Connecticut Justice Information System

Security Compliance Assessment Form

The Connecticut Justice Information System Security Compliance Assessment Form (CJIS-2) is used as a mechanism for municipalities, State and Federal agencies to assess their compliance with the *CJIS Security Requirements & Recommendations* as adopted by the State of Connecticut CJIS Governing Board. This form may be used as an internal document for an agency to assess their present level of compliance and subsequently perform necessary changes to attain compliance or submitted to the Department of Information Technology (DoIT) CJIS Support Group for assistance in attaining compliance.

Location

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

Assessment 1 - Network Infrastructure

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

- **Is the CJIS portion of your agency's network segment protected by a firewall?**
  YES □ NO □ UNKNOWN □
- **Is this firewall configured to allow only permissible protocols and traffic inherent to your agency's network environment?** **YES □ NO □ UNKNOWN □**
- **Is this firewall configured to perform logging and audit capability?**
  YES □ NO □ UNKNOWN □
- **Is this firewall configured to retain logs for a minimum of one (1) year?**
  YES □ NO □ UNKNOWN □

Connecticut Justice Information System
Security Compliance Assessment Form

Assessment 2 - Workstations and Laptops

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

- **How many total workstations and laptops are in your network environment?** ______
- **How many of these are COLLECT certified devices?** ______
- **How many utilize each of the following operating systems?**
  - **Windows 3.1*** ______
  - **Windows 95*** ______
  - **Windows 98 Standard Edition*** ______
  - **Windows 98 Second Edition*** ______
  - **Windows Millennium Edition*** ______
  - **Windows NT Workstation 4.xx*** ______
  - **Windows 2000 Professional** ______
  - **Windows XP Professional** ______
  - **Windows XP Home** ______
  - **Other** ______ **Please specify:** ____________________________
  - **Other** ______ **Please specify:** ____________________________

**Security hot fixes for this release are no longer supported by Microsoft*

- **Is each of the above devices and its operating system presently under contract for maintenance and support with its manufacturer?** YES □ NO □ UNKNOWN □
- **Have you performed "OS Hardening" on each of the above devices to reduce vulnerabilities in the computer hardware and operating system?** YES □ NO □ UNKNOWN □

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

- **Are all workstations and laptops residing within your agency's CJIS network protected by a currently supported virus protection program?** YES □ NO □ UNKNOWN □
- **Does the Anti-Virus program on each workstation and laptop receive virus signature updates automatically?** YES □ NO □ UNKNOWN □
  - **If NO, please explain any existing process**

____

____

____

____

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

- **Are all workstations and laptops residing within your agency's CJIS network protected by a patch management program?** **YES** □ **NO** □ **UNKNOWN** □
- **Does the patch management application receive updates automatically?** **YES** □ **NO** □ **UNKNOWN** □
  - **If NO, please explain any existing process**

    ____

    ____

    ____

    ____

- **Are these patches applied to each workstation and laptop through an automated process?** **YES** □ **NO** □ **UNKNOWN** □
  - **If NO, please explain any existing process**

    ____

    ____

    ____

    ____

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

- **How many total workstations and laptops are browser enabled?** ______
- **How many utilize each of the following browsers?**
  - **Internet Explorer 5.01 or lower*** ______
  - **Internet Explorer 5.5*** ______
  - **Internet Explorer 6** ______
  - **Netscape 6.x+** ______
  - **Netscape 7.x** ______
  - **Netscape 8.x** ______
  - **Other** ______ **Please specify:** ____________________
  - **Other** ______ **Please specify:** ____________________

**Security hotfixes for this release are no longer supported by Microsoft*

+*Security hotfixes for this release are no longer supported by Netscape*

Connecticut Justice Information System

Security Compliance Assessment Form

Assessment 3 – LiveScan Devices

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

- **How many LiveScan devices are in your network environment?** ______
  (*if "0", proceed to Assessment 4*)
- **Which vendor(s) manufacturer the LiveScan(s)?**
  - **Please specify:** ____
  - **Please specify:** ____
  - **Please specify:** ____

- **How many utilize each of the following operating systems?**
  - **Windows NT Workstation 4.xx*** ______
  - **Windows 2000 Professional** ______
  - **Windows XP Professional** ______
  - **Windows XP Home** ______
  - **Other** ______ **Please specify:** ____________________________
  - **Other** ______ **Please specify:** ____________________________
  - **Other** ______ **Please specify:** ____________________________
  - **Unknown** ______

