Criminal Justice Information System (CJIS) Vendor Policy Guidelines

Last Updated: 08/17/2015

Massachusetts Department of Criminal Justice Information Services

200 Arlington Street, Suite 2200
Chelsea, MA 02150

Tel : 617.660.4600
Fax: 617.660.4613
Web: www.mass.gov/CJIS

CJIS Vendor Policy Guidelines

About this Document

The purpose of this document is to establish guidelines for vendors and law enforcement/criminal justice agencies who wish to propose the use of hardware equipment and/or software on the Criminal Justice Information System (CJIS) network. This includes agencies who wish to exchange criminal justice information via the CJIS Broker. It also includes guidelines for the ongoing use and maintenance of approved hardware equipment and/or software on the CJIS network.

Overview

The Department of Criminal Justice Information Services (DCJIS) is charged by Massachusetts General Laws chapter 6, § 168 with the responsibility of providing for and exercising control over the installation, operation, and maintenance of data processing and data communications systems referred to by said statute as the criminal offender record information system. This system is commonly known as the Criminal Justice Information System or CJIS. The DCJIS is further charged with designing the CJIS to ensure the prompt collection, exchange, dissemination, and distribution of information as may be necessary for the efficient administration and operation of criminal justice agencies, as well as for connecting with similar systems in this or other states.

The DCJIS recognizes that there may be instances where functionality desired by members of our user community is not, or cannot, be provided by "standard", previously approved hardware or software. It is the purpose of these guidelines to provide a structure within which the staff of the DCJIS will work with agencies and their vendors to evaluate new types of hardware and software that the user community is interested in obtaining, but which deviate from currently approved and utilized technologies.

CONNECTING TO THE CJIS NETWORK

- Only **technologies approved** by the DCJIS may be connected to the CJIS network.
- Said technologies and associated maintenance services may only be purchased from **vendors approved** by the DCJIS.

The DCJIS will evaluate proposals for new hardware and/or software when:

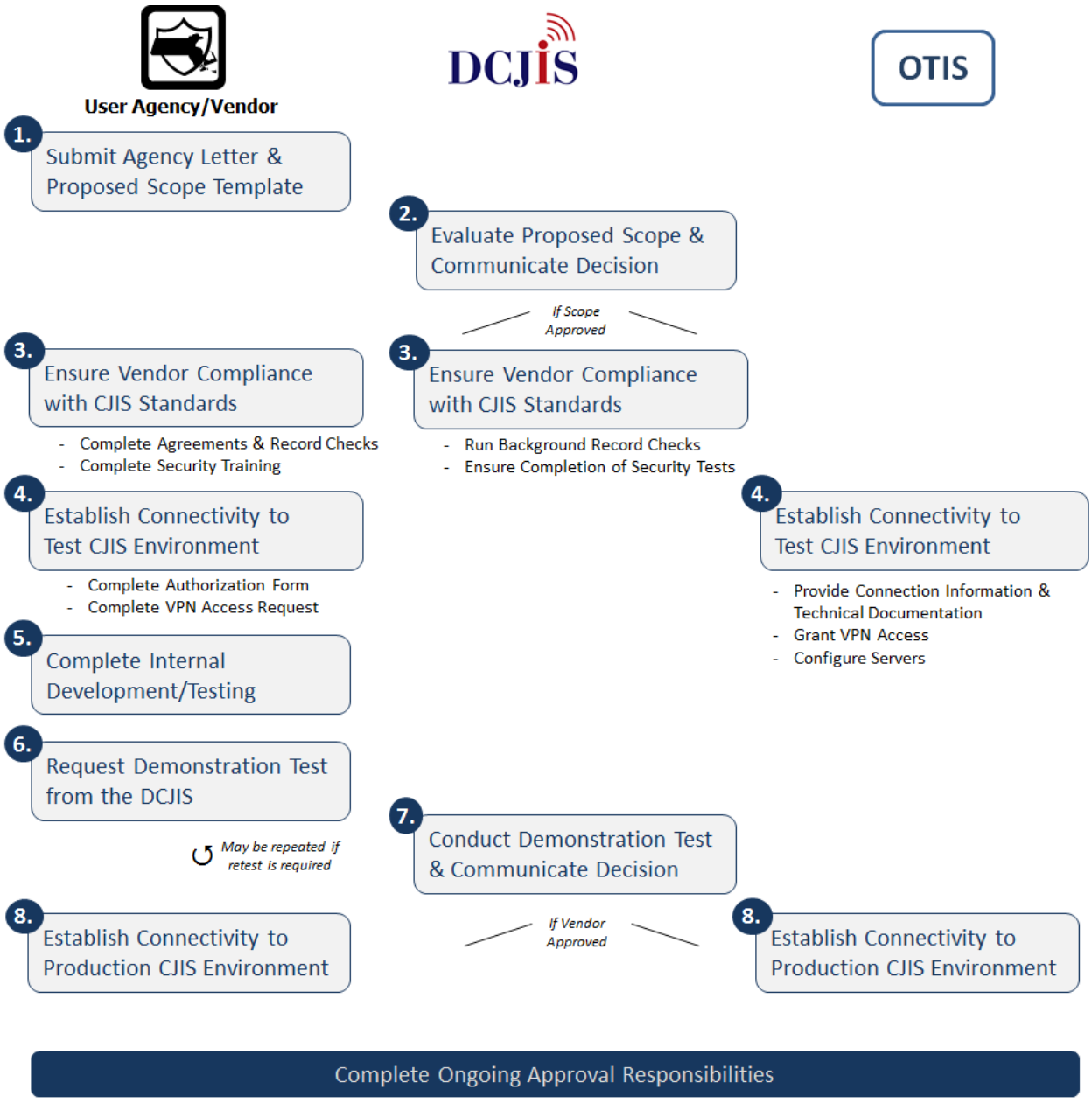
- ✓ A criminal justice agency has expressed interest in the technologies proposed by a vendor, and
- ✓ The DCJIS believes that the benefits of the proposed technologies would be of interest to one or more criminal justice agencies.

