January 9, 2025

To the Iowa Department of Public Safety:

I am writing to formally notify the Department of another active security incident involving the unauthorized dissemination of Criminal Justice Information (CJI), undermining the integrity of the NCIC system and the criminal justice system in Iowa.

This incident again involves Flock Group, Inc. (dba "Flock Safety") and arises from a set of security failures distinct from previously reported violations. I am reporting this violation directly to the Department, because the Department previously confirmed it does not receive security notifications from its vendor, Flock, nor track public security disclosures.

Yesterday, NexaNet.ai published findings regarding a critical vulnerability in the Flock ecosystem, “53 Times Flock Safety Hardcoded the Password for America's Surveillance Infrastructure.” The article[1] describes a vulnerability through which attackers can “mint” credentials and gain access to critical components of the Flock system, writing:

> The exposed API key granted access to the common mapping layer where all Flock Safety applications converge: camera inventories, mobile units, detection outputs, hotlists, search geometries, drone telemetry, Raven analytics, officer-accessible views, and Flock911 incidents.

The author indicates findings were disclosed to Flock on November 13, 2025, but the vulnerability remained unaddressed as of January 7, 2025. This period would have been covered by my earlier Iowa Open Records Act request, for which DPS indicated it had received no notifications from either Flock or any Contracting Government Agency (CGA).

[1] https://nexanet.ai/blog/53-times-flocksafety-hardcoded-the-password-for-americas-surveillance-infrastructure

The apparent nature and severity of the incident suggest Iowa CGAs were required to notify the CSA/CSO and the FBI. Separately, as a Flock customer and CGA itself, DPS's CSO or LASO had a duty to notify the FBI. The Department also has a statutory duty under Iowa Code Chapter 692 to enforce that chapter's provisions on intelligence and surveillance data.

In addition to the previously requested actions, I ask the Department to:

- Direct Iowa agencies to immediately suspend their use of the Flock system, including FlockOS, Flock911, Nova, Raven, LPR, and any other services that have been or may have been compromised.
- Treat this as an "Information Spillage" event under CJISSECPOL, and initiate the mandatory incident response capability to assess the scope of any data loss.
- Order the preservation of all vendor and sub-vendor logs related to the compromised ArcGIS software to investigate the scope and prevent spoliation of evidence.
- Should investigation reveal that information on identifiable individuals has been exposed through a security breach, provide notice to the affected individuals consistent with the Department's obligations under Iowa Code § 715C.2.

Sincerely,

Hendrik van Pelt
PO Box 98
Guttenberg, IA 52052
hcvp@pm.me

CC: Rusty Ringler, Bureau Chief & CSO
Catherine Lucas, General Counsel
FBI Information Security Officer
FBI CJIS Audit Team