Is Your Vendor CJIS-Certified?

How to identify a vendor partner that can help your agency comply with new federal security standards for accessing criminal justice information

Introduction: The Importance of the CJIS Security Policy

In 2011, the FBI's Criminal Justice Information Services Division (CJIS) issued the CJIS Security Policy, a set of standards for organizations that access criminal justice information (CJI). CJIS developed this policy to better protect the data it delivers to federal, state and local law enforcement agencies, from services like the National Crime Information Center (NCIC), the Integrated Automated Fingerprint Identification System (IAFIS) and the National Incident-Based Reporting System (NIBRS). The policy is also designed to protect CJI that comes from sources other than the FBI.[1]

Securing criminal justice data from unauthorized access is crucial, given how heavily agencies rely on information technology to fulfill all aspects of their missions. The need to access CJI at any time and from any location, the increasing interconnection among law enforcement systems, and the growing number and variety of threats to data security all make it vital to safeguard criminal justice IT systems as thoroughly as possible.

CJIS describes its Security Policy as a minimum set of standards. A local government may adopt it just as it stands, or it may augment the CJIS provisions with more stringent requirements.[2] In either case, the CJIS Security Policy applies to all organizations and individuals that access CJI or support criminal justice services. These include contractors, private organizations and non-criminal justice agencies, along with criminal justice agencies themselves.[3]

When it published the Security Policy, CJIS set September 30, 2013, as the deadline for achieving compliance. There is currently one exception to that deadline: Agencies have until September 30, 2014, to implement advanced (multi-factor) authentication for accessing CJI from an environment that is not physically secured. Since 2011, CJIS has modified the Security Policy several times. The most recent version, 5.2, was published in August 2013: *www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view.*

Once an agency becomes compliant with the CJIS Security Policy, the FBI expects to receive a letter attesting to that fact. The FBI may then schedule an audit to confirm the agency meets all of the policy's provisions. If the audit uncovers deficiencies, correcting them could cost hundreds of thousands of dollars.

Although the CJIS deadline has already passed, many government agencies are still working to achieve compliance. They find themselves in a difficult position. A non-compliant organization might face administrative sanctions and lose access to CJIS services. It might also face state and federal criminal penalties.

In addition, a criminal justice agency that leaves its IT systems vulnerable could cause serious problems for itself and the citizens it serves. According to a 2014 study by the Ponemon Institute, U.S. companies and government agencies paid an average of $201 per record in 2013 to deal with the aftermath of data breaches.[4] And, of course, if criminals gain access to sensitive information, that could jeopardize investigations and possibly endanger property and lives.

The prospect of data breaches at a criminal justice agency is far from hypothetical. In early 2014, for instance, hackers broke into the public website of the Washington State Administrative Office of the Courts. That attack exposed the Social Security numbers of as many as 160,000 people who had been booked into city or county jails, and the driver's license numbers of up to 1 million people involved in traffic incidents or criminal court cases.[5]

Achieving CJIS Compliance

As agencies work to comply with the CJIS Security Policy, one of the factors that complicates their efforts is misinformation emerging from the vendor community. Some companies that sell security products and services have been claiming their offerings are "CJIS-certified."

Agencies need to form partnerships with vendors that understand the FBI's requirements, and whose products and services can help agencies reach compliance. However, there is no such thing as a "CJIS-certified" vendor. The FBI's CJIS Division does not evaluate products or services, nor does it issue

any document asserting a vendor or product meets particular requirements. An email from Stephen Exley, information security analyst within the CJIS Information Security Officer Program, testifies to that fact:

"Please be aware there is no CJIS certification process with regard to the CJIS Security Policy. The only certifications related to CJIS that I know of are in regard to facial recognition and finger print capture standards. Those do not have any relation to the CJIS Security Policy. ... We do not certify, nor endorse any product, solution, or vendor."[6]

The sole certification activity conducted in connection with the CJIS Security Policy is self-certification — more properly called self-attestation. In that process, an agency carefully documents how it has complied with each requirement in the CJIS Security Policy. It then sends a letter to the FBI's CJIS Division, outlining the results of that internal audit.

Compliance is an activity that an organization attests to, through policies, practices, hardware and software implementation, combined with personnel training and accountability, to prove they have achieved compliance with a specific mandate or regulation.

Identifying a Suitable Partner

Since the FBI does not issue CJIS certifications, how do you know which vendors, products and services can help bring your agency into compliance with the CJIS Security Policy? Here are some questions to ask as you evaluate potential vendor partners:

Does the vendor offer a complete solution? Your vendor should be able to address as many of the CJIS requirements as possible, especially in the areas of security management, availability, authentication and encryption. The best approach is to work with one partner on the entire range of CJIS requirements. That way, when problems arise, you know who is responsible for solving them. Working with a single partner is also the best way to deal with the increasingly complex and integrated systems that support public safety and criminal justice agencies. Security tools developed by one vendor must operate seamlessly across all those components. When you combine components from multiple vendors, you risk encountering functional gaps and incompatibilities.