A major consideration for the DCJIS in modifying the CJIS, or any of its components, is the security and integrity of the system. The CJIS Vendor Policy Guidelines are designed to optimize the DCJIS' control of the system and to articulate the consequences if the system is compromised in any way.

Steps to Become a CJIS-Approved Vendor

The following diagram summarizes the process for vendors to become approved to provide hardware, software, and/or services on the CJIS network. Immediately following the diagram is additional information about each step in the process.

Figure 1 – Vendor Approval Process



1. Submit Agency Letter and Proposed Scope Template (Agency/Vendor):

The process begins when a criminal justice agency, such as a law enforcement agency, identifies a business need to connect new hardware and/or software to the CJIS network. The criminal justice agency summarizes its support in writing to the DCJIS. The agency support letter must:

- ✓ Describe what CJIS functionality is be being requested and why
- ✓ Be signed by the Police Chief or Agency Head
- ✓ Be submitted to the DCJIS in conjunction with the Proposed Scope of Services.

Once signed by the Police Chief/Agency Head, the Agency Letter must be scanned and emailed along with the completed Proposed Scope template to cjis.support@state.ma.us.

If submitting the Agency Letter and Proposed Scope template via email is not possible, they should be mailed to the following:

Massachusetts Department of Criminal Justice Information Services
ATTN: CJIS Support Services
200 Arlington Street, Suite 2200
Chelsea, MA 02150

Note: If the proposal is for multiple different criminal justice agencies (e.g., multiple police departments) to use the proposed functionality, a joint letter of support must be provided. The joint letter of support must be signed by the Chief/Agency Head of each participating agency.

