Date of Hearing: April 6, 2022

ASSEMBLY COMMITTEE ON COMMUNICATIONS AND CONVEYANCE
Sharon Quirk-Silva, Chair
AB 2732 (Mullin) – As Amended March 24, 2022

SUBJECT: Emergency Telephone Users Surcharge Act: Next Generation 911

SUMMARY: This bill would require that a vendor for any Next Generation 911 (NG911) systems and subsequent technologies be based in the United States.

EXISTING LAW:

1) Establishes the Warren-911-Emergency Assistance Act, which requires every public agency to have in operation a telephone service which automatically connects a person dialing the digits "911" to an established public safety answering point (PSAP) from any communications device; requires every "911" system to include police, firefighting, emergency medical, and ambulance services. (Government Code § 53100 et seq.)

2) Requires the Office of Emergency Services (OES) to develop a plan and timeline of target dates for testing, implementing, and operating a NG911 emergency communication system, including text to 911 services, throughout California. (Government Code § 53121)

3) Sets a fee on each telephone access line, not to exceed $0.80 per access line per month, to fund the "911" emergency system overseen by the OES. (Revenue & Taxation Code § 41030)

4) Establishes the State Emergency Telephone Number Account in the General Fund, and sets the allowable expenses for those funds. (Revenue & Taxation Code § 41135 et seq.)

FISCAL EFFECT: Unknown.

BACKGROUND:

1) *California's 911 System.* The state's 911 program costs are paid from the State Emergency Telephone Number Account (SETNA) funds, which are derived from a statewide 911 surcharge on telephone customer bills. OES is required to determine the surcharge rate annually up to a statutory maximum of $0.80 percent of intrastate service charges. Existing law authorizes OES to use SETNA funds for various explicit purposes, including to pay service suppliers or communications equipment companies for costs connected to the 911 emergency phone number system. This bill would place further limitations on the use of SETNA funds, by requiring that the engineering staff of any vendor of NG911 system and subsequent technologies be based in the United States.

   NG911 is new technology that allows the public to share richer, more detailed data—such as videos, images and texts—with 911 call centers. It also enhances the ability of 911 call centers to communicate with each other and improves system resiliency.[1] Pursuant to existing law, the

[1] Understanding Next Generation 911. https://www.911.gov/project_ng911publicsafety/ems/understandingng911.html

state has been transition away from the legacy 911 system, which is based on 1970's telecommunications technology and is therefore limited in its capabilities. Because NG911 is based on digital technologies, it will provide advanced technological capabilities. However, the digital aspect of NG911 also presents new challenges like cybersecurity and reliability concerns.

COMMENTS:

1) Author's Statement. "AB 2732 aims to provide additional safeguards for the implementation and function of California's Next Generation 911 system. It will require that engineering staff for any vendor of Next Generation 911 systems and subsequent technologies be based in the United States. Requiring these service and infrastructure vendors to be based domestically allows a greater degree of oversight and ensures compliance with industry standards."

2) *NG911 cybersecurity and reliability concerns.* NG911 is a digital telecommunications system that is potentially more vulnerable to cyber-attacks and interruptions in service than the legacy 911 system. Such interruptions to the 911 system pose a threat to public safety, because the reliability and integrity of the 911 system ensures that the public has access to emergency services when they need them. In 2020, a Federal Communications Commission's (FCC) working group - the Communications Security, Reliability, and Interoperability Council - issued a report[2] warning that the 911 system has a particularly large attack surface during this transitional period. In other words, there are many concerns that system administrators must be concerned with during the transition to NG911 to ensure the integrity and reliability of the system.

   To address concerns about cybersecurity, especially foreign interference, this bill proposes that the engineering staff for any vendor of NG911 systems be based in the United States. Requiring domestic engineering staff can help ensure the integrity of the digital systems and components that support NG911.

3) *Double referral and committee jurisdiction.* This bill will be referred to the Assembly Committee on Emergency Management should it pass this committee.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

None on file

Analysis Prepared by: Emilio Perez / C. & C. / (916) 319-2637

---

[2] Communications Security, Reliability, and Interoperability Council. *Report on Security Risk and Best Practices for Mitigation in 911 Legacy, Transitions and NG911 Implementations*. https://www.fcc.gov/file/19298/download