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:	11/17/2025 10:06:16 AM
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:	image505918.png , image042445.png , image775613.png , image674458.png , image570395.png , image185847.png

---

Hi Wendy,
Thank you for sending this. We appreciate the care your community has put into ensuring Benicia is safe from vulnerabilities.
We have addressed these issues here.
These are not material vulnerabilities, and both severity and likelihood to be exploited are low. The exploitation of these vulnerabilities require physical access to a device and knowledge of device debugging. If a person was able to gain physical access to the device (which is typically placed on a pole several feet above normal height), they would still not be able to gain access to footage, as the data is only stored for a very limited time duration on the device following its transmission to the cloud. None of these vulnerabilities affect our cloud platform, where the vast majority of all evidence and metadata is stored.

This device in this whitepaper was not connected to the cloud and to the best of our knowledge not customer installed, so the security is akin to factory settings. It's like looking at an iPhone before it is connected to iCloud. Once our devices are connected to Flock Safety updates are received.

Flock secures data in accordance with industry requirements, including encryption using AES-256, as validated by the company's ISO 27001 compliance certification. As our customers have

come to expect, Flock continues to prioritize their security by continuously evaluating the security of devices and resolving vulnerabilities in accordance with potential risk to customer environments.
Please feel free to send this information to [redacted]
Thank you,
Lily

On Mon, Nov 17, 2025 at 8:59 AM Wendy Stratton Monahan <WMonahan@ci.benicia.ca.us> wrote:

> Please see the email below from one of our community members that is opposed to FLOCK, and who will most likely be in attendance at the meeting on Thursday. Can you please review the information he has emailed directly to City Council and be prepared to speak to his concerns?
>
> Thanks.

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

Subject: Benicia Must Reconsider Its Flock Safety Deployment

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