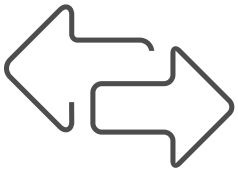
MAKING THE CASE FOR
FBI-CJIS SECURITY POLICY

VIGILANT
SOLUTIONS

MAKING THE CASE FOR FBI-CJIS SECURITY POLICY

The Federal Bureau of Investigation (FBI) created the FBI-Criminal Justice Information Services Division Security Policy (FBI-CJIS Security Policy) to provide authorized agencies with a security management structure for accessing, protecting and safeguarding Criminal Justice Information (CJI) accessed or received from the FBI-CJIS system of services. While FBI-CJIS security policy compliance is not a certification or a cyber-rubber stamp of approval from the FBI, it does provide a security framework and foundation that enables government agencies to evaluate their own networks and procedures, as well as those of private contractors, service providers and cloud providers.



For agencies evaluating third parties, FBI-CJIS compliance is not a one-way street. It requires a unique partnership between the agency customer and the contractor/vendor/cloud provider to assess the products and services.

PETE FAGAN

Pete Fagan, Vigilant Solutions' Director of Information Security and Compliance, is an expert on FBI-CJIS systems and security policy. Before working at Vigilant, Pete served as Virginia State Police's Assistant Criminal Justice Information Services Officer and consulted with federal, state and local law enforcement agencies across the U.S. as an Executive Outreach and Education Program Specialist on behalf of the FBI. As Vigilant's Director of Information Security and Compliance, Pete is responsible for working with agencies to develop and execute the necessary policies to ensure our solutions meet compliance requirements.

Pete Fagan
Director of Information Security and Compliance
E: pete.fagan@vigilantsolutions.com

UNDERSTANDING FBI-CJIS SECURITY POLICY

On February 24, 1992, the Federal Bureau of Investigation (FBI) established the Criminal Justice Information Services (CJIS) Division to consolidate fingerprint identification services, the Uniform Crime Reporting (UCR) Program, and the National Crime Information Center (NCIC) under one law enforcement support umbrella. FBI-CJIS' main purpose: to give 18,000 state, local and federal law enforcement and numerous other criminal justice and non-criminal justice agencies access to Criminal Justice Information (CJI) that FBI-CJIS maintains. To ensure the proper use of this sensitive information, the FBI-CJIS Security Policy was created to provide authorized agencies with a minimum set of security requirements for access to FBI-CJIS Division systems and to protect and safeguard CJI information once obtained from FBI-CJIS through the entire lifecycle.

The policy has become the information technology (IT) security standard accepted and adopted by these agencies whether the policy applies or not since it provides a good framework for information security.

With advances in technology since FBI-CJIS' inception, the way in which law enforcement transmits, stores, and processes CJI has changed. Part of this change now encompasses outsourcing traditional government IT tasks, software applications and data processing functions. There has also been the positive proliferation of new technologies that have significantly improved public safety and cost effectiveness. One of the fastest growing areas includes use of software applications and technologies that incorporate cloud hosting or Co-Location services for the government agency using service providers' applications, information processing or data storage.

As corporate service provider technologies have progressed in this area, it has ultimately aided law enforcement and criminal justice functions. But it is only successful when public-private partnerships are created with a trusted contractual relationship that takes into consideration and meets the requirements of the FBI-CJIS Security Policy.

To accommodate the changes to technology and government business models, the FBI-CJIS Security Policy is periodically updated to reflect evolving business models, technology, threats and improved security requirements. The Security Policy now provides guidance for agencies when engaging in private contracting IT services and considering cloud or Co-Location service providers to be FBI-CJIS compliant. As an agency considering the use of a cloud-based solution, it is crucial to know if FBI-CJIS Security Policy applies, what aspects apply, why selecting a compliant vendor is important, and how to determine that a solution is compliant.

WHAT DATA DOES FBI-CJIS SECURITY COVER?