Along with the letter of support, the agency and its selected vendor must provide a proposal of the scope of the technology to be implemented using the CJIS Vendor Proposed Scope template available at mass.gov/CJIS. The scope template includes sections for:

- **Contact Information** – For the agency(ies) and its vendor organization. This includes a key contact person from each participating agency and from the vendor assigned to work with the DCJIS on the evaluation of the proposed scope.
- **Proposed Functionality** – A detailed description of the proposed hardware, software, and/or services to be provided to the end user community. This information is critical to the DCJIS understanding what CJIS functionality will be available to the criminal justice agency(ies) at the completion of the process. Should the scope proposal be approved for development, the proposed functionality will also be used by the DCJIS to design demonstration test scripts.
    - o CJIS Transactions – For agencies/vendors proposing software/services that utilize one or more of the CJIS transactions available via the CJIS Broker, the agency/vendor must select which transactions are proposed to be implemented from the functionality checklist. See the CJIS Broker Documentation available at mass.gov/CJIS for additional information on CJIS transactions.
    - o Hardware Location and Specifications – For agencies/vendors proposing hardware equipment, the agency/vendor must provide information about the intended

hardware location, including whether the hardware will be fixed (e.g., installed in a car or a police station) or mobile (e.g., mobile tablet). Agencies/vendors also need to provide the specifications for the equipment to be connected, including proposed configurations. Finally, if the hardware will not be fixed in a secure location as defined in the latest version of the FBI CJIS Security Policy, the agency/vendor must describe how they intend to meet the authentication, encryption, and management requirements of the CJIS Security Policy.

  - Envisioned Benefits – A written narrative describing the envisioned benefits to the end user community of the proposed hardware, software, and/or services.

- **Security Approach** – Specific details about the proposed methods to comply with the CJIS security requirements and to maintain a high level of security within the network at all times. The security approach will vary based on the proposed hardware, software, and/or services (e.g., iPad versus Windows encryption).

- **Testing Approach** – A detailed description of how the agency/vendor proposes to test the hardware, software, and/or services within the CJIS network including:

  - Test Sites: The proposed agency site(s) for testing. The DCJIS will determine whether or not a site is an agreed upon test site based in part on that site's compliance with DCJIS and FBI regulations and policies, as well as on that site's history of working with the DCJIS.

  - Uninterrupted Access: The plan for ensuring the agency has uninterrupted access to the production CJIS environment during all testing activities.

- **Maintenance Approach** – A written explanation of how the vendor intends to ensure the long-term viability of the proposed hardware, software, and/or services. This includes a description of how the vendor will provide maintenance services on anything connected to the CJIS network. Maintenance services are required for compliance with DCJIS policies.

The agency letter and proposed scope template must be submitted electronically via email to the DCJIS. See the CJIS Vendor Proposed Scope template available at mass.gov/CJIS for additional information and submission instructions.

2. Evaluate Proposed Scope and Communicate Decision (DCJIS):

Upon receiving the letter of agency support and the accompanying proposed scope template, the DCJIS will evaluate the scope proposal and make a determination as to whether or not the agency/vendor is approved to proceed with development and testing activities. If the DCJIS has any questions about the proposal or requires any additional information to make its decision, it will reach out to the contacts specified.

Once the DCJIS has made an evaluation decision, it will inform the agency and vendor in writing via email of its decision using the contact information specified.

- ✓ **Approve**: If the decision is to approve the proposal for development/testing, the DCJIS will also notify the Executive Office of Public Safety and Security's Office of Technology

and Information Services (OTIS) of the approval decision. The DCJIS will provide the agency/vendor with information for individuals at OTIS to contact to establish connectivity to the test CJIS environment.

In addition, the DCJIS will designate a primary contact person to work with the agency/vendor and OTIS to provide assistance when required, to conduct spot audits of the vendor's pre-implementation use of the system, and to report on the progress of the implementation.

- ✗ **Do Not Approve**: If the decision is to deny the proposal, the DCIJS will notify the agency/vendor as to why the proposal was denied.

☝ Please note, the Commissioner/designee of the DCJIS reserves the right to deny or delay the processing of requests under these guidelines based upon technical staff availability or in consideration of other priorities within the DCJIS.

