

Horst, Rachel

From: CEER@brevardfl.gov
Sent: Monday, January 19, 2026 11:27 PM
To: Horst, Rachel
Subject: A new CEER Recommendation has been submitted as ID #2026029

Recommendation # 2026029

Dear CEER Administrator,

Speak Up Brevard Recommendation ID #2026029 has been submitted. Please login to the CEER Application to start the recommendation evaluation workflow.

Contact Information:

Group/Organization

Name Sean Gildea
Address 738 Sea Palm Ln, Satellite Beach FL 32937
Phone (774) 210-2947
Email seangildea@gmail.com
Alternate Email

Recommendation Information:

Recommendation ID 2026029
Recommendation Title Stop Full Encryption of Public Safety Radios – Restore Transparency Without Risk
Areas Affected
Department Affected SHERIFF'S OFFICE
Current problem Brevard County's full encryption of all police and fire/EMS radio channels on the new P25 system unnecessarily restricts public access to real-time emergency communications. FBI CJIS policy requires encryption only for Criminal Justice Information (CJI) like warrants or criminal histories—not routine dispatch or operations. Fire/EMS channels transmit no CJI and have no encryption requirement, yet they are fully encrypted as well. This overreach blocks residents from monitoring storms, traffic, neighborhood incidents, fires, and other events—reducing situational awareness, community trust, accountability for taxpayer-funded services, and informal public oversight. Criminals benefit from the secrecy, while law-abiding citizens lose a longstanding safety tool used safely for decades.
Recommendation Adopt a proven partial encryption approach compliant with FBI CJIS and used successfully by agencies nationwide and in Florida: keep main police dispatch and fire/EMS channels unencrypted for routine operations, while encrypting only dedicated talkgroups for Criminal Justice Information (CJI) like warrants or sensitive queries which can also be handled via mobile data terminals. Benefits: - Fully satisfies FBI

CJIS requirements without risking access to critical databases. - Restores real-time public awareness of routine police dispatch, fires, storms, traffic, and incidents—enhancing community safety and situational awareness for residents. - Boosts trust, accountability, and engagement, aligning with Brevard's Home Rule Charter focus on open government and citizen input. - Protects responders' sensitive data (e.g., officer safety, personal info) while allowing monitoring of non-sensitive routine calls—preventing unnecessary secrecy that benefits criminals more than citizens. This common-sense balance prioritizes both security and transparency—it's the right choice to better serve Brevard residents.

Attachments

No Documents were attached.

Please do not reply to this e-mail, as it will go to an unmonitored mailbox.



BOARD OF COUNTY COMMISSIONERS

TO: Jim Liesenfelt, County Manager

THRU: Matt Wallace, Public Safety Director

FROM: John Scott, Emergency Management Director

SUBJ: Citizen Efficiency and Effectiveness Recommendation #2026029

CEER #2026029, titled Stop Full Encryption of Public Safety Radios – Restore Transparency Without Risk, was received by the County from Sean Gildea.

Citizen Statement:

Brevard County's full encryption of all police and fire/EMS radio channels on the new P25 system unnecessarily restricts public access to real-time emergency communications. FBI CJIS policy requires encryption only for Criminal Justice Information (CJI) like warrants or criminal histories—not routine dispatch or operations. Fire/EMS channels transmit no CJI and have no encryption requirement, yet they are fully encrypted as well.

This overreach blocks residents from monitoring storms, traffic, neighborhood incidents, fires, and other events—reducing situational awareness, community trust, accountability for taxpayer-funded services, and informal public oversight. Criminals benefit from the secrecy, while law-abiding citizens lose a longstanding safety tool used safely for decades.

Citizen Recommendation:

Adopt a proven partial encryption approach compliant with FBI CJIS and used successfully by agencies nationwide and in Florida: keep main police dispatch and fire/EMS channels unencrypted for routine operations, while encrypting only dedicated talkgroups for Criminal Justice Information (CJI) like warrants or sensitive queries which can also be handled via mobile data terminals.

