From: **OGC** ogc@txcc.texas.gov
Subject: Re: Texas Public Information Act Request – City of Mount Pleasant/OpenGov Security Records and DIR Transfer
Date: September 18, 2026 at 3:28 PM
To: Kyle Moring [redacted]

Good afternoon, Mr. Moring,

Texas Cyber Command (TXCC) received your Texas Public Information Act request. TXCC searched its files and *did not* locate any responsive information.

With this correspondence your request is now fulfilled and closed. If you have any questions, please do not hesitate in contacting the Office of the General Counsel by email.

Sincerely,

TXCC
TEXAS CYBER COMMAND

Office of General Counsel
Texas Cyber Command
P: (512) 461-7993
E: ogc@txcc.texas.gov
PREVENT ★ SECURE ★ PROTECT ★ DEFEND ★ EDUCATE

From: OGC <ogc@txcc.texas.gov>
Sent: Thursday, September 3, 2026 10:56 AM
To: Kyle Moring [redacted]
Subject: Re: Texas Public Information Act Request – City of Mount Pleasant/OpenGov Security Records and DIR Transfer

Dear Requestor:

Texas Cyber Command (TXCC) is in receipt of your public information request. Your request is being processed, and all future correspondence and retrieval of any responsive information will be sent by email. We strive to promptly respond to requests for information by no later than 10 business days following TXCC's receipt of the request, excluding holidays, skeleton crew holidays, and weekends. **Please note that TXCC offices will be closed September 7, 2026, in observance of the Labor Day holiday.**

Please note that if your request was submitted after 5:00 p.m. CST Monday through Friday, during the weekend, a state or federal holiday, a state skeleton crew day, or other date on which the agency is closed, we will begin processing the request on the first business day after your submission.

Please continue to monitor your email inbox and spam folder for any correspondence or responsive information from TXCC. For information about TXCC's Public Information Policy, you may visit our website at Public Information

TXCC's Public Information Policy, you may visit our website at: Public Information Act | Texas Cyber Command.

For prompt processing of any future public information requests, you may submit by email at: ogc@txcc.texas.gov.

Sincerely,

Office of General Counsel
Texas Cyber Command
P: (512) 461-7993
E: ogc@txcc.texas.gov
PREVENT ★ SECURE ★ PROTECT ★ DEFEND ★ EDUCATE

From: Kyle Moring [redacted]
Sent: Wednesday, September 2, 2026 6:48 PM
To: OGC <ogc@txcc.texas.gov>
Subject: Texas Public Information Act Request – City of Mount Pleasant/OpenGov Security Records and DIR Transfer

You don't often get email from [redacted] Learn why this is important

Office of General Counsel:

Under the Texas Public Information Act, Chapter 552 of the Texas Government Code, I request electronic copies of the following existing records created, received, maintained, possessed, or held by or for the Texas Cyber Command from January 1, 2026 through the date of this request, including responsive records acquired or transferred from the Texas Department of Information Resources:

1. All submissions, reports, complaints, attachments, acknowledgments, intake records, tickets, case records, and related correspondence concerning cybersecurity or privacy concerns I reported involving the City of Mount Pleasant, Texas, or its OpenGov systems.
2. All records concerning my April 28, 2026 email to DIRSecurity@dir.texas.gov with the subject "THIRD-PARTY CYBERSECURITY / PRIVACY INCIDENT TIP – City of Mount Pleasant OpenGov Portal – Apparent Public SSN Exposure," including records showing its receipt, forwarding, routing, referral, assignment, transfer, review, or disposition.
3. All internal records concerning that report or the underlying security concerns, including assignments, routing records, analyst or investigator notes, assessments, findings, referrals, status updates, follow-up activities, closure records, and records sufficient to show the matter's current status or disposition.
4. All communications concerning the report or underlying concerns between Texas Cyber Command and any of the following:
    - The Texas Department of Information Resources;
    - The City of Mount Pleasant, Texas;
    - OpenGov, Inc., or its representatives;
    - Any vendor, contractor, consultant, governmental entity, or law-enforcement agency; and

- Any other person or organization notified about, consulted regarding, or involved in reviewing the reported concerns.

5. Records sufficient to identify when the report was received by or transferred to Texas Cyber Command, the office or personnel to whom it was assigned, any entity to which it was referred, actions taken in response, and whether the matter was closed, resolved, transferred, or remains pending.
6. Records concerning the transfer, migration, or custodial disposition under House Bill 150 of DIR records responsive to the foregoing categories, including relevant mailboxes, incident-reporting queues, ticketing or case-management records, shared-drive materials, and associated metadata.

Search assistance:

- **Requester/reporting party:** Kyle Douglas Moring
- **Email:** [redacted]
- **Telephone:** [redacted]
- **Original reporting date:** April 28, 2026
- **Relevant entity:** City of Mount Pleasant, Texas
- **Relevant vendor/platform:** OpenGov
- **DIR public-information request:** R004678-081926
- Relevant terms include "Kyle Douglas Moring," [redacted]" "Mount Pleasant," "City of Mount Pleasant," "OpenGov," "financial transparency," "SSN," "Social Security number," "privacy," "exposure," "incident," "vulnerability," "report," and "complaint."

I have attached copies of my April 28 incident-tip email and DIR's September 2 response directing me to Texas Cyber Command. The April 28 attachment is supplied as a search aid and does not contain any full Social Security number.

This request does not seek full Social Security numbers, the unredacted findings file, passwords, authentication tokens, exploit instructions, or technical details whose release would create a present security risk. If responsive records contain confidential or properly excepted information, please redact only that information and release all reasonably segregable portions, including dates, participants, routing information, nontechnical communications, general findings, and disposition information.

Please provide the records electronically by email. I welcome rolling production if that will permit earlier release of readily available records.

If Texas Cyber Command believes any information may be withheld, please identify the legal authority relied upon and release all non-exempt portions. If an Attorney General ruling is requested, please provide me with the required copy or redacted copy of the agency's submission.

Because these records concern the handling of a reported exposure of sensitive personal information through a public-facing municipal system, I request a waiver or reduction of charges on the ground that disclosure would primarily benefit the general public. If estimated charges will exceed $40, please provide the required written itemized estimate before incurring the charges and allow me an opportunity to narrow the request.

This is a request for existing records, not a request that Texas Cyber Command create information, answer legal questions, or perform legal research.

Please confirm receipt and provide the assigned tracking number.

Respectfully,

Kyle Douglas Moring
[redacted] | [redacted]

This email originated from outside of DIR. Computer viruses can be transmitted via email attachments and links. The recipient should check this email and any attachments for the presence of viruses. Do not click any links or open any attachments unless you recognize the sender and know the content is safe. To report a suspicious email or to verify if an email is legitimate, please save the email as a file and send the file as an attachment to phish@dir.texas.gov.