3. Ensure Vendor Compliance with CJIS Standards (Agency/Vendor and DCJIS):

If the DCJIS approves the proposal for development/testing, it will initiate the process for clearing vendor personnel for access to CJIS and agency systems. This includes both initial vendor personnel and personnel changes over time. Prior to those persons having access to any agency or CJIS system or data, the DCJIS will require the following from the vendor and its personnel:

- ✓ **Signed Authorization Agreements**: In accordance with 803 C.M.R. 3.02(3), all vendor personnel who will be working on the proposed project must complete and sign the Individual Agreement of Non-Disclosure (AOND). The criminal justice agency will ensure compliance with this requirement, will keep completed AOND forms on file, and will provide them to DCJIS personnel upon request.

  In addition, the vendor must execute the Vendor Agreement of Non-Disclosure. This agreement is signed on behalf of the vendor and must be provide along with any Individual AONDs.

  FBI CJIS Security Addendum: Vendor personnel will be required to execute the FBI CJIS Security Addendum. The criminal justice agency will ensure compliance with this requirement, will keep completed forms on file, and will provide them to DCJIS personnel upon request.

- ✓ **Fingerprint-Supported Criminal Record Checks**: The DCJIS will fingerprint all vendor personnel who will work on the project and conduct state, national, and state-of-residence fingerprint-supported criminal record checks. Fingerprints will be taken at the DCJIS location in Chelsea Massachusetts. The DCJIS will make a suitability decision on each individual based upon the results of these checks.

  ☝ Fingerprint-supported criminal record checks will be conducted annually for each person who continues to work on the project. See the Annual Reporting Requirements section for additional information.

- ✓ **CJIS Security Awareness Training**: All vendor personnel must complete the CJIS Security Awareness Training. Testing will be conducted via the CJISonline.com security awareness testing tool.

  ☝ Note: Any individual who has a current certification that he/she obtained using the CJISonline.com tool will not be required to be recertified until his/her current certification expires.

- ✓ **Vendor Personnel List**: The criminal justice agency must maintain an up-to-date list of all vendor personnel working with the agency on the project, including initial personnel and changes over time. At a minimum, this must include the person's name, state of residence, the date he/she started on the project, the date he/she signed the security agreement and individual disclosure agreement, the date fingerprinted, the date of last background record check/result, the date he/she successfully completed the CJIS security training, and the date he/she left the project (if applicable). The criminal justice agency must also maintain a list of vendor personnel who requested but were denied access and why.

  The agency must be prepared to provide this information to the DCJIS before demonstration testing, annually, and upon request. See the Vendor Personnel template available at mass.gov/CJIS for additional information.

4. Establish Connectivity to the Test CJIS Environment (Agency/Vendor and OTIS)

When ready to begin development and testing activities, the agency/vendor must reach out to the OTIS contacts provided to establish connectivity to a CJIS test environment at the test site(s) specified. OTIS and the agency/vendor will work closely to establish technical connectivity. The following items must be completed:

What	Who	Comments
1. Send the **VPN User Application** to OTIS (if needed)	Agency/Vendor	Used if the vendor requires external access independent of the agency for which the vendor is providing services. The Virtual Private Network (VPN) User Application form can be found on mass.gov/CJIS.
2. Establish **VPN access** (if needed)	OTIS	OTIS will create a VPN account. Accounts are typically created within 10 business days after approval.
3. Provide **CJIS Broker Connection** and **Transaction Specific** Information (if needed)	OTIS	For those approved to implement CJIS transactions, OTIS will collect and provide the information required to connect to the test CJIS Broker environment including: • Test Server IP • Web Server URL • Access to CJIS Broker WSDL OTIS will also provide access to any additional technical documentation available for the specific CJIS

What	Who	Comments
		transactions the agency/vendor has been approved to develop, such as sample XML schemas. The content of the information will vary by transaction and should supplement the Broker Documentation available on mass.gov/CJIS.
4. Email **CJIS Broker Authorization Form** to OTIS (if needed)	Agency/Vendor	Used to request authorization to access the CJIS Broker web service via the CJIS network. Information provided by the agency/vendor on this form will be used by the Commonwealth to authenticate and authorize requests and responses to and from the CJIS Broker. The CJIS Broker Authorization Form is available on mass.gov/CJIS.
5. Complete **server configurations**	OTIS	OTIS will make any server configurations necessary to support connectivity based on the information provided. This may include coordinating with MassIT regarding any required firewall changes.