Are the vendor's products compatible with all computing platforms? The computing environment in a criminal justice agency may encompass multiple operating systems, including diverse mobile devices. The tools you implement need to work with all of them. They must also be able to protect data when your agency collaborates with other organizations that use different combinations of platforms.

Has your vendor completed the Federal Identity, Credential, and Access Management (FICAM) or FedRAMP certification process? The FICAM Roadmap is a document developed by the U.S. government to guide federal agencies in developing and implementing architectures for identity, credential and access management (ICAM). The U.S. General Services Administration provides a list of products and services related to ICAM implementation that have gained approval through a FICAM Testing Program.[7] FedRAMP (Federal Risk and Authorization Management Program) is a federal program that standardizes the approach to security assessment, authorization and continuous monitoring for cloud projects and services.

www.fbi.gov

Organizations had until September 30, 2013, to comply with the FBI's CJIS Security Policy and have until September 30, 2014, to implement advanced (multi-factor) authentication.

Symantec: Providing a Complete CJIS Compliance Solution

Symantec offers a full range of enterprise-class solutions that work together to keep criminal justice data safe, available and accessible to authorized individuals, across most technology platforms.

Although there is no such thing as a CJIS-certified product or service, many of Symantec's solutions have been certified for compliance with other important security standards. For example, Symantec is one of only two vendors to offer two-factor authentication that has achieved Level 4 certification under the Federal Information Processing Standards (FIPS) 140 standard.

Symantec's portfolio includes products and services that address nearly all of the 12 areas covered in the CJIS Security Policy. In each of these areas, an agency must implement specific processes and technologies to safeguard criminal justice information, and the requirements are stringent. The policy areas are:

1. Information Exchange Agreements
2. Security Awareness Training
3. Incident Response
4. Auditing and Accountability
5. Access Control
6. Identification and Authentication
7. Configuration Management
8. Media Protection
9. Physical Protection
10. Systems and Communications Protection & Information Integrity
11. Formal Audits
12. Personnel Security

Figure 1 on page 5 indicates how products and services from Symantec address 11 out of the 12 CJIS policy areas. A detailed description of Symantec's approach to each of these 11 areas is beyond the scope of this paper. However, the following sections provide high-level explanations of how Symantec's products and services help criminal justice agencies carry out five activities that are crucial for achieving CJIS compliance.

1. Develop and enforce CJIS IT policies.

Symantec Control Compliance Suite provides a framework on which to build an agency's IT governance, risk and compliance program. It helps the agency communicate IT risk in terms that are relevant to its mission, set priorities for remediation and automate its assessment processes.

Symantec Data Loss Prevention allows an agency to discover where all of its data is stored; identify true data owners; receive alerts about unusual activity; monitor how data is being used and when users are on and off the enterprise network; notify users about policy violations; secure exposed files and folders; stop inappropriate outbound communications; and manage data loss policies, workflow and remediation, reporting and administration.

Symantec Network Access Control helps ensure that each client computer complies with the agency's security policy before that computer is allowed to access the network. Non-compliant computers are directed to a remediation server, which downloads the software, patches, virus definition updates and other elements needed to achieve compliance. The tool also monitors endpoints for changes in their compliance status.

2. Authenticate identities to CJIS systems.

Symantec Validation and ID Protection Service (VIP) provides secure and reliable authentication in a cloud-based service. It offers multiple options for two-factor authentication, including the use of one-time passwords delivered via hardware, software or a variety of mobile devices.

Symantec Norton Secure Login, a cloud-based offering, is a turnkey solution that operates out of Symantec's secure and highly available data centers that generate over 4 billion daily two-factor, PKI and SSL authentications for millions of users, devices, servers and websites. As an approved Credential Service Provider, Symantec received LOA 2 and LOA 3 certification in accordance with the FICAM Roadmap and Implementation Guidance.[8]

Symantec Managed PKI Service, a cloud-based offering, issues X.509 certificates that interoperate with

Figure 1

Symantec Solutions/ Criminal Justice Information Services (CJIS)

