

Security Requirements & Recommendations

Section 1 - Firewall

- Networks requiring access to CJIS applications must be protected by firewall devices configured explicitly to allow only permissible protocols and traffic inherent in the networked environment. Configuration must provide a point of defense with controlled access from both inside and outside the CJIS network. The device must provide logging and audit capability.

<u>Platforms Impacted:</u>	Network Infrastructure
<u>Implementation Status:</u>	Required
<u>Implementation Priority:</u>	Immediate
<u>FBI CJIS Compliance Reference:</u>	7.10

Section 2 - Anti-Virus Program

- All servers and workstations must be protected by a comprehensive Anti-Virus program. The Anti-Virus software must be configured to receive automatic virus pattern updates. Virus scanning must be configured to execute scanning processes without user intervention.

<u>Platforms Impacted:</u>	Workstations, Laptops, Servers and Simple Mail Transfer Protocol (SMTP) Gateways
<u>Implementation Status:</u>	Required
<u>Implementation Priority:</u>	Immediate
<u>FBI CJIS Compliance Reference:</u>	7.12

Section 3 - Patch Management Process

- All servers and workstations must be protected by a patch management program. Servers and workstations must be enabled to receive distributed operating system upgrades, patches and hotfixes without user intervention. All updates must be certified in a test environment prior to distribution.

<u>Platforms Impacted:</u>	Workstations, Laptops and Servers
<u>Implementation Status:</u>	Required
<u>Implementation Priority:</u>	Immediate
<u>FBI CJIS Compliance Reference:</u>	None

Security Requirements & Recommendations

Section 4 - Operating System

- Only servers and workstations with operating systems having a current support commitment by the manufacturer will be allowed to reside within a CJIS network.
- Implement processes to support “Best Practices” to reduce vulnerabilities in computer hardware and operating systems. This is commonly known as “OS Hardening.” (e.g. turning off services that are not being utilized)

<u>Platforms Impacted:</u>	Workstations, Laptops and Servers
<u>Implementation Status:</u>	Required
<u>Implementation Priority:</u>	Immediate
<u>FBI CJIS Compliance Reference:</u>	None

Section 5 - 128 Bit Encryption

- All newly developed CJIS applications must adopt 128 bit encryption that meets NIST, CSL certification of the cryptographic module. Currently, 128 bit encryption is required with the higher standard NIST, CSL requirement being effective on September 20, 2010.

<u>Platforms Impacted:</u>	All CJIS Applications
<u>Implementation Status:</u>	Required
<u>Implementation Priority:</u>	Immediate
<u>FBI CJIS Compliance Reference:</u>	7.8

Section 6 - Browsers

- Only versions of Microsoft Internet Explorer and Netscape having a current support commitment by the manufacturer will be allowed to reside within a CJIS network.
- Only versions of Microsoft Internet Explorer and Netscape supporting 128 bit encryption or better are permitted.

<u>Platforms Impacted:</u>	Workstations and Laptops Accessing CJIS Applications
<u>Implementation Status:</u>	Required
<u>Implementation Priority:</u>	Immediate
<u>FBI CJIS Compliance Reference:</u>	None

Security Requirements & Recommendations

Section 7 - Multiple Browser Sessions

- Concurrent browser sessions open to internet sites while accessing any CJIS application are strictly prohibited.

<u>Platforms Impacted:</u>	Workstations and Laptops Accessing CJIS Applications
<u>Implementation Status:</u>	Required
<u>Implementation Priority:</u>	Immediate
<u>FBI CJIS Compliance Reference:</u>	None

Section 8 - Intrusion Detection

- All CJIS network environments should be protected by an intrusion detection system. Such systems examine information from a number of system and network sources then analyze the information for signs of intrusion (attacks aimed at the organization) and misuse
- All servers residing inside a CJIS subnet should be protected by host intrusion detection software.

