

CJIS Compliance for Google Apps:

Uncovering a Solution for
Secure Email, Document, and Video Sharing

CJIS Compliance for Google Apps:

**Uncovering a Solution for
Secure Email, Document, and Video Sharing**



I. Protecting the Data that Protects Our People

One of the most gruesome tragedies in Connecticut history might have been prevented if law enforcement could have shared criminal justice information more effectively.

In 2007, two parolees raped and murdered a mother and her two young daughters during a home invasion in Cheshire, CT. After the murders, it was discovered that a sentencing transcript, in which a judge described one of the suspects as a "[calculated, cold-blooded predator](#)," never reached the parole board.

The communication lapse that could have prevented these fatal killings, reveals the very problem that the Criminal Justice Information Services Division was developed to solve: how can government entities protect their most valuable data while keeping it easily accessible?

While this problem remains as relevant as ever, many law enforcement and criminal justice organizations still struggle to find cost-effective, compliant ways to share their most critical info. Understanding the background and requirements of CJIS is the first step toward finding a solution.



What is CJIS?

Established 15 years before the Cheshire murders, CJIS is the [largest division of the FBI](#), and comprises several departments, including the National Crime Information Center (NCIC), Integrated Automated Fingerprint Identification System (IAFIS) and the National Instant Criminal Background Check System (NICS). CJIS monitors criminal activities in local and international communities using analytics and statistics provided by law enforcement, and their databases provide a centralized source of criminal justice information (CJI) to agencies around the country.

CJIS enables millions of law enforcement and national security professionals to access and share critical criminal justice data, such as:

- Arrest reports
- Fingerprint data
- Criminal background checks
- License plate numbers
- Stolen property reports
- Protective orders
- Foreign identity information
- Sentencing and parole reports
- Body worn camera footage

Any organization with access to these databases must ensure that its employees comply with CJIS regulations. Examples of groups governed by CJIS compliance include:

- U.S. Federal Agencies dealing with CJI
- State, County, and City Police Departments
- Departments of Public Safety
- Departments of Corrections
- Offices of Attorney Generals
- Offices of the Public Defender
- Offices of the U.S. Courts
- Offices of County Sherriffs
- Government Contractors

What CJIS Requirements Affect Email and File Sharing in the Cloud?

The emergence of the Internet and cloud computing has changed data sharing drastically since CJIS formed in 1992. To guard against the growing rate and sophistication of cybersecurity threats, CJIS came up with a set of security standards for organizations, agencies, and cloud vendors.

The [policies set forth by CJIS](#) cover best practices in wireless networking, remote access, data encryption, and authentication. The guidelines for email and file sharing are rigorous, and rules around “physically secure locations” confine most organizations to on-premise systems rather than the cloud. According to [CJIS Security Policy](#), “A physically secure location is a facility, a criminal justice conveyance, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems” (5.9.1).

Building and maintaining a physically secure location requires law enforcement entities to dedicate valuable time, money, and manpower toward such safeguards as:

- Separating the location from non-secure locations via security perimeters and controls
- Issuing credentials for and maintaining lists of all personnel with location access
- Limiting access to any devices (phones, computers, tablets) capable of displaying CJI
- Controlling physical access to distribution and transmission lines within the location

“Anytime CJI is transmitted outside the boundary of a physically secure location, the data must be immediately protected via encryption.”

Perhaps even more tedious than establishing a physically secure location is facilitating CJIS compliant communications between two separate physical facilities. CJIS policy dictates that anytime “CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via [encryption]” (5.10.1.2). This means that even if an agency establishes secure CJIS control rooms on separate floors of the same building, an additional system to perform encrypted email and file exchanges between locations is necessary.

What Makes CJIS Compliance So Difficult to Achieve in the Cloud?

For states, counties, and agencies that must protect exchanges between dozens of CJI storage systems, scalable secure data transport becomes exponentially more difficult to achieve.

That’s why, in the wake of the Cheshire tragedies, the State of Connecticut set out to build its own centralized information portal to connect its [52 different information systems](#) and over [23,000 criminal justice personnel](#). However, Connecticut’s CJIS project, which remains unfinished after 7 years, [\\$52M, and a 40% budget overrun](#), highlights another glaring problem: building CJIS infrastructures entirely in-house is not financially or technically feasible for most organizations.

To combat the increased hardware, storage, and maintenance costs that highly customized email portals like Connecticut’s require, more and more organizations are relying on private third party vendors to move their CJIS communications to the cloud. In 2011, the State of Florida became the largest group to do so, migrating 115,000 employees to a cloud email system that would house both CJI and non-CJI data accessed by state personnel.



David Taylor, Florida’s CIO who oversaw the CJIS project, claimed that fixed costs and increased collaboration would make more of these government cloud migrations “[inevitable](#)” in the years to come. Taylor also mentioned how challenging these moves continue to be for organizations governed by CJIS regulations and the third-party cloud vendors that they enlist.

