

Caution: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Sent: 11/18/2025 4:28:11 PM
From: Lily Ho <lily.ho@flocksafety.com>
To: "Wendy Stratton"
Cc: "Mark" , "Edward"
Bcc:
Importance: Normal
Subject: Re: FW: Benicia Must Reconsider Its Flock Safety Deployment
Attachments [image604200.png](#) , [image724539.png](#) , [image324275.png](#)
:
 , [image611335.png](#) , [image438156.png](#) , [image074009.png](#)
 , [image158946.png](#) , [image189917.png](#) , [image585058.png](#)
 , [image473993.png](#) , [image109081.png](#) , [image347389.png](#)

Thanks, Wendy. I'm ready. :)

On Tue, Nov 18, 2025 at 3:59 PM Wendy Stratton Monahan <WMonahan@ci.benicia.ca.us> wrote:

Lily,

Please be prepared to speak to the vulnerability of the system to hacking.



Wendy Stratton Monahan
Senior Management Analyst / PD PIO
Police Department
O: 707-746-4306

WMonahan@ci.benicia.ca.u
s
www.ci.benicia.ca.us/police



From: Mark Menesini <MMenesini@ci.benicia.ca.us>
Sent: Tuesday, November 18, 2025 3:54 PM
To: Wendy Stratton Monahan <WMonahan@ci.benicia.ca.us>
Subject: FW: Benicia Must Reconsider Its Flock Safety Deployment



Mark Menesini
Police Chief
Police Department
O: [707-746-4262](tel:707-746-4262)

[MMenesini@ci.benicia.ca.u](mailto:MMenesini@ci.benicia.ca.us)
[s](http://www.ci.benicia.ca.us/police)
www.ci.benicia.ca.us/police



Mario: Do we still have under contract a cyber security consultant?

I watched the Video and the majority doesn't address the use and major issues other communities have experienced. My question to The Chief would be about the concerns related to the vulnerability and security of our systems from hacking?



Sent from my iPhone

“Life is what happens when you’re busy making other plans,” John Lennon



Terry Scott
Council Member
Elected Official
O: 707-746-4213
TScott@ci.benicia.ca.us
www.ci.benicia.ca.us
f i y i n

City Hall is closed on alternating Fridays. Learn more about closures [here](#).

Begin forwarded message:

From: [REDACTED]
Date: November 16, 2025 at 10:49:15 AM PST
To: Steve Young <SYoung@ci.benicia.ca.us>, Lionel Largaespada <LLargaespada@ci.benicia.ca.us>, Trevor Macenski <TMacenski@ci.benicia.ca.us>, Terry Scott <TScott@ci.benicia.ca.us>, Kari Birdseye <Kbirdseye@ci.benicia.ca.us>, Mario Giuliani <MGiuliani@ci.benicia.ca.us>, Mark Menesini <MMenesini@ci.benicia.ca.us>
Subject: Benicia Must Reconsider Its Flock Safety Deployment

Caution: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Benicia’s City Council should urgently reconsider its reliance on Flock Safety surveillance devices. Independent security research into the same ecosystem of Flock hardware deployed nationwide reveals systemic vulnerabilities that place public data, city infrastructure, and law-enforcement operations at risk—not hypothetically, but demonstrably.

The whitepaper documents **51 security findings** across Flock’s gunshot detection units, license plate readers, and AI compute boxes. Many are **critical**, including:

- **Disabled Secure Boot** on multiple devices, allowing attackers to load malicious firmware and gain persistent control (e.g., CVE-2025-47819).
- 2. **Exposed debug interfaces** such as UART, JTAG, and Android Debug Bridge, enabling shell access or full system compromise with minimal skill.
- 3. **Hardcoded Wi-Fi credentials** and automatic connection behavior, allowing attackers to impersonate access points and intercept traffic.
- 4. **Unauthenticated administrative API endpoints** and multiple paths to **remote code execution**, including wireless attacks across devices.
- 5. **Unencrypted storage** of sensitive recordings, logs, and cryptographic secrets—including API keys and authentication tokens.

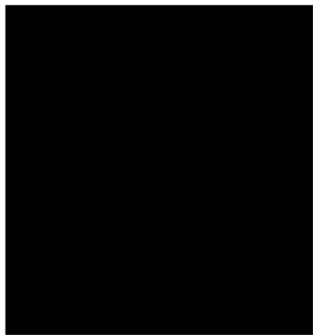
6. Flock license plate readers operating on **Android Things 8.1**, a long-abandoned, end-of-life OS with no security updates.

These issues are not edge cases—they are systemic design and hardening failures. They expose Benicia to risks of data breaches, evidence tampering, operational disruption, and legal liability. Deploying devices with known critical vulnerabilities—many carrying CVE identifiers—does not meet any reasonable security standard for systems that monitor the public or support police operations.

Before expanding or renewing any Flock contract, Benicia must demand independent verification of remediation, transparent risk assessments, and a clear plan to eliminate these security failures. Public safety technology must be secure to be trustworthy—and today, Flock’s ecosystem simply is not.

The Whitepaper can be found here and a video outlining the findings is below
<https://zenodo.org/records/17584876>

<https://www.youtube.com/watch?v=uB0gr7Fh6lY>



Public Records Exemptions

Enclosed please find a copy of the response documents for your public records request. The following information is provided to explain the process employed to review and produce the response documents.

Reason	Description	Pages
--------	-------------	-------