According to the FBI-CJIS Security Policy, Criminal Justice Information (CJI) refers to all of the FBI-CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to the following categories of data sets:

1. Biometric Data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and face images.

2. Identity History Data textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.

3. Biographic Data information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.

4. Property Data information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).

5. Case/Incident History information about the history of criminal incidents.

NCIC FILE TYPES COVERED BY FBI-CJIS SECURITY POLICY

FBI-CJIS defined Criminal Justice Information also encompasses some NCIC File information. The NCIC Restricted Files require treating that sensitive information equivalent to Criminal History Record Information (CHRI). The FBI-CJIS Security Policy states, "The NCIC hosts restricted files and non-restricted files. NCIC restricted files are distinguished from NCIC non-restricted files by the policies governing their access and use. Proper access to, use, and dissemination of data from restricted files shall be consistent with the access, use, and dissemination policies concerning the Interstate Identification Index (triple - III) described in Title 28, Part 20, CFR, and the NCIC Operating Manual. The restricted files, which shall be protected as CHRI, are as follows:"

1. **Gang Files**
2. **Known or Appropriately Suspected Terrorist Files**
3. **Supervised Release Files**
4. **National Sex Offender Registry Files**
5. **Historical Protection Order Files of the NCIC**
6. **Identity Theft Files**
7. **Protective Interest Files**
8. **Person With Information (PWI) Data in the Missing Person Files**
9. **Violent Person File**
10. **NICS Denied Transactions File**

In addition, transaction control type numbers (e.g. ORI, NIC FNU, etc.) require the same protection levels when accompanied by information that reveals CJI or PII. The types of data listed above are only classified as CJI, requiring FBI-CJIS Security Policy compliance when the FBI-CJIS Division provides the data. If you, the agency, are gathering and sharing this data and it is not obtained from the FBI-CJIS Division, it is not CJI and you are NOT responsible for FBI-CJIS Policy compliance. You can require a vendor or service provider to be FBI-CJIS Security Policy compliant as a best practice even if the data does not qualify as CJI, but that is for you, the agency, to decide and negotiate in your service agreement.

However, in today's legislative and regulatory environment where a bright light is being shone on privacy rights and license plate reader technologies and data, FBI-CJIS Policy compliance provides an agency with a means of building trust. Well-documented policies and procedures show – in a tangible way – a law enforcement agency's dedication to protecting all data, whether it is personally-identifiable or not. So, while FBI-CJIS Policy compliance may not be strictly required for many cases involving PlateSearch™, FaceSearch™, and BallisticSearch™, it is "good business" to go above and beyond.

MAKE SURE YOUR DATA IS SECURE

When U.S. law enforcement, criminal justice and non-criminal justice agencies contract with an outside entity to transmit, store or process the types of CJI listed above, the agency, and their service provider, are required to comply with the FBI-CJIS Security Policy. FBI-CJIS governs how that data is handled by those accessing the information through the entirety of its life cycle.

In addition to the specific types of data that CJIS is meant to protect, the Security Policy explains in great detail the minimum security requirements for outsourcing to private contractors. The policy provides guidance and identifies requirements in thirteen policy areas. Among other things, they govern the physical and technical security, along with personnel security for those who: access or maintain the information, work-on or maintain the applications that may access the CJI and work-on or maintain the systems and telecommunication that can transmit, store or process the information. Each of these is important to evaluate.

The relevant requirements must be met before granting access or potential access to CJI and being permitted to perform those criminal justice functions on behalf of law enforcement, criminal justice or non-criminal justice agency. The central principle for outsourcing is to ensure that each aspect of the administrative, personnel, physical and technical security controls used by the private contractor software applications and cloud solution meet or exceed FBI-CJIS Security Policy requirements for authorized access to CJI. Based upon evaluation of the project, the agency needs to determine the nature of the information accessed and understand if there are some aspects of Policy compliance that are more important than others.