The FBI provides a 65-page [Cloud Computing Report](#) to help with these challenges, and even acknowledges them in its official CJIS Security Policy: “Admittedly, the existing [CJIS Security Policy] requirements may be difficult for some cloud-computing vendors due to the sheer numbers and the geographic disbursement of their personnel” (G-16). Ultimately, three limitations make cloud email and file sharing particularly tough for CJIS-bound entities:

1. Cloud vendors often struggle to meet CJIS requirements

Many of the more tedious CJIS requirements affecting government organizations also apply to the third party service providers that they enlist to meet compliance. Without added encryption, cloud vendors like Google and Microsoft must host some of their customers’ plaintext email and file content on their servers.

As a result, these companies must complete “the same screening and agreement requirements as any other private contractors hired to handle CJI” (G-17), such as “state of residency and national fingerprint-based record checks” (5.12.1.1.) for their employees.

As Taylor explains, many large vendors simply cannot make such guarantees. In Florida’s case, one vendor, Affiliated Computer Services (ACS), managed the data center that housed the state’s Microsoft Outlook Exchange email server. All 140 ACS employees working on the project—“from the architects to the person who opened cardboard boxes”—had to undergo stringent background checks, and [several employees failed](#). These workers had to be removed from the project, creating added complexities for ACS that might prohibit some vendors from bidding on CJI-related work altogether.

“Three limitations make cloud email and file sharing particularly tough for CJIS-bound entities.”

2. Many governments are reluctant to trust third-party providers with their data.

Since CJIS policy was created before the cloud existed, many government entities do not trust their ability to migrate from on-premise systems in safe, compliant ways. Richy Vaughn, IT Director of the Metropolitan Nashville Police Department, claims that it would be “[insane](#)” to house his department’s sensitive data in the cloud. He highlights the risk of third party breaches via cloud providers, as well as unintentional data leaks from offices accessing CJI remotely, as two main deterrents.

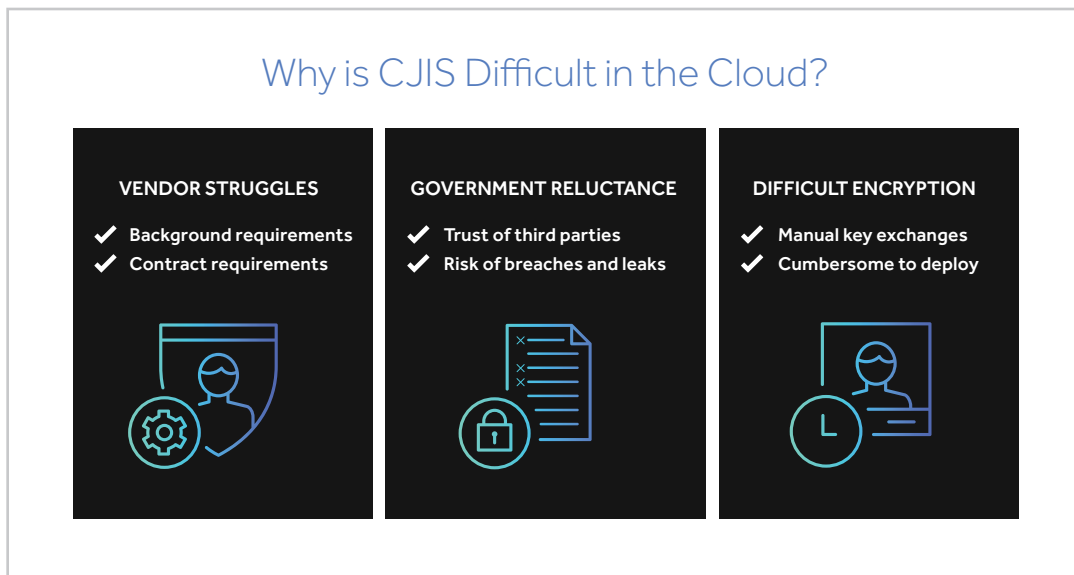
Given the emphasis on physically secure locations in CJIS policy, some law enforcement agencies will always prefer to store and manage their data entirely on-site—even if this creates painful workflows for employees and compromises quick access to CJI.

3. End-to-end encryption eliminates many complexities, but has been historically difficult to implement.

The [2012 CJIS Cloud Computing Report](#) provides a key option (in both senses of the word) for CJI transmission in the cloud that reduces the compliance burdens of third-party email and storage providers, while also preventing them from ever accessing an agency’s sensitive content. According to section G-26 of the report, “Client end-to-end encryption with cryptographic keys managed solely by law enforcement would prevent exposure of sensitive data,” and should be considered by organizations moving to the cloud.