5. Complete Internal Development/Testing (Agency/Vendor):

Once able to access the test CJIS environment, the agency/vendor will complete their internal development and testing activities using the approach described in the approved scope proposal.

6. Request Demonstration Test from the DCJIS (Agency/Vendor):

When an agency/vendor has completed its internal testing and is confident that it is production ready, they should contact the DCJIS to schedule a demonstration test. The agency/vendor must email their CJIS demonstration test request to the DCJIS at cjis.support@state.ma.us. The subject of the email should be "Request for DCJIS Demonstration Test" and the email must include a certification that the agency/vendor is in compliance with DCJIS and FBI security standards and policies, which will initially be evaluated during the testing phase and monitored on an ongoing basis.

7. Conduct Demonstration Test and Communicate Decision (DCJIS and Agency/Vendor):

Upon receiving a CJIS demonstration test request email, the DCJIS will reach out to the vendor contact identified to schedule a time to demonstrate the approved functionality. The DCJIS will provide specific guidelines for system use during all testing. This may involve the use of test or restricted network addresses or physical locations, during which time the DCJIS may monitor the activities of the vendor to ensure compliance with the approved scope.

A full demonstration of the system is expected and appropriate DCJIS staff will make a determination of the system's full compliance with the approved scope. The DCJIS will prepare a series of test scripts the agency/vendor will be asked to demonstrate based on the specific functionality and sites for which they were approved.

Upon completion of the demonstration test, the DCJIS will make a determination as to whether or not the system complies with DCJIS and FBI standards and policies and that it functions properly in the current technology environments. The DCJIS will notify the agency/vendor in writing of the results including:

- ✓ **Pass:** If an agency/vendor is found to be in compliance, the DCJIS will also notify the Executive Office of Public Safety and Security's Office of Technology and Information Services (OTIS) that the agency/vendor is approved to connect to the production CJIS environment for the approved scope.

- × **Do Not Pass:** If the agency/vendor fails to demonstrate the ability of the hardware/software to satisfy the functionality contained in the scope proposal, the DCJIS will work with the agency/vendor to identify the problem areas. The agency/vendor will be given an opportunity to continue testing in accordance with the provisions of this section for the purpose of bringing the system into full compliance.

  The agency/vendor may then request an additional demonstration as outlined in step 6 – Request Demonstration Test from the DCJIS. The DCJIS will conduct a maximum of two (2) demonstration visits for the purpose of determining full compliance. After two failed attempts, further evaluation will be at the discretion of the DCJIS Commissioner/designee.

DCJIS & FBI Security Standards

During demonstration testing, the DCJIS may ask agencies/vendors to demonstrate how they comply with DCJIS and FBI security standards from a technical and operational perspective.

☝ Please note, the DCJIS reserves the right to delay or terminate the testing at any time under conditions including, but not limited to:

- The DCJIS determines that the testing is interfering with the normal operations of the CJIS system or network;
- The DCJIS determines that the agency/vendor is in violation of any provision of these guidelines;
- The DCJIS determines that the agency/vendor is not performing its testing in accordance with the approved scope;
- The agency/vendor requests that the DCJIS suspend testing activities;
- The DCJIS determines that the agency/vendor is utilizing the CJIS system in an inappropriate way, or in such a way as to cause the user agency to be in violation of its CJIS user agreement;

- The DCJIS becomes aware of a problem in the approved scope which represents a possible or real breach of security, or which would otherwise jeopardize the proper functioning of the network.

8. Establish Connectivity to Production CJIS Environment (OTIS and Agency/Vendor):

For agencies/vendors approved by the DCJIS, OTIS will work with the agency/vendor to enable access to the production CJIS environment at the agreed upon sites. This may involve the establishment of additional user credentials as well as modifying server/firewall configurations.

Once the system is live in the production environment, the DCJIS expects that, except for agreed upon maintenance windows as described in the scope proposal, the criminal justice agency will have uninterrupted access to the functionality. Thirty (30) days after go live, the contact person at the sponsoring agency must inform the DCJIS via email whether the functionality was available without interruption for a period of at least 30 days and to confirm whether the agency is satisfied with overall performance. If satisfactory performance has not been achieved, the DCJIS will work the criminal justice agency and vendor contacts regarding a mitigation plan.

