Connecticut Justice Information System
Security Compliance Certification Form

The Connecticut Justice Information System Security Compliance Certification Form (CJIS-3) is used as a mechanism for municipalities, State and Federal agencies to certify their compliance with the *CJIS Security Requirements/Recommendations* as adopted by the Connecticut CJIS Governing Board. This form must be submitted to the Department of Information Technology (DoIT) CJIS Support Group annually on or before June 30th.

Location

Agency Name:	
Agency Address/Location Address:	
Agency Location Router IP Address:	
Internal IP Scheme/SubNet Mask:	

Certification 1 - Network Infrastructure

1.1 Firewalls – Refer to *CJIS Security Requirements/Recommendations* Section 1.

- **The CJIS portion of our agency's network segment is protected by a firewall.** **YES ☐ NO ☐**
- **This firewall is configured to allow only permissible protocols and traffic inherent to our agency's network environment.** **YES ☐ NO ☐**
- **This firewall is configured to perform logging and audit capability.** **YES ☐ NO ☐**
- **This firewall is configured to retain logs for a minimum of one (1) year.** **YES ☐ NO ☐**

Certification 2 - Workstations and Laptops

2.1 Hardware and Operating Systems – Refer to *CJIS Security Requirements/Recommendations* Section 4.

- **All workstations and laptops residing within our agency's CJIS network utilize an operating system presently supported by its manufacturer.** **YES ☐ NO ☐**
- **All workstations and laptops residing within our agency's CJIS network have been "OS hardened" to reduce vulnerabilities and mitigate potential risks.** **YES ☐ NO ☐**

2.2 Anti-Virus Program – Refer to *CJIS Security Requirements/Recommendations* Section 2.

- **All workstations and laptops residing within our agency's CJIS network are protected by a currently supported virus protection program.** **YES ☐ NO ☐**
- **There is a process in place for these workstations and laptops to receive virus patterns in an automated fashion.** **YES ☐ NO ☐**

2.3 Patch Management Process – Refer to *CJIS Security Requirements/Recommendations* Section 3.

- **All workstations and laptops residing within our agency's CJIS network are protected by a patch management program.** **YES ☐ NO ☐**
- **There is a process in place for these workstations and laptops to apply patches without user intervention.** **YES ☐ NO ☐**

2.4 Browsers Supporting 128 Bit Encryption – Refer to *CJIS Security Requirements/Recommendations* Section 6.

- **All deployed browsers within our agency's CJIS network are currently supported versions of Microsoft Internet Explorer and/or Netscape and support 128 bit or better encryption.** **YES ☐ NO ☐**

Certification 3 – LiveScan Devices

Check here ☐ if there are no LiveScan devices on your agency's CJIS network and proceed to Certification 4

3.1 Hardware and Operating Systems – Refer to *CJIS Security Requirements/Recommendations* Section 4.

- **All LiveScan devices residing within our agency's CJIS network utilize an operating system presently supported by its manufacturer.** **YES ☐ NO ☐**
- **All LiveScan devices residing within our agency's CJIS network utilize an operating system presently contracted for maintenance and support with its manufacturer.** **YES ☐ NO ☐**
- **All Livescan devices residing within our agency's CJIS network have been "OS hardened" to reduce vulnerabilities and mitigate potential risks.** **YES ☐ NO ☐**

3.2 Anti-Virus Program – Refer to *CJIS Security Requirements/Recommendations* Section 2.

- **All LiveScan devices residing within our agency's CJIS network are protected by a currently supported virus protection program.** **YES ☐ NO ☐**
- **There is a process in place for these LiveScan devices to receive virus patterns in an automated fashion.** **YES ☐ NO ☐**

3.3 Patch Management Process – Refer to *CJIS Security Requirements/Recommendations* Section 3.

- **All LiveScan devices residing within our agency's CJIS network are protected by a patch management program.** **YES ☐ NO ☐**
- **There is a process in place for these LiveScan devices to apply patches without user intervention.** **YES ☐ NO ☐**

Connecticut Justice Information System
Security Compliance Certification Form

Certification 4 - Servers

Check here ☐ if there are no servers on your agency's CJIS network and proceed to Certification 5

4.1 Operating Systems – Refer to *CJIS Security Requirements/Recommendations* Section 4.

- **All servers residing within our agency's CJIS network utilize an operating system presently supported by its manufacturer. YES ☐ NO ☐**
- **All servers residing within our agency's CJIS network utilize an operating system presently contracted for maintenance and support with its manufacturer. YES ☐ NO ☐**
- **All servers residing within our agency's CJIS network have been "OS hardened" to reduce vulnerabilities and mitigate potential risks. YES ☐ NO ☐**

4.2 Anti-Virus Program – Refer to *CJIS Security Requirements/Recommendations* Section 2.

- **All servers residing within our agency's CJIS network are protected by a currently supported virus protection program. YES ☐ NO ☐**
- **There is a process in place for these servers to receive virus patterns in an automated fashion. YES ☐ NO ☐**

4.3 Patch Management Process – Refer to *CJIS Security Requirements/Recommendations* Section 3.

- **All servers residing within our agency's CJIS network are protected by a patch management program. YES ☐ NO ☐**
- **There is a process in place for these servers to apply patches without user intervention. YES ☐ NO ☐**

Certification 5 - Physical Location

5.1 Physical Safeguards – Refer to *CJIS Security Requirements/Recommendations* Appendix A.

> Special Note: While the actual requirements of Appendix A are required for COLLECT devices only, it is the desire of the Security Committee of the CJIS Governing Board that a physical safeguard "best effort" exist on ALL devices that reside in an agency's CJIS network segment and access CJIS systems.

- **We believe that our agency has adequate physical safeguards in place to protect against unauthorized access or routine viewing of display devices or printed materials by unauthorized persons. YES ☐ NO ☐**
- **We believe that our agency has adequate physical safeguards in place to protect network and infrastructure components from unauthorized access. YES ☐ NO ☐**

Connecticut Justice Information System

Security Compliance Certification Form

Certification 6 - General

- **Our agency understands that noncompliance of any of these certifications may result in sanctions, as adopted by the CJIS Governing Board, being levied on our agency which may result in, but are not limited to, the removal of access rights to certain CJIS applications.** **YES ☐ NO ☐**
- **Our agency understands that our location may be subject to an audit by representative(s) of the DoIT CJIS Support Group upon no less than five (5) business days prior notification.** **YES ☐ NO ☐**
- **Our agency understands that any additional devices connected to the CJIS portion of our agency's network after the approval of this form must also comply with these certifications and are subject to the same policies.** **YES ☐ NO ☐**
- **Our agency understands that, upon return receipt of this form signed and approved by the DoIT CJIS Support Group, this agency is granted permission to access CJIS applications from any compliant device effective the date of the approving signature.** **YES ☐ NO ☐**

I HEREBY CERTIFY THAT, TO THE BEST OF MY KNOWLEDGE AND BELIEF, THE INFORMATION CONTAINED HEREIN IS TRUE AND CORRECT.

For the Agency

Certification Date:	
Certifying Individual Signature:	
Certifying Individual Printed Name:	
Certifying Individual eMail Address:	
Certifying Individual Phone Number:	
Agency Head Signature:	
Agency Head Printed Name:	

For the DoIT CJIS Support Group

Approval Date:	
Approving Individual Signature:	