When CJI is encrypted end-to-end, it is protected before it leaves a sender’s device or email client, and it remains encrypted until it reaches the intended recipient. Therefore, if a user shared CJI in the cloud using end-to-end encryption, that user’s cloud provider (or any third party, for that matter) would never have access to the content in unencrypted form, thus eliminating the vendor’s need to comply with background checks and other regulations affecting those who directly handle CJI.

End-to-End Encryption



[End-to-end encryption](#) can make widespread cloud adoption a reality for CJIS-covered entities, but it has traditionally required manual key exchanges that make it difficult to deploy.

This means that, for an officer to send an end-to-end encrypted email or file to an employee in another department, he would first have to retrieve a unique encryption key from that employee. The employee would also need to have the same encryption technology implemented on his device. If the officer were to lose the employee’s key for any reason, he would have to repeat the process again.

Traditional end-to-end encryption techniques alleviate many of law enforcement’s most common cloud concerns, but they are not typically well-suited to CJIS use cases.

II. A New Day for CJIS Compliance in the Cloud—Simple End-to-End Encryption

[In a 2013 article](#), Paul Rosenzweig, Senior Advisor at global security firm The Chertoff Group, reinforces end-to-end encryption's ability to eliminate longstanding issues around CJIS compliance in the cloud, and even explains what a practical solution might look like:

“To be effective, this sort of solution would need to be compatible with large cloud-services like Google Apps and Microsoft Office 365. To be scalable, these encryption solutions would need to be ‘add-on’ functions that do not require the technical cooperation, prior approval or even awareness of the cloud provider. In other words, a law enforcement agency (or any other cloud user) should be able to adopt an encryption solution without the participation of its service provider.”

Rosenzweig describes a configuration that would provide CJIS organizations all of the collaboration and cost savings of the cloud without compromising compliance or other data privacy concerns. His vision had long been unattainable, but end-to-end encryption add-ons like [Virtru](#) have now made it a reality.

Introducing Virtru End-to-End Encryption for CJIS Compliance

Virtru adds end-to-end encryption to Google Apps and Microsoft Office 365 via simple plug-ins and browser extensions. By automating the key exchanges that make traditional end-to-end encryption so difficult, Virtru simplifies CJIS compliance in the cloud in several ways:

1. Virtru's encryption meets or exceeds all CJIS requirements.

The strength of an encryption tool depends on the length of the keys used to encrypt the data being shared. Encryption keys are measured in commonly used computing units called bits. The more bits in a key, the more difficult it is to guess, and thus the safer the encrypted data is from hackers.

CJIS policy mandates a minimum of 128 bit (5.10.1.2) encryption, but Virtru exceeds these requirements by using 256-bit encryption.

For other cryptographic assurances, CJIS references existing federal standards, including those of Federal Information Processing Standard Publication 140-2, better known

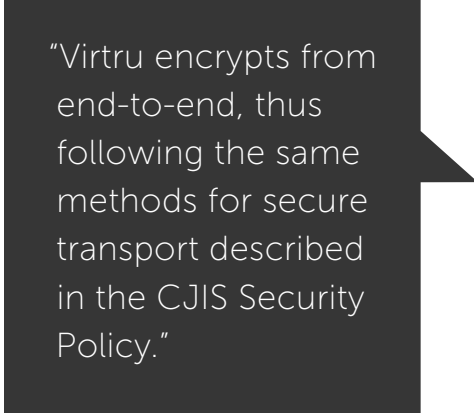
as FIPS 140-2. Issued by the National Institute of Standards and Technology, FIPS 140-2 identifies requirements for cryptographic modules, and outlines the different circumstances under which these modules could provide adequate data security.

When law enforcement employs encryption of any form, CJIS mandates that the encryption meets FIPS 140-2 standards, which Virtru's does.

2. Virtru encrypts CJI at rest and in-transit.

In order to make their customers' emails and files widely accessible, cloud providers must host this content in multiple data servers distributed across geographic locations. These servers constantly exchange CJI with each other and the employee devices that must access the content, making it difficult (if not impossible) to confine sensitive data to isolated facilities in the same way that an on-premise system would.

That's why CJI must be encrypted before it ever leaves its original location, whether on an employee's computer or a shared local database. Virtru encrypts from end-to-end, thus following the same methods for secure transport described in the CJIS Security Policy:



"Virtru encrypts from end-to-end, thus following the same methods for secure transport described in the CJIS Security Policy."

