# CJIS-Compliant Email Security from the Mimecast Public Sector Team

US state and municipal law enforcement organizations are required by the Federal Bureau of Investigation (FBI) to meet Criminal Justice Information Services (CJIS) Security Policy. According to the FBI policy, that means "protecting the sources, transmission, storage, and generation of Criminal Justice Information (CJI) … and by extension the hardware, software and infrastructure required to enable the services provided by the criminal justice community." But the IT and physical security requirements mandated by CJIS policy are stringent, and not just any technology vendor can meet them.

**Mimecast helps law enforcement agencies to meet CJIS requirements, keeping email data safe and avoiding non-compliance fines.**

**Key Milestones**

Mimecast has put in the time and effort, and can now demonstrate CJIS compliance:

1. Mimecast earned the "CJIS Ready" badge from Diverse Computing's CJIS ACE (Audit & Compliance Experts) consultancy, the industry's premier CJIS experts.

2. Mimecast's US-based Public Sector Support organization is staffed entirely by US personnel screened and approved by individual FBI Identity History Summary Checks. This ensures our customers' CJIS data is accessed only by properly cleared US-based personnel.

3. Mimecast Public Sector is also participating in development of the StateRAMP secure cloud procurement standards, and intends to be among the first to comply.

## CJIS ACE

The Criminal Justice Information Services (CJIS) is a division of the US FBI that sets standard for information security, guidelines and agreements aimed at protecting the Criminal Justice Information (CJI). The standards are reflected in the CJIS Security Policy, which describes the appropriate controls to protect the transmission, storage and access to data. While there is no CJIS authorization body or standardized assessment approach determining CJIS compliance, Mimecast has engaged with CJIS ACE to perform an audit of the controls within our Public Sector Grid to ensure they meet the requirements of the CJIS. This resulted in obtaining a CJIS Ready badge demonstrating that Mimecast satisfies those requirements across the 13 policies outlined in the CJIS Security Policy.

## Mimecast Email Security Complies with CJIS Security Policy

Mimecast contributes to your CJIS compliance posture by providing CJIS-Ready services in four key "Policy Areas" that are relevant to email security services:

**Personnel Security:** The entire Mimecast Public Sector US-based support team is cleared to access CJI.

**Access Control:** Our user access and authentication enable "least privilege" and other approaches required by CJIS Security Policy.

**Security Awareness Training:** Mimecast's award-winning training capabilities can be a force multiplier that builds a human firewall for detecting phishing and other dangerous emails through engaging and entertaining training videos. It delivers dramatic improvements in employee security awareness and behavior.

**Physical Protection:** Mimecast has partnered with DataBank — the premier datacenter provider to state, local and federal cloud service providers (CSPs) — to build out our new Public Sector Grid, consisting of secure cloud data centers located exclusively within the US. Multifactor authentication is required just to gain entry.

## The Mimecast Solution

Cyber threats have become far more frequent — and more sophisticated — whether the cybercriminals are seeking to steal CJI or sensitive private sector information. To protect law enforcement agencies and private enterprises alike, Mimecast implements a layered approach:

### Advanced Email Security
Defend against malware, ransomware, and credential harvesting with Mimecast email security.

### Business Continuity
Keep email flowing and the email archive accessible during a planned or unplanned email outage.

### Immutable Cloud Archive
Protect data and support compliance needs with an industry-leading cloud archive.

### Threat Remediation
Apply advanced email security and data leak prevention to all internal and outgoing email with the ability to remediate and contain the threat.

### Security Awareness Training
Turn employees into a security asset through engaging security awareness training.

### Email Encryption
Automatically encrypt messages based on the content, sender or recipient to keep data safe.