



KATHLEEN JENNINGS
ATTORNEY GENERAL

DEPARTMENT OF JUSTICE
820 NORTH FRENCH STREET
WILMINGTON, DELAWARE 19801

CIVIL DIVISION: (302) 577-8400
CRIMINAL DIVISION: (302) 577-8500
FAMILY DIVISION: (302) 577-8400
FRAUD DIVISION: (302) 577-8600
DIVISION OF CIVIL RIGHTS & PUBLIC TRUST: (302) 577-5400
FAX: (302) 577-2610

Office of the Attorney General of the State of Delaware

Attorney General Opinion No. 26-IB53

September 9, 2026

Via Email

Jason Steagall
jason@steagall.net

RE: FOIA Petition Regarding the City of Dover

Dear Mr. Steagall:

We write in response to your correspondence alleging that the City of Dover violated Delaware's Freedom of Information Act, 29 *Del. C.* §§ 10001-10008 ("FOIA"). We treat your correspondence as a Petition for a determination pursuant to 29 *Del. C.* § 10005 of whether a violation of FOIA has occurred or is about to occur. For the reasons set forth below, we determine that the City violated FOIA by failing to meet its burden to demonstrate that camera locations were properly withheld under the intelligence file exemption. However, we find no violation with respect to the denial of access to the Network Audit Report.

Background

In August 2026, you submitted a FOIA request to the City seeking various records related to the City of Dover's Flock Safety license plate camera system, including the contracts, invoices, number and location of the cameras, "Network Audit [R]eport" for the last twelve months, Flock Safety external agency sharing configuration, and current policies.¹ On August 10, 2026, the City responded by producing several responsive records, with redactions for privacy concerns, including contracts, invoices, use policy, and Flock Safety external sharing list. The City denied your request for documents regarding the camera locations pursuant to the exemption for intelligence files compiled for law enforcement purposes, the disclosure of which could constitute an endangerment to public welfare and security at the local, state, or national level; the City stated

¹ Petition.

that this “determination is based on an ongoing security issue involving the tampering of FLOCK cameras at locations throughout the United States.”² The City noted that the number of cameras, as identified in the agreement, would be provided. The City also denied access to the Network Audit Report that you requested, asserting the report was considered part of investigatory files under Section 10002(o)(3) and criminal files and records under Section 10002(o)(4). This Petition followed.

In the Petition, you contend that the City improperly refused to produce the locations of the license plate cameras and the Network Audit Report. For the location of the cameras, you point out that the external sharing list indicates that the City shares access with more than a thousand law enforcement agencies across two dozen states, and a search result identifies the camera that captured each hit. You point out that the cameras are in plain view. Additionally, you state the records show that City shares a running master list of camera locations with the City’s planning and electric departments. You argue that as these camera locations are disclosed to outside parties, they cannot constitute secret intelligence files.

The Petition alleges that the Network Audit Report logs who has searched the camera system and why. You believe this report is a system-generated log of each search, date and time, user, user’s agency, and as such, you do not believe it would be part of an investigatory or criminal file, but an administrative accountability record. You note that the request explicitly stated you would accept the report with the license plate query terms redacted, and without plate numbers, the only remaining information would describe the official conduct of government users.

On August 19, 2026, the City, through its legal counsel, replied to the Petition (“Response”). The City included the affidavit of the Administrative Division Commander in support of its Response. The City states that “License Plate Readers (“LPR”) manufactured by Flock Safety record vehicle sightings at a specific place and time, capture license plates and vehicle characteristics, help authorized users find relevant vehicle evidence and provide leads for law enforcement investigators to assess alongside other evidence.”³ The City states that the cameras are vulnerable to widespread vandalism, and the City has experienced this vandalism. The City argues that the camera locations are part of intelligence files, the disclosure of which could cause an endangerment to local welfare and security. The Administrative Division Commander attests that disclosure of the camera locations, which are critical elements to intelligence gathering, would expose those cameras to likely damage and destruction. The City asserts that the affidavit, clear that the locations of the Flock LPR cameras “are intelligence matters used for law enforcement purposes inasmuch as the location of the cameras are determined by a deliberative process by the Police Department to identify locations where criminal activity may be likely to occur.”⁴ The Division Commander attests that the City’s policy indicates that the cameras are designed to be placed in areas surrounding recent crimes, areas where intelligence indicates criminal activity is

² *Id.*

³ Response, p. 1.