	Product	Information Exchange Agreements	Security Awareness Training	Incident Response	Auditing and Accountability	Access Control	Identification and Authentication	Configuration Management	Media Protection	Physical Protection	Systems & Communications Protection & Information Integrity	Formal Audits	Personnel Security
Governance & Security Management	Control Compliance Suite	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	
	Data Loss Prevention			✓	✓	✓			✓			✓	
	Data Insight				✓	✓	✓	✓			✓	✓	
	Critical System Protection			✓	✓	✓	✓	✓	✓		✓	✓	
	O3				✓	✓							
	Mobile Mgmt Suite					✓			✓		✓		
	Protection Suite	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	
Business Continuity & Availability	Veritas Cluster Server							✓			✓		
	NetBackup	✓			✓	✓		✓	✓	✓	✓	✓	
	OpsCenter	✓				✓		✓	✓	✓	✓	✓	
	Enterprise Vault/Clearwell			✓	✓	✓		✓	✓		✓	✓	
	Storage Foundation (HA/DR/CFS)	✓						✓	✓		✓		
	Operations Manager VOM/VBS				✓	✓		✓	✓		✓	✓	
Authentication & Encryption	VeriSign Solutions (2FA & MPKI)		✓			✓	✓				✓		
	PGP Encryption Products		✓	✓	✓	✓	✓	✓	✓	✓	✓		

operating systems, devices, virtual private networks (VPNs) and Web browser software. Among other features, the Managed PKI Service can automatically configure a user's browser, VPN client, mail client or other application to use certificates, and it can automate the renewal of certificates.

3. Protect confidential CJIS information.

Symantec Data Loss Prevention allows an agency to discover, protect and manage data wherever it is located, including endpoints, mobile devices, networks and storage systems.

Symantec NetBackup provides a single solution for backing up all data assets, with support for virtually every popular server, storage system, hypervisor, database and application platform.

Symantec Backup Exec allows an agency to back up local or remote data to tape, disk or the cloud, and to quickly search for and restore file or application objects, applications, VMs and servers directly from backup storage.

Symantec Enterprise Vault is an archiving solution that agencies can use to store, manage and discover unstructured information.

Symantec Replicator includes the Volume Replicator and File Replicator solutions. It provides continuous data replication, allowing users to quickly recover critical applications at remote recovery sites, using IP networks.

4. Manage CJIS infrastructure.

Symantec IT Management Suite, including Mobile Device Management, provides application virtualization and streaming, asset management, cross-platform management, discovery and inventory, operating system deployment and migration, patch management, process automation, remote management, reporting and analytics, software distribution and software license management. It offers these capabilities for remote and mobile users as well as for users connected to the primary infrastructure.

5. Protect the CJIS infrastructure.

Symantec Protection Suite provides fast, effective protection — beyond antivirus measures — for laptops, desktops and servers, and for messaging and Web gateways. Its advanced content filtering catches more than 99 percent of spam, and its Web gateway security protects against malicious software, spyware, malware and other Web threats. It can recover individual files or folders in seconds, and complete Windows systems in minutes.

Symantec Web Gateway uses a global network of more than 210 million systems to identify new Web-borne malware threats before they cause disruption. An agency can deploy this tool as either a virtual appliance or physical hardware.

Symantec Messaging Gateway provides real-time protection against spam and malware, targeted attack protection, advanced content filtering, data loss prevention and email encryption.

Symantec Critical Systems Protection secures physical and virtual data centers with host-based intrusion detection (HIDS) and intrusion prevention (HIPS). It provides complete protection for VMware vSphere, stopping zero-day and targeted attacks, while providing real-time visibility and control into compliance.

The Road to Compliance: First Steps

Before a criminal justice agency can become compliant with the CJIS Security Policy, it must first take four important preliminary steps:

Appoint a Chief Systems Officer.

The Chief Systems Officer (CSO) is responsible for administering an agency's CJIS network. According to the CJIS Security Policy, an agency may not outsource this role; the CSO must be an employee of the agency. The main role of the CSO is to set, maintain and enforce:

- ✓ Standards for selecting, supervising and separating people who have access to CJI
- ✓ Policy to govern the operation of IT components that make up and support all systems and networks that process, store or transmit CJI
- ✓ Requirements regarding functions that may be outsourced and those that must stay within the agency's direct control[9]

Since the CSO participates in every one of the 12 CJIS policy areas, the choice of an appropriate person to fill this role is crucial.

Conduct a policy implementation and review.

Within each of the 12 policy areas, CJIS requires that an agency establish and document certain policies and procedures. For instance, under the first area, Information Exchange Agreements, CJIS says that before an agency can exchange CJI with any external entity, the two parties must sign an agreement that defines their roles and responsibilities and the details of data ownership. Under the third area, Incident Response, CJIS requires an agency to develop internal procedures for responding to security breaches, and for coordinating those responses with other organizations.