"Encryption/decryption occurs on the law enforcement controlled client prior to data entering the cloud and decryption occurs only on the client device after encrypted data is removed from the cloud service." (G-26)

Some CJI might not need to be transmitted between different servers and devices, like files housed in cloud storage platforms like Google Drive, Box, and Dropbox, or old emails that sit in a user's inbox. Even in these scenarios, CJIS policy requires that that data be encrypted via what is referred to as at-rest encryption:

"When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected via cryptographic mechanisms (encryption)." (5.10.1.2)

When Virtru encrypts CJI, the encryption remains no matter where the CJI goes (i.e., if a recipient forwards an email to another recipient), and protections persist even when the content is not travelling. As a result, users do not have to apply additional security layers to the data that has already been emailed to them or uploaded to the cloud. In locking down sensitive info from the moment it is created, end-to-end encryption provides CJIS compliance by ensuring third parties can never access the content regardless of where it ends up being stored.

3. Virtru prevents third party vendors from having to handle CJI.

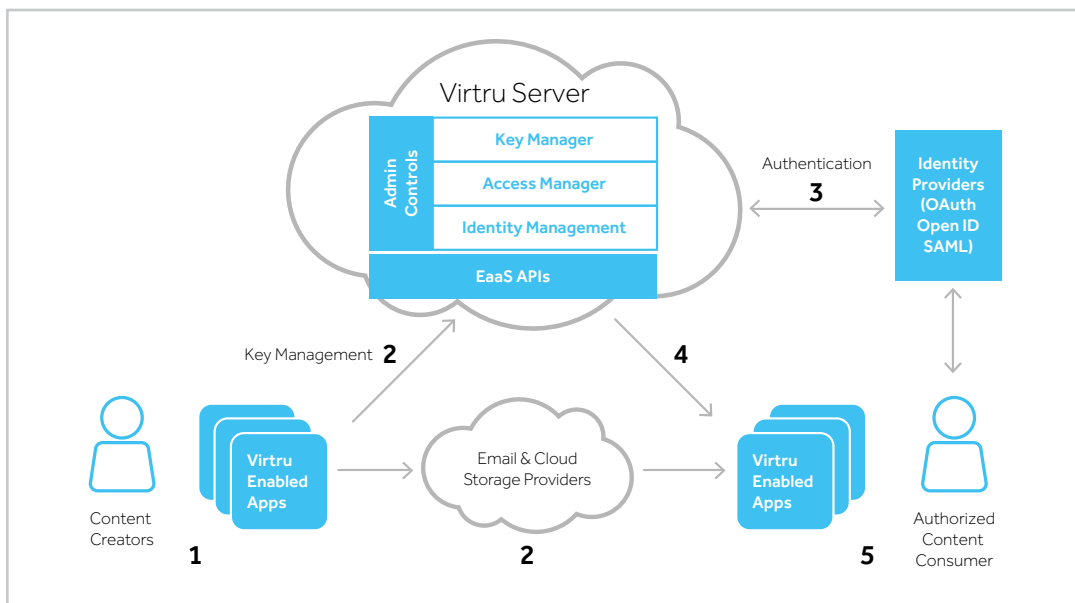
When cloud platforms cannot provide end-to-end encryption, they must manage in-transit and at rest encryption themselves for their government customers. This gives them access to unencrypted CJI, which means they must comply with some of CJIS' more stringent vendor requirements.

As CJIS Security Policy explains, "Use of cloud services without end-to-end encryption implemented by the client is [an] option that would require cloud service provider participation in the encryption of data" (G-26). In these instances, third party vendors encounter several obstacles that could make a functioning cloud system unfeasible:

- Personnel background screening and training
- Specialized Service Level Agreements (SLAs) to identify specific personnel that may have access to unencrypted CJI
- High costs and time delays due to the high degrees of technical complexity

Virtru's architecture enables customers to manage their own encryption keys, so cloud service providers never participate in the encryption of CJI. In addition, Virtru does not host any CJI on its servers (this content is stored on the cloud provider's servers in encrypted form), so Virtru never has access to the sensitive emails and files either.

Virtru Encryption Key Management Architecture



By removing the need for third party vendors to handle unprotected CJI or the required encryption of it, Virtru enables law enforcement organizations to work with cloud service providers like Google and Microsoft without the traditional bureaucratic burdens.

