental body's or contractor's electronically stored information containing sensitive or critical information is vulnerable to alteration, damage, erasure, or inappropriate use; [and]
> >
> > . . .
> >
> > (4) information directly arising from a governmental body's routine efforts to prevent, detect, investigate, or mitigate a computer security incident, including information contained in or derived from an information security log.

Gov't Code § 552.139(a), (b)(1)-(2), (4). Section 2059.055 of the Government Code provides, in pertinent part:

> (b) Network security information is confidential under this section if the information is:
>
> > (1) related to passwords, personal identification numbers, access codes, encryption, or other components of the security system of a governmental entity;
> >
> > (2) collected, assembled, or maintained by or for a governmental entity to prevent, detect, or investigate criminal activity; or
> >
> > (3) related to an assessment, made by or for a governmental entity or maintained by a governmental entity, of the vulnerability of a network to criminal activity.

Id. § 2059.055(b). You state the information at issue "relates to an assessment of the vulnerabilities of the [d]istrict's telecommunications and computer network and security, and details measures the [d]istrict has employed or plans to employ to protect [the district's] system." Additionally, you state the information at issue "includes information directly arising from the [d]istrict's routine efforts to prevent, detect, investigate, and respond to a cyber-attack or security breach." You assert release of the information at issue "would provide confidential network security information, including information related to vulnerabilities to the [d]istrict's technology networks[.]" Based upon your representations and our review, we find section 552.139 is applicable to some of the information at issue.

Accordingly, the district must withhold the information we marked under section 552.139 of the Government Code.[1] However, we find you have failed to demonstrate any of the remaining responsive information relates to computer network security, or to the design, operation, or defense of a computer network as contemplated by 552.139(a), consists of a network vulnerability report or assessment as contemplated by section 552.139(b), or relates to restricted information under 2059.055. Therefore, the district may not withhold any of the remaining responsive information under section 552.139.

Section 552.101 of the Government Code excepts from public disclosure "information considered to be confidential by law, either constitutional, statutory, or by judicial decision." *Id.* § 552.101. Section 552.101 encompasses information protected by chapter 418 of the Government Code. As part of the Texas Homeland Security Act (the "HSA"), sections 418.176 through 418.182 were added to chapter 418 of the Government Code. These provisions make confidential certain information related to terrorism. Section 418.181 of the Government Code provides the following:

> Those documents or portions of documents in the possession of a governmental entity are confidential if they identify the technical details of particular vulnerabilities of critical infrastructure to an act of terrorism.

Id. § 418.181; *see also id.* § 421.001(2) (defining "critical infrastructure" to include all public or private assets, systems, and functions vital to security, governance, public health and safety, economy, or morale of state or nation). The fact that information may relate to a governmental body's security concerns does not make the information *per se* confidential under the HSA. *See* Open Records Decision No. 649 at 3 (1996) (language of confidentiality provision controls scope of its protection). Furthermore, the mere recitation by a governmental body of a statute's key terms is not sufficient to demonstrate the applicability of a claimed provision. As with any exception to disclosure, a governmental body asserting one of the confidentiality provisions of the HSA must adequately explain how the responsive records fall within the scope of the claimed provision. *See* Gov't Code § 552.301(e)(1)(A) (governmental body must explain how claimed exception to disclosure applies).

You state the information at issue consists of "information relating to the [d]istrict's computer network and network security, including preparations and coverage regarding potential cybersecurity attacks." We understand you to assert, and we agree the district's computer network is critical infrastructure for purposes of section 418.181. *See generally id.* § 421.001. You assert release of the information at issue "would provide specific information to potential terrorists showing the exact policies and procedures in place to secure the [d]istrict's telecommunications and computer network, and such information could be used to impair operations and threaten [d]istrict cybersecurity management capabilities, as well as provide access to data related to the location and detailed operations of critical infrastructure, within the [d]istrict and could potentially be used in acts of terrorism." Based upon these representations and our review, we find you have

[1] As our ruling is dispositive, we need not address the remaining argument against disclosure of this information.

demonstrated release of some of the information at issue would identify the technical details of particular vulnerabilities of the district to an act of terrorism. Accordingly, the district must withhold the information we marked under section 552.101 of the Government Code in conjunction with section 418.181 of the Government Code. However, we find you have failed to demonstrate the remaining information at issue identifies the technical details of particular vulnerabilities of critical infrastructure for purposes of section 418.181, and the district may not withhold any portion of the remaining information at issue under section 552.101 on that basis.

In summary, the district must withhold the information we marked under section 552.139 of the Government Code. The district must withhold the information we marked under section 552.101 of the Government Code in conjunction with section 418.181 of the Government Code. The district must release the remaining responsive information.

This letter ruling is limited to the particular information at issue in this request and limited to the facts as presented to us; therefore, this ruling must not be relied upon as a previous determination regarding any other information or any other circumstances.

This ruling triggers important deadlines regarding the rights and responsibilities of the governmental body and of the requestor. For more information concerning those rights and responsibilities, please visit our website at https://www.texasattorneygeneral.gov/open-government/members-public/what-expect-after-ruling-issued or call the OAG's Open Government Hotline, toll free, at (877) 673-6839. Questions concerning the allowable charges for providing public information under the Public Information Act may be directed to the Cost Rules Administrator of the OAG, toll free, at (888) 672-6787.

Sincerely,

James M. Graham
Assistant Attorney General
Open Records Division

JMG/be

Ref: ID# 923336

Enc. Submitted documents

c: Requestor
(w/o enclosures)