Ongoing Responsibilities for Approved Vendors

Criminal justice agencies and their approved vendors have an ongoing responsibility to comply with the provisions of these guidelines, including, but not limited to, ensuring that they continue to meet DCJIS and FBI security standards and policies. The DCJIS will not provide an endorsement for use of the vendor's products, but it will provide a statement of compliance with current agency technologies and policies upon request. The vendor name and contact information will also be posted to the DCJIS Extranet.

DCJIS and FBI Security Standards and Policies

Agencies and their approved vendors are responsible for ensuring ongoing compliance with DCJIS and FBI security standards and policies from both a technical and operational perspective. This includes ensuring that the approved hardware/software meets the latest DCJIS and FBI security standards and working with the DCJIS using the process described in the Steps to Become an Approved CJIS Vendor section if any changes are required to the approved scope to comply with security standards.
See mass.gov/CJIS for additional information on DCJIS and FBI security standards and policies.

The criminal justice agency is responsible for maintaining information about changes to vendor personnel working on the project over time. When a new person joins the project, the criminal justice agency must complete the following steps prior to allowing those persons to have access to any agency hardware or software containing, or allowing access to, criminal justice information (CJI) and/or connected to the CJIS network.

- ✓ **Signed Authorization Agreements**: The criminal justice agency must ensure that all vendor personnel complete and sign the Individual Agreement of Non Disclosure (in accordance with 803 C.M.R. 3.02(3)) as well as the FBI CJIS Security Addendum. The agency must keep a copy of the fully executed agreements on file and be prepared to provide the information to the DCJIS upon request.
- ✓ **Fingerprint Supported Record Checks**: The criminal justice agency must notify the DCJIS of any vendor personnel changes so that the DCJIS can conduct fingerprint-supported criminal

record checks on those individuals at its office in Chelsea Massachusetts. Notifications must be made to the CJIS Support Services Unit either via email to cjis.support@state.ma.us or via written correspondence to the DCJIS address listed under step one in the Steps to Become a CJIS-Approved Vendor section of this document.

- Fingerprint-supported criminal record checks will be conducted annually for each person who continues to work on the project. See the Annual Reporting Requirements section for additional information.

- ✓ **CJIS Security Awareness Training**: The criminal justice agency must ensure that all vendor personnel have completed the CJIS Security Awareness Training.

- ✓ **Vendor Personnel List**: The criminal justice agency must maintain an up-to-date list of all vendor personnel working with the agency on the project, including changes over time. At a minimum, this must include the person's name, state of residence, the date he/she started on the project, the date he/she signed the security addendum and individual disclosure agreement, the date fingerprinted, the date of last background record check/result, the date he/she successfully completed the CJIS security training, and the date he/she left the project (if applicable). The criminal justice agency must also maintain a list of vendor personnel who requested but were denied access and why. The agency must be prepared to provide this information to the DCJIS before demonstration testing, annually, and upon request.

Vendor Name Changes

Agencies and their approved vendors are responsible for ensuring that the DCJIS has up-to-date information about the vendor organization. If the legal name, location, or primary contact of the vendor changes for any reason (e.g., merger, acquisition, rebranding, etc.), the agency/vendor are to email an updated scope proposal to the DCJIS at cjis.support@state.ma.us. The subject of the email should be "Vendor Information Change for {Previous Vendor Name}." See the CJIS Vendor Proposed Scope template available on mass.gov/CJIS for additional information.

Additional Sites

Approved vendors are authorized to offer the approved system to additional user sites in accordance with the approved scope without further approval by the DCJIS.

New/Changed Functionality

If the vendor wishes to make improvements or changes in the way the system operates, including implementing additional CJIS transactions, a revised scope proposal must be submitted to the DCJIS for review and testing prior to implementation. The revised scope proposal must be submitted and will be evaluated using the process described in the Steps to Become an Approved CJIS Vendor section above.