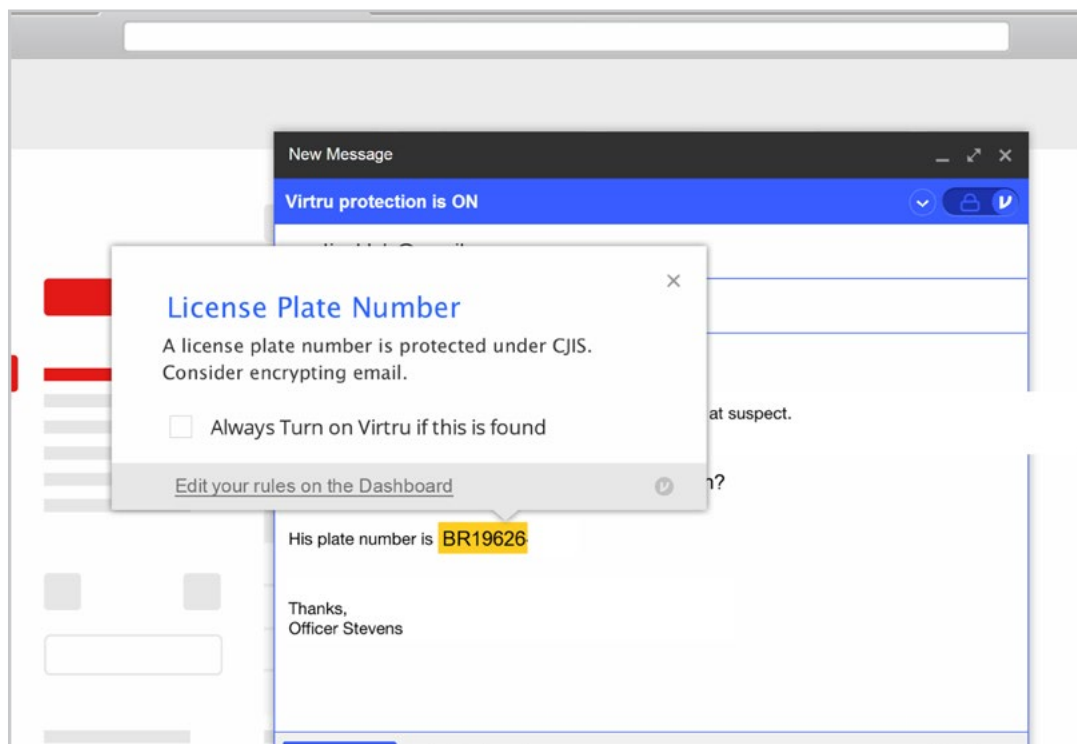
You can read more about Virtru’s technical architecture [here](#).

4. Virtru Data Loss Prevention (DLP) detects CJI before it leaves secure locations.

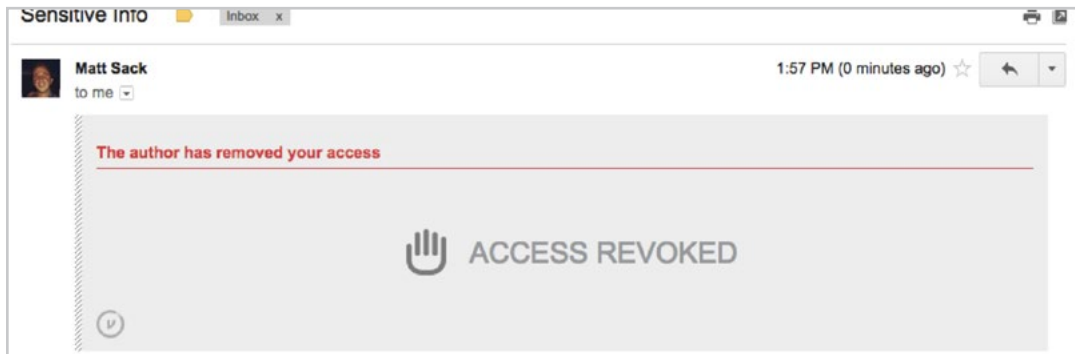
Even if an organization has implemented robust encryption protocols, it faces severe CJIS penalties anytime unauthorized access to CJI is granted. Whether a user sends an email to the wrong recipient, or accidentally uploads a sensitive file to the wrong folder, human error can easily disrupt the security posture of a cloud environment—unless Data Loss Prevention (DLP) has been implemented.

Virtru’s [DLP capabilities](#) scan emails and files before they ever leave the sender’s inbox or local folders, thus preventing CJI from ever hitting the cloud unprotected. Most DLP tools scan sensitive content after it has already travelled from the user’s device to a separate server, but Virtru enables these scans to occur on the client-side, which keeps unencrypted content out of third party control.

Virtru DLP also comes equipped with CJIS-related rule packs that can be turned on to scan emails for criminal codes, SSNs, and other CJI material. By notifying end users when they have triggered these rules and why, Virtru DLP educates individuals about CJIS compliance directly, which helps foster long-term adoption of agency policies and best practices.