⁴ *Id.*, p. 4.

likely to occur, and near critical infrastructure sites, potential targets of subversive groups, or areas of a sensitive nature.

In addition, the City argues that the Network Audit Reports are exempt, noting that this license plate reader program is used as an investigative lead, as stated in its policy and that the data captured is only for law enforcement purposes. The City attests that the searches must include an investigative purpose, a specific case number, and explain the reason for the search; thus, because the searches are only conducted on existing cases and this investigative information must be included, the reports are part of the law enforcement investigatory and criminal files that are exempt.

Discussion

Delaware's FOIA law "was enacted to ensure governmental accountability by providing Delaware's citizens access to open meetings and meeting records of governmental or public bodies, as well as access to the public records of those entities."⁵ FOIA requires that citizens be provided reasonable access to and reasonable facilities for the copying of public records.⁶ The public body has the burden of proof to justify its denial of access to records.⁷ In certain circumstances, a sworn affidavit may be required to meet that burden.⁸

The City asserts that the camera locations were properly withheld under Section 10002(o)(5), which exempts "intelligence files compiled for law-enforcement purposes, the disclosure of which could constitute an endangerment to the local, state or national welfare and security." The City presents sworn statements that these cameras are critical to intelligence gathering operations, and disclosing the locations would expose the cameras to damage, which the City alleges could endanger welfare and security. The City does not dispute that the cameras are in plain view. While the cameras may enhance law enforcement officers' intelligence gathering abilities, it does not follow that disclosing information about plainly visible cameras could lead to the endangerment of "local, state or national welfare and security;" thus, we find that the intelligence files exemption is inapplicable here, as it is not sufficiently supported on this record.⁹

⁵ *Judicial Watch, Inc. v. Univ. of Del.*, 267 A.3d 996, 1004 (Del. 2021).

⁶ 29 Del. C. § 10003(a).

⁷ 29 Del. C. § 10005(c).

⁸ *See Judicial Watch, Inc.*, 267 A.3d at 1008-1012.

⁹ *See ACLU of Massachusetts v. Massachusetts State Police*, C.A. No. 2384CV25060 (Mass. Super. Ct. Sept. 2, 2026) (determining that the Massachusetts' security exemption does not preclude disclosure of the camera locations, noting as part of this analysis that the cameras are plainly visible; the public has access to crowdsourced websites with the cameras' locations; and the potential for increased vandalism does not make the locations exempt without this public safety showing).

We find a violation with respect to the failure to disclose the location of the cameras in plain view and recommend that the location of those cameras be disclosed.

For the Network Audit Report, the request states that this report consists of a system-generated log of the searches the police conducted, including the date/time, searching user, query parameters, and network searched. The City asserts that this report is exempt under the investigatory files exemption and criminal files and records exemption because, as demonstrated by the Division Commander's attestations, each search requires a user to input an investigative purpose, case number, and reason to conduct a search. This search information therefore would be part of a civil or criminal law enforcement investigation file and exempt under Section 10002(o)(3). Thus, based on the City's sworn representations, we find no violation with respect to the City's withholding of this report pursuant to Section 10002(o)(3).

Conclusion

For the foregoing reasons, we conclude that the City violated FOIA by failing to meet its burden to demonstrate that the camera locations were properly withheld under the intelligence file exemption. However, we find no violation with respect to the denial of access to the Network Audit Report.

Very truly yours,

/s/ Dorey L. Cole

Dorey L. Cole
Deputy Attorney General

Approved:

/s/ Patricia A. Davis

Patricia A. Davis
State Solicitor

cc: Daniel A. Griffith, City Solicitor