CASE STUDY

# Protecting Sensitive Police Department Data with Phishing-Resistant Multi-Factor Authentication

A 360-question data security audit conducted by a government security agency on a week's notice would be a daunting prospect for any law enforcement entity. But one police department in the southeastern U.S. passed with flying colors, thanks to identity management capabilities from RSA.

## The challenge:

Could there be a greater challenge for a local police department than learning that auditors are on the way to check for compliance with Criminal Justice Information Service (CJIS) security policies? How about learning that they'll be there within the week?

It's a development that would have left many scrambling to prepare—but for one midsized police department in the southeastern U.S., it proved to be a relatively light lift, thanks to its deployment of FIDO2 passkey from RSA.

## The solution:


RSA had worked with the police department over time to evolve their technology for securing data related to sensitive criminal justice information (CJI), starting with traditional MFA and ultimately evolving to the RSA iShield Key 2 Series, which provides phishing-resistant, passwordless authentication via hardware authenticators based on the FIPS 140-3 Level 3 standard.

As a result, a state audit that was expected to take a week to complete was over within about five hours. This also meant the police didn't need to worry about the prospect of having to dedicate extra personnel to the audit effort for a longer period—which could have left the department light on resources for the duration. That would also prove to be important shortly after the state team left, when the FBI began its own audit to check compliance with federal policies governing protection of CJI.

## The future:

The police department and the city with which it is affiliated can both look forward to continuing their exemplary status when it comes to protecting and securing sensitive data and preventing it from being breached. The department is part of one of a very small number of local municipalities deploying advanced identity management technology such as the RSA iShield Key 2 in the cloud.

Next for the police department is the continuation of its successful cloud journey with RSA, as it moves to convert from its current hybrid deployment to having identity and access management operations 100% in the cloud.

## Key Takeaways:

### Challenge

- Passing local and federal audits intended to demonstrate police department competence and capabilities for protecting sensitive data

### RSA Solution

- The RSA iShield Key 2 Series, which provides advanced multi-factor authentication, including phishing-resistant hardware-based authentication managed in the cloud

### Impact

- Law enforcement that continues to secure some of the most sensitive data in local government