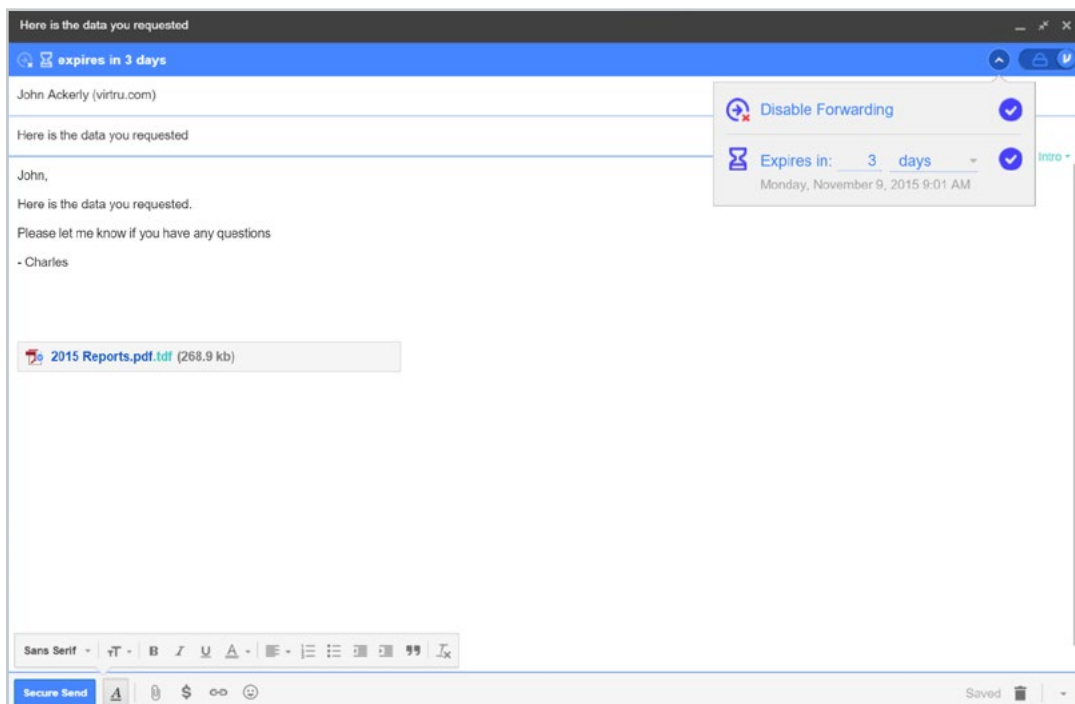
Even if you disable Virtru DLP and accidentally send CJI to the wrong recipient, Virtru gives users the ability to revoke any email or file they've sent, even after recipients have already viewed the sensitive content. These kind of granular tracking capabilities enable law enforcement organizations to take back much of the control that might otherwise get lost in the cloud.



What Does the Virtru Experience Look Like for Senders and Receivers?

Compared with legacy approaches, Virtru provides the best of security, ease of use, and persistent data control. It only takes a minute to add to your domain, and your users only have to download a simple plugin to start sharing encrypted emails and files directly from existing platforms like Gmail, Google Drive, and Microsoft Outlook.

