Gmail

Cadhla McBride <admin@transparentlawenforcement.com>

FOIL Appeal – FOIL #25-673 (Denial under POL §87(2)(i))

1 message

Cadhla McBride <admin@transparentlawenforcement.com> Sat, Feb 7, 2026 at 5:51 PM
To: Lisa Santillo <LSantillo@greeceny.gov>, Ivana Casilio <icasilio@greeceny.gov>

Records Appeal Officer Lisa Santillo,

I am appealing the denial of my FOIL request, FOIL #25-673.

Background

- Original request submitted: December 3, 2025 (email to Town Clerk/RAO Ivana Casilio).
- Denial issued: January 8, 2026, citing POL §87(2)(i) (information technology security), with no additional record-specific explanation.

Request at issue (FOIL #25-673)
My request sought records identifying and documenting the data systems used by the Greece Police Department ("GPD") and/or maintained by the Town of Greece, GPD, or Monroe County 911 on behalf of GPD, including:

1. RMS identification: vendor/product/version/module list; contracts/agreements/licensing; statements of work; user manuals/admin guides; internal documentation describing use.
2. RMS data tables/field dictionaries: data dictionary/schema/field list/table list (table names, field names/definitions/data types; required vs optional); configuration documents showing enabled modules.
3. CAD/dispatch system information (Monroe County 911): CAD system used; documentation describing call types, disposition codes, narrative/remarks fields, status codes; Greece-specific codes/categories if applicable.
4. CAD field definitions/codebooks: call type/disposition/signal/status codes; any specialized codes for communication needs/disability flags/communication-barrier notations; documentation on codes used for Deaf/Hard-of-Hearing encounters (if they exist).
5. RMS–CAD integration documents: how systems interface; which CAD fields populate RMS; Greece-specific CAD→RMS import configuration.
6. Data retention/archival policies: GPD/Town retention schedules for RMS/CAD; Monroe County 911 retention policies governing CAD records provided to municipal departments.

Grounds for appeal

1. The denial is conclusory and does not justify withholding the requested categories.
   POL §87(2)(i) is not a categorical exemption for "anything about an IT system." It applies only where disclosure of specific information "would jeopardize" the security of IT assets. The Town's denial provides no record-by-record (or even category-by-category) explanation of what is withheld and how disclosure would jeopardize security, and therefore does not provide a sufficient factual basis to deny the request as a whole.
2. Failure to disclose non-exempt portions as required by POL §89(3).
   Public Officers Law §89(3) expressly requires that "portions of a record which are not exempt from disclosure … shall be disclosed." The Town's blanket denial does not identify any segregable portions for release and does not explain why redaction could not address any legitimate IT-security concern.

Even if limited portions of responsive records could legitimately implicate security (e.g., passwords, access credentials/tokens, internal IP addresses, firewall rules, system hardening specifics, detailed network diagrams, vulnerability/exploit information), FOIL requires release of non-exempt material and permits targeted redactions. Many items requested here are policy-level, administrative, contractual, retention-related, or definitional records that can be disclosed with appropriate redactions rather than withheld in full.

3. Overbreadth of applying §87(2)(i) to administrative and high-level documentation.
Several request components are inherently administrative and do not reasonably "jeopardize" security when disclosed, including (for example):

- Vendor/product identification, version, and licensed module list (at least at a high level);
- Contracts, agreements, and licensing documents (with redaction of truly security-sensitive technical attachments, if any);
- Retention schedules and retention policies;
- High-level descriptions of data fields/code lists that define what categories of information are stored, without disclosing credentials or detailed security configurations.

If the Town believes any subset is sensitive, it must narrow its claim and explain why redaction cannot address the concern.

Narrowing for avoidance of doubt (without waiving rights)
To reduce any legitimate §87(2)(i) concern and expedite disclosure, I am expressly not seeking:

- passwords, passphrases, access keys, authentication tokens, API secrets;
- internal IP addresses, VPN configurations, firewall rules, or security monitoring configurations;
- vulnerability scans, penetration testing results, exploit narratives, or detailed "how to break in" guidance.

I am seeking the policy-level and administrative records described above, and field/code definitions and system documentation to understand what record types exist and what data elements are maintained.

Relief requested
I request that you:

A) Reverse the denial and direct release of responsive records; or

B) At minimum, issue a new determination that:

- identifies the responsive record categories withheld (by category, date range, and custodian),
- provides a particularized explanation for any withholding under §87(2)(i),
- releases all reasonably segregable portions with targeted redactions only where necessary, and
- states whether any records (or portions) were withheld in full and, if so, why disclosure of non-exempt portions via redaction was not feasible under POL §89(3).

If any portion is still denied, please also confirm that a copy of the appeal determination will be transmitted to the Committee on Open Government as required by POL §89(4)(a).

Please confirm receipt.

Sincerely,
Cadhla McBride
Transparent Law Enforcement
admin@transparentlawenforcement.com