MINIMUM SECURITY REQUIREMENTS

Some, but not all, of the minimum requirements and security protocols to consider include:

Private Contractor User Agreements and CJIS Security Addendum:
The FBICJIS Security Addendum is a uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information is consistent with existing regulations and the FBI-CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies. All private contractors who perform criminal justice functions or have outsourced information technology functions involving FBI-CJIS shall acknowledge, via signing of the FBI-CJIS Security Addendum Certification page, and abide by all aspects of the FBI-CJIS Security Addendum and FBI-CJIS Security Policy.

Fingerprint-Based Background Checks: Authorized private contractor employees must pass a state and national fingerprint-based background check in order to be granted access to systems or physical media containing CJI data.

Auditing and Accountability: Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior. Agencies shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.

Identification and Authentication: The agency shall identify information system users and processes acting on behalf of users and authenticate the identities of those users or processes as a prerequisite to allowing access to agency information systems or services components.

Advanced Authentication Policy and Rationale: The requirement to use or not use AA is dependent upon the physical, personnel, and technical security controls associated with the user location and whether CJI is accessed directly or indirectly.

Access Control Mechanisms: One of the following must be employed: access control lists (users, groups, machines), resource restrictions (permission sets), encryption and strong key management, or application level access control.

Configuration Management - Access Restrictions for Changes: Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. The goal is to allow only qualified and authorized individuals access to information system components for purposes of initiating changes, including upgrades, and modifications.

Least Privilege: The agency shall approve individual access privileges and enforce the most restrictive set of rights/privileges needed by users for the performance of specified tasks. Logs maintained on access privilege changes are to be maintained for a minimum of one year or at least equal to the agency's retention policy, whichever is greater.

Physical Protection: Physical protection policy and procedures shall be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

System and Communications Protection and Information Integrity: Encryption (FIPS -140-2 NIST Certified): When CJI is transmitted outside the boundary of the physically secure location; the data shall be immediately protected via cryptographic mechanisms (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). It is important to note that the protocols laid out in FBI-CJIS are the minimum standards for agencies and private contractors like technology and cloud service providers to be in compliance. Agencies are free to augment or create additional standards in addition to CJIS, but may not detract from the minimum FBI-CJIS Security Policy standards if required.

DETERMINE IF A VENDOR IS COMPLIANT

In order to be in compliance, any technology provider using a cloud service that an agency attempts to make an agreement with must demonstrate compliance through an evaluation of relevant FBI-CJIS Security Policy. That part is very straight forward. However, because different state, local, and federal information security criteria may be required for different contract relationships, the variation of circumstances prevents any cloud service provider to indicate that they are FBI-CJIS Security Policy compliant nationally.

At this point in time, there is no central FBI-CJIS authorization body, no accredited pool of independent assessors, nor a standardized assessment approach to determining whether a particular solution is "FBI-CJIS compliant" within a given state or nationally. Because different state, local, and federal information security criteria may be required for different contract relationships, the variation of circumstances prevents any service provider from indicating that they are FBI-CJIS Security Policy compliant within a state or nationally. To be FBI-CJIS compliant requires an individual evaluation and assessment by the government agency that contracts for that specific technology or cloud service. It is important for an agency to have a collaborative effort with the service provider as well as the local, state and federal CJIS Information Security Officer(s) to discuss the issues surrounding the project. This process will be the only path forward for the agency to thoroughly evaluate the service provider's information and make an informed decision.

As an agency, it becomes your responsibility to determine whether a potential vendor operates in compliance with the FBI-CJIS Security Policy.

THE CJIS TOP 10 LIST

To help start that process, here are some questions to help you determine if a potential cloud services provider is up to the minimum standards set forth by the FBI:

1. What parts of the FBI-CJIS Security Policy apply to me?
2. Do the terms and conditions of the contract specify if the service provider is willing to agree to meet the requirements of the FBI-CJIS Security Policy and provide the necessary information for an evaluation? Are there parts of compliance that are negotiable?
3. Does the service provider outsource or use a third party for cloud hosting or Co-Location Services?
4. Are state and national fingerprint based background checks permitted for data hosting staff?
5. Who manages the applications and data storage and who owns the data?
6. Is data deleted as specified by the data owner?
7. Is the hosting facility on U.S. Soil and are the day-to-day managers U.S. citizens?
8. Do the terms and conditions specify if the service provider and third party hosting facility are willing to agree to FBI-CJIS style audits?
9. Does software have configurations that are flexible for Physically Secure and Physically Non-Secure Locations? Is the data encrypted: "data in transit" and "data at-rest"? Is it FIPS 140-2 NIST certified?
10. Has the service provider had any previous approvals for compliance with FBI-CJIS Security Policy? Can they provide the documentation for evaluation?

MANDATING FBI-CJIS COMPLIANCE

The FBI-CJIS Security Policy requirements serve as a good baseline for information security and can be mandated by agencies – even when not accessing CJI. On some occasions an agency may require FBI-CJIS Security Compliance for some aspects of the policy because the service provider is accessing the infrastructure that may contain CJI or provide potential access to systems that may have CJI.

As a result, some aspects of the FBI-CJIS Security Policy may not be achievable for cloud solutions, but serve to act as a best practice. For instance, if there is no direct FBI-CJIS relationship to the services of the private contractor – due to the type of data or type of access – state and national Fingerprint Based Background Checks may not be authorized and permissible by law. The checks are permitted however, when private contractors are accessing any infrastructure that has or potentially has access to CJI.

Another area can include Management Control Agreements (MCA). The MCA is often used when the criminal justice function, such as dispatching or background check screening, has been outsourced. If staff are not accessing CJI, CHRI or performing administration of criminal justice functions, then the terms and conditions are the more appropriate mechanism for the parties to agree on compliance issues when compulsory measures are not germane.

DATA SECURITY IMPLICATIONS: LICENSE PLATE DATA

LPR data must meet two requirements to be considered CJI:

1. The FBI-CJIS Division must provide the data.
2. The data is accompanied by PII in accordance with the property data definition listed earlier in this document.

For example, the FBI-CJIS Division often creates license plate hotlists for local law enforcement. The data is distributed by FBI-CJIS, but contains no PII. In the absence of PII, the data is not CJI, and FBI-CJIS Security Policy compliance is not required. Alternately, if your agency generates the LPR data and attaches PII to it, that data is technically not CJI because FBI-CJIS did not provide it. Your agency may choose to treat it as CJI and find added value in vendors who voluntarily comply with the FBI-CJIS Security Policy. However, by definition that data requires no Security Policy compliance.

DATA SECURITY IMPLICATIONS: FACIAL RECOGNITION DATA

According to the FBI-CJIS Security Policy's section on biometric data, "facial recognition data in any form is CJI if accessed through or provided by FBI-CJIS." Much like LPR data not provided by FBI-CJIS, if your agency creates facial recognition data on its own, then you are not obligated to comply with the FBI-CJIS Security Policy unless you voluntarily choose to do so.

DATA SECURITY IMPLICATIONS: BALLISTICS ANALYSIS DATA

Ballistic analysis data from Vigilant's BallisticSearch only collects data from abandoned evidence of a crime scene and does not link to any Personally Identifiable Information or sourced from FBI-CJIS and not CJI. However, Vigilant Solutions application figurations are driven toward FBI-CJIS compliance for confidentiality, integrity and availability.

FBI-CJIS COMPLIANCE ROADMAP

In summary, it is your responsibility to determine if your vendors operate in compliance with the FBI-CJIS Security Policy. By understanding the FBI-CJIS Security Policy, knowing what questions to ask, and what documentation to request from your proposed vendor, you will be well on your way to ensuring that any CJI data being stored outside of your agency's network is secure.

Working together, vendors and their agency customers now have a blueprint for success where information security protections are in place enabling the agency to fulfill its mission of serving its citizens.

BE SAFE. BE SMART. BE VIGILANT.

VIGILANTSOLUTIONS.COM · 925-398-2079

VIGILANT SOLUTIONS

VS-0318-BS-SS-02-en