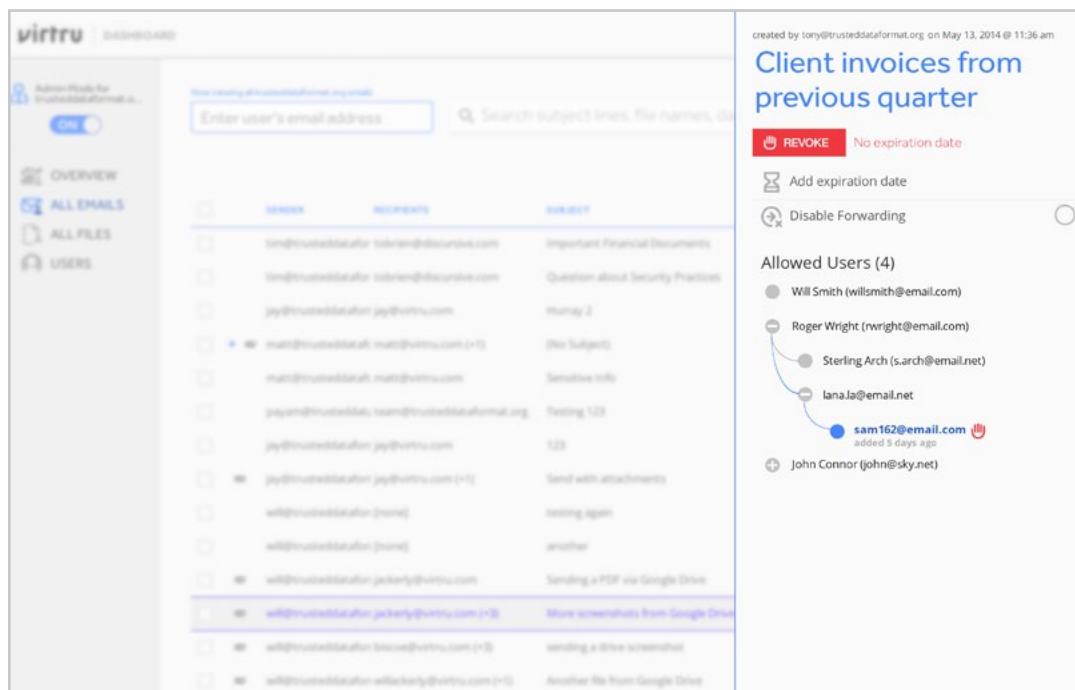
Virtru End-to-End Encryption for Gmail



Virtru End-to-End Encryption for Google Drive

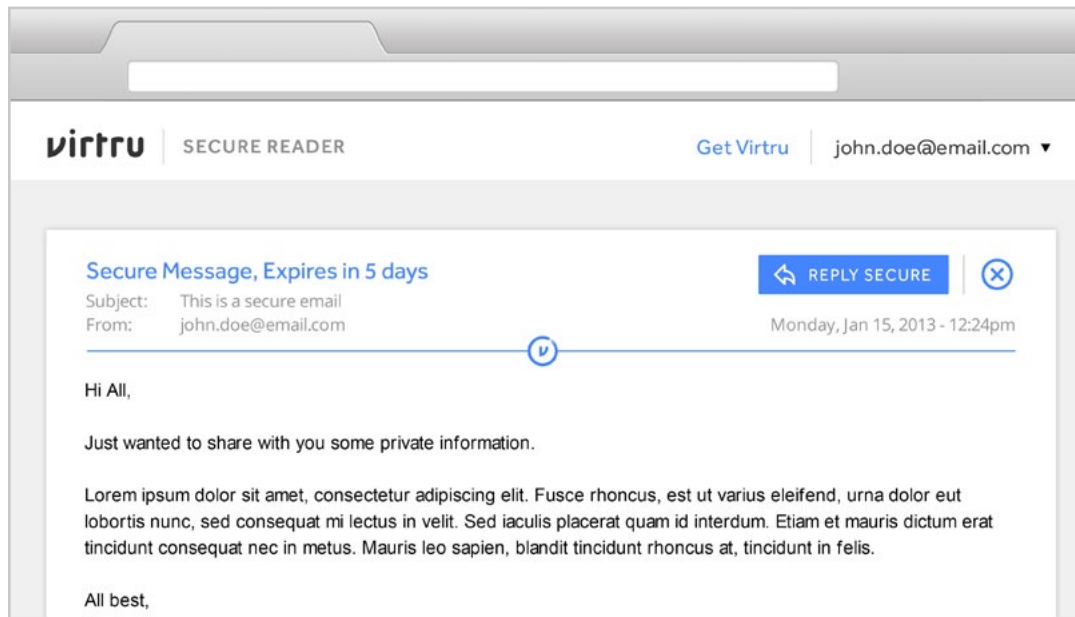


With Virtru, you can monitor data going in and out of your domain from a centralized dashboard. You can also track emails and files shared by anyone in your organization, control forwarding and revoke sensitive content at any time. It is even possible to trace where outgoing emails and files have been forwarded.



In order to ensure high adoption rates, Virtru makes the encryption process convenient for both senders and recipients. Users never have to leave their current mail platforms to send and receive encrypted email. There are no extra credentials to remember and no manual keys to exchange with recipients. To send an encrypted email or share an encrypted document, users simply click a switch, compose or upload and share as normal.

Virtru First-Time Recipient Experience (Without Virtru Installed)



CJIS Compliance for Google Apps: A Customer Success Story

With 54,000 employees scattered across 60 independent agencies, the State of Maryland is responsible for an enormous amount of data flow—much of which involves CJI. For years, individual Maryland agencies managed their own on-premise email servers via solutions like Microsoft Exchange, Novell, and even in-house platforms, as was the case in Connecticut. To reduce technical complexities and increase intra-agency collaboration, Maryland knew a unified move to the cloud was imminent.



In 2014, Maryland's state government began migrating its employees to Google Apps for Government. With Google Drive, Maryland employees were now able to access and collaborate on shared documents from various devices. With Google Apps' mobile device management, Maryland could push out new software at the enterprise level, rather than relying on individual agencies to make these updates on their own.

Despite these significant cloud benefits, 10,000 Maryland employees were unable to fully migrate to Google Apps. Personnel in the state's Department of Public Safety and Correctional Services (DPSCS) had to continue using on-premise email platforms, because they had no way to meet the end-to-end email encryption requirements of CJIS.

All of that changed in August 2015, when Maryland's DPSCS rolled out Google Apps email, integrated with Virtru encryption, to 500 users. Virtru enables these users to send CJIS compliant email directly from their inboxes. Two months later, DPSCS deployed Virtru to another 2,000 employees.

The department is evaluating Virtru as a solution for all 10,000 of its members, which would enable Maryland to move its entire email and file sharing infrastructure to Google Apps.

