Horst, Rachel

From: CEER@brevardfl.gov
Sent: Thursday, January 1, 2026 5:54 PM
To: Horst, Rachel
Subject: A new CEER Recommendation has been submitted as ID #2026005

Recommendation # 2026005

Dear CEER Administrator,

Speak Up Brevard Recommendation ID #2026005 has been submitted. Please login to the CEER Application to start the recommendation evaluation workflow.

Contact Information:

Group/Organization	
Name	Daniel Ellery
Address	1595 Rainsville Road Southeast, Palm Bay FL 32909
Phone	(321) 427-7242
Email	danielellery2000@gmail.com
Alternate Email	danielellery2000@gmail.com

Recommendation Information:

Recommendation ID	2026005
Recommendation Title	Publis Service Radio Encryption
Areas Affected	
Department Affected	PUBLIC SAFETY GROUP
Current problem	Radio encryption has significantly reduced transparency within your county by limiting public access to information that was once readily available through open radio communications. In the past, citizens, journalists, and community watchdogs could monitor police and emergency channels to stay informed about ongoing incidents and local safety concerns. However, with encryption, these communications are now restricted to authorized personnel, making it difficult for the public to verify official reports or understand how local authorities are responding to emergencies. While encryption is often justified as a measure to protect sensitive information and officer safety, its widespread use has created a barrier between public agencies and the communities they serve, fostering perceptions of secrecy and reducing accountability.
Recommendation	I would reccomend removing the encryption of the radios within our county so that our citizens can trust that our public servats are out the doing the due diligence of serving and protecting. This will allow the citizens of Brevard to fully trust out public servants.
Attachments	No Documents were attached.

Emergency Management Department
1751 Huntington Lane
Rockledge, FL 32955

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 #2026005

CEER #2026005, titled Publis Service Radio Encryption, was received by the County from Daniel Ellery.

Citizen Statement:
Radio encryption has significantly reduced transparency within your county by limiting public access to information that was once readily available through open radio communications. In the past, citizens, journalists, and community watchdogs could monitor police and emergency channels to stay informed about ongoing incidents and local safety concerns. However, with encryption, these communications are now restricted to authorized personnel, making it difficult for the public to verify official reports or understand how local authorities are responding to emergencies. While encryption is often justified as a measure to protect sensitive information and officer safety, its widespread use has created a barrier between public agencies and the communities they serve, fostering perceptions of secrecy and reducing accountability.

Citizen Recommendation:
I would reccomend removing the encryption of the radios within our county so that our citizens can trust that our public servats are out the doing the due diligence of serving and protecting. This will allow the citizens of Brevard to fully trust out public servants.

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.

BOARD OF COUNTY COMMISSIONERS

Emergency Management Department
1751 Huntington Lane
Rockledge, FL 32955

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
- 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

Emergency Management Department
1751 Huntington Lane
Rockledge, FL 32955

BOARD OF COUNTY COMMISSIONERS

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 #2026005 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.