Benefits:

- Fully satisfies FBI CJIS requirements without risking access to critical databases.
- Restores real-time public awareness of routine police dispatch, fires, storms, traffic, and incidents—enhancing community safety and situational awareness for residents.
- Boosts trust, accountability, and engagement, aligning with Brevard's Home Rule Charter focus on open government and citizen input.
- Protects responders' sensitive data (e.g., officer safety, personal info) while allowing monitoring of non-sensitive routine calls—preventing unnecessary secrecy that benefits criminals more than citizens.



BOARD OF COUNTY COMMISSIONERS

This common-sense balance prioritizes both security and transparency—it's the right choice to better serve Brevard residents.

Staff Analysis:

While Emergency Management's 800MHz Division provides and manages the backbone equipment for the Brevard Public Safety Radio system, it is each Law Enforcement and Fire Agency that makes the decision to encrypt or not.

What is encryption:

The conversion of radio transmissions into secure signals using digital keys to ensure only authorized radios can receive protected information.

Why implement encryption:

Advances in technology have made it easier for criminals and potential terrorist to gain immediate access to sensitive public safety communications, putting the first responder community at greater risk

Examples of sensitive/protected information include:

- Tactical information that could jeopardize law enforcement operations
- Details of ongoing investigations and surveillance
- Protected health information and Personally Identifiable Information (PII); crucial for reducing response times when transporting patients to medical centers
- Disaster incident response information

Federal requirement for encryption:

The FBI CJIS (Criminal Justice Information Services) Security Policy mandates strict encryption standards for Land Mobile Radio (LMR) systems that transmit Criminal Justice Information (CJI)

- **Risk of non-compliance:** Agencies can lose access to CJIS systems if standards are not met
- **Mandatory Encryption:** Dissemination of CJI over LMR systems must be encrypted to protect sensitive data from interception. This requirement is outlined in Section 5.10.1.2.1 - Encryption for CJI in Transit, and Section 5.13.1 - Wireless Communications Technologies of the CJIS Security Policy
- **Advanced Encryption Standards (AES):** Required for public safety agencies using CJIS data for activities such as conducting records checks, verifying criminal histories, and tracking criminal activity

Which channels are encrypted:

- Only law enforcement, fire, and EMS channels



BOARD OF COUNTY COMMISSIONERS

- Non-sensitive channels such as Public Works and Space Coast Area Transit remain unencrypted

What about partial encryption?

Emergency response is simply too dynamic of an environment for certain law enforcement, fire, or EMS channels to be encrypted, while others are not

- **Fast-moving operations:** Law enforcement, fire, and EMS often need to share information instantly, making it hard to predict which calls will require protection
- **Time-critical switching:** Expecting first responders to toggle between encrypted and unencrypted channels is neither effective nor efficient
- **Interoperability limits:** When an unencrypted channel patches with an encrypted one, the secure data becomes exposed, defeating the value of encryption

Regional Perspective:

- Encryption of law enforcement, fire, and EMS channels enables secure, seamless interoperability across agencies, improving emergency response
- Majority of Brevard's neighboring counties have already implemented encryption for their Public Safety Radio systems

Alternative methods for residents to stay informed:

- **PulsePoint** – Free public safety app providing real-time visibility into active incidents (fires, medical calls, traffic crashes), residents can download and follow local agencies
- **AlertBrevard** – Location-based notifications for severe weather, missing persons, boil water notices, etc., residents can sign up at <https://www.brevardfl.gov/EmergencyManagement/AlertSignup>
- **Brevard EOC Texts** – Text service for countywide notifications on evacuations, sheltering, prescribed burns, launches, etc., residents can sign up by texting "BrevardEOC" to 888777
- **Social media** (Facebook, X, Nextdoor) – Agencies share real-time updates, preparedness information, community notices, residents can join the platform and follow official accounts

Staff Recommendation

It is recommended that the Board of County Commissioners reject CEER #2026029 because Brevard County has limited authority and the recommendation does not enhance the effectiveness or efficiency of County government as required by Home Rule Charter.