Not only would this full transition save Maryland significant costs by centralizing its IT needs under one platform, it would mark one of the more complete cloud migrations by a state to-date.

Cost-Effective Video Storage for Body Worn Cameras

CJIS Policy dedicates an entire section (5.8) to the storage and transmission of media. In recent years, these clauses, which mandate encryption anytime media leaves a physically secure location, have become top-of-mind for law enforcement, as the need for police body worn cameras has skyrocketed.

In light of increased public awareness of police-related violence, agencies across the country are facing pressure to implement body worn cameras for all public safety officers. These videos can be essential in assessing claims of police violence and mistreatment, but they have traditionally required massive investments in secure storage and administration for terabytes of video files.

For agencies interested in cutting these expenses by storing video footage in the cloud, Google and Virtru have developed a CJIS compliant option that can reduce costs by over \$100 per user while still meeting all search, storage, archiving, and regulatory requirements.

By integrating [Virtru's end-to-end encryption into its Google Drive product](#), Google enables law enforcement to store unlimited CJIS compliant video content with low, predictable storage costs. This solution leverages Google's fast, encrypted, fully redundant file storage architecture, as well as its robust policy engine, to impose retention periods, litigation holds, and discovery requests.

For more information on this CJIS compliant video storage solution, you can view [this webinar](#) from Google and Virtru, or [contact Virtru directly](#).



III. More Information on CJIS Cloud Transformations

Given the rate at which cloud technology continues to evolve, it is important to stay up-to-date on how these developments impact CJIS regulations. As new applications for CJI management emerge, such as the need for secure storage of body worn camera video footage, expect cloud providers and software vendors to adapt their offerings accordingly.

As thought leaders in the government compliance arena, Google and Virtru offer a valuable array of resources to help law enforcement keep pace with the ever-changing landscape of the cloud:

- **Blog Post:** [CJIS Compliance and Data Encryption – Here’s What You Need to Know](#)
- **Blog Post:** [The 5 Professions that Most Need Email Encryption Most](#)
- **Webinar:** [CJIS Compliance with Google Apps](#)
- **Webinar:** [Secure Your Org: A Practical Guide and Case Study on Email Encryption](#)
- **Webinar:** [Cost-Effective Unlimited Video Storage for Body Worn Cameras](#)
- **Case Study:** [How Virtru Shows Columbia County Employees When to Encrypt](#)
- **eBook:** [The Complete Guide to Email Encryption for Google Apps Administrators](#)

CJIS Compliance Needs Assessment Checklist

Although there are several components to CJIS compliance that are unrelated to email and file sharing, these exchanges pose some of the biggest risks for CJI leaks at an organization. As a result, it’s critical that you take inventory of your team’s best and worst data security practices.

The following checklist will help you to evaluate your organization’s need for email and file encryption and determine appropriate solutions to meet your related CJIS requirements.

Requirement	Yes or No?
Do any employees at your organization have access to CJI?	
If yes, do these employees ever share CJI via email or file sharing?	
Does a cloud provider like Google or Microsoft host email or file sharing services for those employees who have access to CJI?	
If yes, do you have CJIS SLAs in place with these providers?	
Does your cloud provider meet the standards of FIPS 140-2?	

Requirement	Yes or No?
Have you conducted criminal background checks for all employees responsible for managing the cloud services your organization uses?	
Does your cloud provider guarantee that your organization's email and file data will not leave U.S.-based servers?	
Does your organization use any type of email or file encryption?	
Is the encryption your organization uses at least 128 bit?	
Does your encryption protect files both at rest and in-transit?	
Do CJI personnel use end-to-end encryption to share sensitive data?	
Do you utilize DLP to prevent unintended users from gaining access to sensitive CJI?	
Would you prefer to use a centralized platform for all of your organization's CJI and non-CJI communications?	
Do you have a need to securely store and access vast amounts of body worn camera video footage?	

Release the Shackles of CJIS Compliance Today

Whether you are already using a cloud service like Google or Microsoft, or are just beginning to evaluate a move away from on-premise systems, [Virtru's CJIS solutions](#) for email, file sharing, and police worn body camera video footage are the easiest, most secure ways to comply with CJIS regulations in the cloud. To determine whether Virtru is right for your organization, you can:

- [Download Virtru for free](#) now and start sending securely
- [Install the Virtru for Google Apps Marketplace App](#) (if applicable) and access admin controls within minutes
- [Request a demo](#) with Virtru today

About Virtru

By combining military grade encryption, cloud-based access and controls and seamless integration with applications like Google Apps for Work and Microsoft Exchange, Virtru enables security without getting in your way. Whether for regulatory compliance like CJIS, data security, or corporate privacy, Virtru is the easiest way to protect sensitive information.

www.virtru.com
sales@virtru.com