  Security hot fixes for this release are no longer supported by Microsoft

- **Is each of the above LiveScan devices and its operating system presently under contract for maintenance and support with its manufacturer?**
  YES □ NO □ UNKNOWN □
- **Have you or the manufacturer(s) performed "OS Hardening" on each of the above LiveScan devices to reduce vulnerabilities in the computer hardware and operating system?**
  YES □ NO □ UNKNOWN □

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

- **Are all LiveScan devices residing within your agency's CJIS network protected by a currently supported virus protection program?** **YES □ NO □ UNKNOWN □**
- **Does the Anti-Virus program on each LiveScan device receive virus signature updates automatically?** **YES □ NO □ UNKNOWN □**
  - **If NO, please explain any existing process**

    ____

    ____

    ____

    ____

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

- **Are all LiveScan devices residing within your agency's CJIS network protected by a patch management program?** **YES □ NO □ UNKNOWN □**
- **Does the patch management application receive updates automatically?** **YES □ NO □ UNKNOWN □**
  - **If NO, please explain any existing process**

    ____

    ____

    ____

    ____

- **Are these patches applied to each LiveScan device through an automated process?** **YES □ NO □ UNKNOWN □**
  - **If NO, please explain any existing process**

    ____

    ____

    ____

    ____

<u>Assessment 4 - Servers</u>

<u>4.1 Hardware and Operating Systems</u> – Refer to *CJIS Security Requirements & Recommendations* Section 4.

- **How many total servers are in your network environment?** ______
  (*if "0", proceed to Assessment 5*)
- **How many utilize each of the following operating systems?**
  - **Windows NT Server 4.xx**[*] ______
  - **Windows 2000 Server** ______
  - **Windows Server 2003** ______
  - **Other** ______ **Please specify:** ____________________________
  - **Other** ______ **Please specify:** ____________________________
  - **Other** ______ **Please specify:** ____________________________
  - **Other** ______ **Please specify:** ____________________________
  - **Other** ______ **Please specify:** ____________________________
  - **Other** ______ **Please specify:** ____________________________

[*] *Security hotfixes for this product are no longer supported by Microsoft*

- **Is each of the above servers and its operating system presently under contract for maintenance and support with its manufacturer?** **YES □ NO □ UNKNOWN □**
- **Have you performed "OS Hardening" on each of the above servers to reduce vulnerabilities in the computer hardware and operating system?** **YES □ NO □ UNKNOWN □**

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

- **Are all servers residing within your agency's CJIS network protected by a currently supported virus protection program?** **YES □ NO □ UNKNOWN □**
- **Does the Anti-Virus program on each server receive virus signature updates automatically?** **YES □ NO □ UNKNOWN □**
  - **If NO, please explain any existing process**

____

____

____

____

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

- **Are all servers residing within your agency's CJIS network protected by a patch management program?** **YES □ NO □ UNKNOWN □**
- **Does the patch management application receive updates automatically?** **YES □ NO □ UNKNOWN □**
  - **If NO, please explain any existing process**

____

____

____

____

- **Are these patches applied to each server through an automated process?** **YES □ NO □ UNKNOWN □**
  - **If NO, please explain any existing process**

____

____

____

____

Connecticut Justice Information System
Security Compliance Assessment Form

Assessment 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 only for COLLECT devices, it is the desire of the Security Committee of the CJIS Governing Board that “best effort” physical safeguards be in place for ALL devices that reside in an agency’s CJIS network segment and access CJIS systems.

- **Does your agency have adequate physical safeguards in place to protect against unauthorized access or routine viewing of display devices or printed materials by unauthorized persons?** **YES □ NO □ UNKNOWN □**
  - **If NO, please explain**

____

____

____

____

- **Does your agency have adequate physical safeguards in place to protect network and infrastructure components from unauthorized access?** **YES □ NO □ UNKNOWN □**
  - **If NO, please explain**

____

____

____

____

For the Agency/Location

Assessment Date:	
Assessing Individual Signature:	
Assessing Individual Printed Name:	
Assessing Individual eMail Address:	
Assessing Individual Phone Number:	