Special Report
September 2019

# Criminal Justice Information Security Compliance

During an audit, we identified potential issues related to compliance with federal Criminal Justice Information Services (CJIS) Security Policy. Audit standards require that we communicate this issue in a written report.

## Summary

The City could lose access to criminal justice information because it may be violating several elements of federal information security policy, including those related to physical security and background checks. The Austin Police Department's operations would be significantly hampered if it lost access to this information, and it would also disrupt other City operations that rely on criminal justice information.

## Background

The Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Division gives entities access to criminal justice information, such as fingerprints and criminal records. Several City departments use or access CJIS information as part of their operations. For example, both the Austin Police Department (APD) and the Austin Fire Department use CJIS information for law enforcement purposes. The Human Resources Department (HRD) also uses CJIS information as part of the City's background check process. Other City departments, and even some City vendors, have access to CJIS information as well. For example, Communications and Technology Management (CTM) staff can access systems that contain CJIS information and Building Services staff maintain some of the buildings that contain CJIS information.

To ensure that criminal justice information is protected, the FBI created the CJIS Security Policy. This policy describes security measures, such as security training, data encryption, and physical security, that must be in place for entities that use or access criminal justice information.

Every City department and vendor that can access CJIS information must comply with the CJIS Security Policy. APD is responsible for ensuring compliance for most of the City.[1] CJIS Security Policy calls the person responsible for ensuring compliance the Local Agency Security Officer (LASO), and this role is currently filled by an employee in APD's Police Technology Unit.

One of the requirements of the CJIS Security Policy is that entities must undergo a compliance audit every three years. The Texas Department of Public Safety (DPS) audits APD's compliance with the CJIS Security Policy, and the FBI may also conduct compliance audits. DPS's most recent audit of APD was done in February 2019.[2]

[1] HRD does not use CJIS information for law enforcement purposes and is responsible for their own compliance with CJIS Security Policy.

[2] An HRD manager said that DPS last audited HRD in 2012.

## Finding

### The City knew about but did not address issues related to compliance with federal information security policy. Violating this policy could result in the loss of access to criminal justice information and impact critical City operations.

The City must comply with the federal information security policy to access criminal justice information maintained by the FBI. During the most recent audit in February 2019 though, DPS auditors noted several areas of noncompliance. APD staff said they reported these issues to the DPS auditors during the audit. However, prior to the audit APD staff submitted a document to DPS indicating that the City was fully compliant with the information security policy. Documentation indicates City staff were aware of issues several years before DPS's 2019 audit.

A presentation given to APD managers in 2018 noted the City had nearly failed the 2016 audit and identified several compliance issues that needed to be addressed before the 2019 audit. One of those issues related to the lack of a written agreement between APD and Building Services. This agreement was needed because Building Services staff had access to buildings with criminal justice information. Despite APD staff knowing this was an issue as early as 2017, it was not corrected and was one of the findings in DPS's 2019 audit.

DPS audits involve a limited part of City operations that use criminal justice information, which means there may be more compliance issues beyond what DPS identified in their 2019 audit. For example, an investigation by the City Auditor's Integrity Unit noted that City staff may not know the location of all criminal justice information in the City. This is a compliance risk because the City cannot ensure all criminal justice information is adequately protected if staff does not know where it is located. Additionally, during the Public Safety Dispatch Audit our office identified potential issues with background checks and security training for personnel at the Combined Transportation and Emergency Communications Center. Since criminal justice information is used at this site, these issues with background checks may create violations of the information security policy.

Continued violations of the federal information security policy could result in the City losing access to important criminal justice information maintained by the FBI. This would have a significant impact on several critical City operations.

To address these issues, the Austin Police Chief should work with the City Manager to ensure APD has the necessary support from other City departments to ensure compliance with CJIS Security Policy. Additionally, the Austin Police Chief should ensure APD fully complies with CJIS Security Policy by identifying where CJIS information exists in City operations and establishing appropriate controls necessary to protect that information.

## Scope

The project scope included the City's efforts to comply with CJIS Security Policy.

## Methodology

To complete this project, we performed the following steps:

- reviewed CJIS Security Policy;
- reviewed CJIS audits conducted by Texas DPS in 2013 and 2016;
- reviewed documentation related to the CJIS audit conducted by Texas DPS in 2019;
- reviewed information from interviews conducted by the City Auditor's Integrity Unit;
- reviewed documentation and interviews from the Public Safety Dispatch Audit; and
- interviewed CTM and APD staff.

## Project Type

This project is considered a non-audit project under Government Auditing Standards and was conducted in accordance with the ethics and general standards (Chapters 1-3).

The Office of the City Auditor was created by the Austin City Charter as an independent office reporting to City Council to help establish accountability and improve City services. We conduct performance audits to review aspects of a City service or program and provide recommendations for improvement.


**Team**
Andrew Keegan, Audit Manager
Kathie Harrison

**City Auditor**
Corrie Stokes

**Deputy City Auditor**
Jason Hadavi

**Office of the City Auditor**
**phone:** (512) 974-2805
**email:** AustinAuditor@austintexas.gov
**website:** http://www.austintexas.gov/auditor

AustinAuditor
@AustinAuditor


Copies of our audit reports are available at
http://www.austintexas.gov/page/audit-reports

*Alternate formats available upon request*