<u>Platforms Impacted:</u>	Networks and Servers
<u>Implementation Status:</u>	Recommended
<u>Implementation Priority:</u>	None
<u>FBI CJIS Compliance Reference:</u>	None

Section 9 - Content Filtering

- All CJIS network environments hosting E-mail platforms and internet access points should implement content filtering tools to mitigate risk associated with viruses and OS vulnerability exploits.

<u>Platforms Impacted:</u>	None (Content filtering tools are normally installed on a server/workstation and interface with the internet access point or E-mail platform)
<u>Implementation Status:</u>	Recommended
<u>Implementation Priority:</u>	None
<u>FBI CJIS Compliance Reference:</u>	None

Security Requirements & Recommendations

Appendix A - Additional COLLECT Requirements

Items below are the sole responsibility of the Department of Public Safety and are NOT subject to CJIS Governing Board oversight

- **Security Requirements** – Existing or proposed environments that will include COLLECT devices must meet or exceed the security recommendations as outlined by this document.
- **Device Authentication** – Access control lists presently maintained by DoIT will continue to be utilized to authenticate devices authorized to access COLLECT.
- **Certified COLLECT Device** – COLLECT access will only be allowed by certified COLLECT devices. Once certified, Public Safety will request that DoIT add the device to appropriate access control lists.
- **Internet and E-mail access** – Internet and E-mail access from COLLECT devices will only be allowed after compliance with the COLLECT Unit's request process.
- **Physical Safeguards** – The computer site and related infrastructures (*e.g.* information systems servers, controlled interface equipment, associated peripherals, communications equipment which provides access to the CJIS network) must have adequate physical security at all times to protect against unauthorized access to, or routine viewing of, computer devices, access devices, and printed and stored data.

Security Requirements & Recommendations

Appendix B - Glossary of Terms

Access Control - The process that limits and controls access to resources of a computer system; a logical or physical control designed to protect against unauthorized entry or use.

Access Rights - Also called permissions or privileges, these are the rights granted to users by the administrator or supervisor. Access rights determine the actions users can perform (e.g., read, write, execute, create and delete).

Antivirus software - Applications that detect, prevent and possibly remove all known viruses from files located in a microcomputer hard drive.

Authentication - The act of verifying the identity of a user and the user's eligibility to access computerized information. Authentication is designed to protect against fraudulent logon activity. It also can refer to the verification of the correctness of a piece of data.

Client/Server - A group of computers connected by a communications network, where the client is the requesting machine and the server is the supplying machine. Software is specialized at both ends. Processing may take place on either the client or the server, but it is transparent to the user.

Data Security - Those controls that seek to maintain confidentiality, integrity and availability of information.

Encryption - A technique used to protect the plaintext, by coding the data so it is unintelligible to the reader.

Firewall - A device that enforces security policies for traffic traversing to and from different network segments. A firewall no longer only protects an organization from the Internet, but also protects sensitive segments within organizations.

Intrusion Detection System - Host Based - consists of an agent on a host which identifies intrusions by analyzing system calls, application logs and host activities.

Intrusion Detection System - Network - is an independent platform which identifies intrusions by examining network traffic and monitors multiple hosts. Network Intrusion Detection Systems gain access to network traffic by connecting to a hub, network switch configured for port mirroring, or network tap. An example of a NIDS is Snort (<http://www.snort.org>).

Local Area Network (LAN) - Communications networks that server several users within a specified geographical area. Personal computer LANs functions as distributed processing systems in which each computer in the network does its own processing and manages some of its data. Shared data are stored in a file server that acts as a remote disk drive for all users in the network.

Operating System - A master control program that runs the computer and acts as a scheduler and traffic controller. It is the first program copied into the computer's memory after the computer is turned on and must reside in memory at all times. It sets the standards for the applications programs that run in it.

OS Hardening - The process of executing standard security procedures on computer operating systems for the purposes of remediating known vulnerabilities and weaknesses in default installations.

Virus - Malicious programs designed to spread and replicate from computer to computer through telecommunications links or through sharing of computer diskettes and files.

Wide Area Network (WAN) - A computer network connecting different remote locations that may range from short distances, such as a floor or building, to extremely long transmission that encompass a large region or several countries.