Before it can work toward CJIS compliance, an agency must review all CJIS requirements for implementing policies and procedures, take stock of which of those policies already exist and are fully documented, identify which policies it has not yet created and/or documented, and establish a plan for closing those gaps. When this work is complete, the agency will have a solid framework for compliance.

Identify your assets.

Of the 12 CJIS policy areas, 3 require a detailed knowledge of an agency's IT assets. They are:

- ✓ **Auditing and Accountability:** Agencies must put controls in place to generate audit records when specific events that might have a bearing on security occur on specific IT components, including servers and mobile devices. In order to implement these controls, the agency must have a thorough inventory of its assets.
- ✓ **Access Control:** Agencies must put mechanisms in place to ensure only users with specific authorization can read, write, process or transmit specific kinds of CJIS information, or make changes to any systems that allow access to such information. To achieve this, the agency must be able to identify all of the system components through which a user might gain access to information.
- ✓ **Configuration Management:** Only qualified and authorized individuals may make changes to an agency's information systems. To help maintain this control, the agency must create a complete topological drawing that shows how its network connects to criminal justice information, systems and services. The agency must also keep this drawing up to date. It is not possible to develop an accurate drawing without first taking stock of the agency's IT components.

As threats from both external hackers and disgruntled employees continue to expand and evolve, organizations must move beyond baseline security measures. They must develop strategies for continuously monitoring and diagnosing activity on their systems.

Conduct risk and vulnerability assessments.

Before you can fully protect your IT infrastructure, you must understand where the dangers lie. An agency gains that knowledge by conducting two distinct procedures:

- ✓ **Risk Assessment:** In this internal process, the agency first examines each IT component to determine the characteristics that might lead to a security breach or data loss. For example, consider a server. Is it a standalone component? Do you back up its data on a regular basis? Do you download patches to correct weak spots in the operating system? Does it have only one power supply? Is there no other server to serve as a backup? Each of those conditions poses a risk that data might be lost, damaged, stolen or destroyed. Once the agency identifies a risk, it can take steps to eliminate it.
- ✓ **Vulnerability Assessment:** This process is generally conducted by a third-party auditing team. Once officials at the agency believe they have secured their IT system in all possible ways, the external team uses hacking strategies, social engineering and other tools to try to break into the system. This process exposes any remaining vulnerabilities so the agency can correct them.

Beyond CJIS Compliance: Automated, 24/7 Monitoring

An agency's efforts to secure its IT systems and CJI don't end on the day it passes a CJIS audit. As threats from both external hackers and disgruntled employees continue to expand and evolve, organizations must move beyond baseline security measures. They must develop strategies for continuously monitoring and diagnosing activity on their systems.

The CJIS Security Policy does not currently address the need to continuously monitor the security of an agency's IT system in an automated fashion. For further information on automated and continuous monitoring, contact Symantec.

The Time is Now to Ensure Compliance

Criminal justice agencies that have not yet made their systems compliant with the CJIS Security Policy need to do so as quickly as possible. Further delay increases the chance that the agency will face penalties, and also increases the risk of security breaches and data loss.

The best partner on the road to CJIS compliance is an experienced vendor with an integrated solution that addresses every aspect of data security.

Endnotes

1. "Meeting the CJIS Mandate for Advanced Authentication," Digital Communities white paper, 2012, www.digitalcommunities.com/library/Meeting-the-CJIS-Mandate-for-Advanced-Authentication.html
2. Criminal Justice Information Services (CJIS) Security Policy, Version 5.2, August 9, 2013
3. Ibid.
4. Ellen Messmer, "Data breaches 9% more costly in 2013 than year before," Network World, May 5, 2014, www.networkworld.com/article/2176589/malware-cybercrime/data-breaches-9-more-costly-in-2013-than-year-before.html
5. Washington Courts Data Breach Information Center, www.courts.wa.gov/newsinfo/?fa=newsinfo.displayContent&theFile=dataBreach/home
6. Email from Stephen Exley, information security analyst within the CJIS Divisions' Information Security Officer Program, to Robert Myles, National Practice Manager, Public Safety and Cybersecurity, U.S., state and local government, Symantec, April 25, 2014
7. "Approved Products List," www.idmanagement.gov/approved-products-list
8. Certification is provided by Kantara, Trust Framework Certified under FICAM for FICAM Credential Service Providers
9. This and subsequent details on the 12 areas of the CJIS security policy come from Criminal Justice Information Services (CJIS) Security Policy, Version 5.2

Symantec™

For information on how Symantec can help your agency achieve CJIS compliance, contact your local/area Symantec Account Executive or Robert Myles, National Practice Manager of Programs and Alliances:

Robert_Myles@symantec.com / 817-488-2630