The DCJIS may, at its sole discretion, approve the changes for immediate implementation without further review, may require an informal technical review/demonstration of the function(s) prior to implementation, or may, if the changes appear significant enough, require a formal demonstration test as outlined above.

CJIS System Changes

The DCIS may periodically make changes to the CJIS system to provide enhanced functionality to the end user community and/or to comply with current laws, regulations, or policy requirements. The DCJIS is not responsible for any impact that changes to the CJIS system may have on vendor systems approved under these guidelines. The DCIJS will make every effort to provide advanced notice to agencies/vendors of all CJIS changes that may impact their systems.

Annual Reporting Requirements

By January 15th of each year, the vendor must report the following to the DCJIS. This information must be emailed to cjis.support@state.ma.us with a subject of "Annual Vendor Report for {VENDOR NAME}".

- **Current Agency List**: A list of Massachusetts criminal justice agency sites using hardware and/or software approved under these guidelines.
- **Potential Agency List**: A list of Massachusetts criminal justice agencies the vendor believes may be considering using the vendor's product(s). This information will be used by the DCJIS for planning purposes only and will not be disclosed by the agency in any way.
- **Contact Information**: Any changes to the contact information for the vendor organization and/or sponsoring agency, including the key contact person assigned to work with the DCJIS.

By January 15th of each year, criminal justice agencies must also report the following to the DCJIS. This information should be emailed to cjis.support@state.ma.us with a subject line of "Annual Vendor Report for {CITY/TOWN NAME}".

- **Vendor Personnel List:** An up-to-date list of vendor personnel as described above. At a minimum, this must include the person's name, state of residence, the date he/she started on the project, the date he/she signed the security addendum and individual disclosure agreement, the date fingerprinted, the date of last background record check/result, the date he/she successfully completed the CJIS security training, and the date he/she left the project (if applicable). See the Vendor Personnel List template available on mass.gov/CJIS for additional information.

Spot Audits and Site Visits

The DCJIS will conduct on-site audits of every CJIS agency on a triennial basis. As part of the audit, the DCJIS auditor(s) will check to ensure that the functionality being provided by the installed system(s) is in compliance with the currently approved scope, and to verify that all provisions of these guidelines are being met. This includes compliance with DCJIS and FBI security standards and policies.

Systems found to be out of compliance shall be subject to suspension of service, in addition to any and all sanctions that may be imposed by the DCJIS pursuant to state law and regulations, as well as to the terms and conditions of the CJIS User Agreement. In addition, if systems are found to be out of compliance, the DCJIS reserves the right to prevent the use of the product(s) in question at additional new sites. Finally, if systems are found to be out of compliance, the DCJIS reserves the right to terminate any further testing, and/or revoke the vendor's privileges to work with the DCJIS on future projects.

Additional Supporting Materials

The following materials are available to supplement the information provided in these CJIS Vendor Policy Guidelines. Please contact the CJIS Support Services Unit via phone at 617.660.4710 or via email at cjis.support@state.ma.us if you have questions or require additional information.

What	Where
Scope Proposal Template (including the Agency Support Letter)	mass.gov/CJIS
FBI CJIS Security Policy Information	mass.gov/CJIS
FBI Security Addendum	mass.gov/CJIS
Vendor Agreement of Non-Disclosure	mass.gov/CJIS
Individual Agreement of Non-Disclosure Form	mass.gov/CJIS
Authorized Vendor Personnel List Template	mass.gov/CJIS
VPN User Access Application Form	mass.gov/CJIS
CJIS Overview Broker Documentation	mass.gov/CJIS
CJIS Broker Authorization Form	mass.gov/CJIS
Additional CJIS Broker Documentation (WSDL, Schemas, etc.)	To be provided based to approved vendors (if required) based on approved scope.
Frequently Asked Questions	mass.gov/CJIS

Revision History

The CJIS Vendor Policy Guidelines document is a living document that is updated as required over time. Following is a summary of key changes made, including the date and nature of changes.

Date	Nature of Changes
08/17/2015	Updated guidelines to reflect current process and templates.
11/04/2014	Initial version.