# Criminal Justice Information Services (CJIS) Compliance Solutions

*Media and Systems Protection, Integrity and Accountability*

*Whitepaper*


**GreenTec™**

22375 Broderick Drive, Suite 155

Sterling, VA 20166

www.GreenTec-USA.com

# Table of Contents

# Introduction

The Criminal Justice Information Services (CJIS) Security Policy (CJISD-ITS-DOC-08140-5.5) provides guidance to law enforcement and other agencies for timely and secure access to services and data and the creation, viewing, modification, transmission, dissemination, storage, and destruction of Criminal Justice Information (CJI).

Technologies described were initially developed for DOJ video surveillance programs to ensure the integrity of digital evidence and to simplify immutable chain of custody issues. The uniqueness of this technology is that the cyber protections reside at the lowest level in the security stack, inside of the disk drive itself with the data bits, there is no layer in-between. Since this hardware-level solution is inside of the disk drive and travels with the disk wherever it goes, it cannot be bypassed or circumvented, regardless of operating system used, or access permissions.

Further enhancement of the secure data storage technologies beyond video applications enabled adoption for protection of various types of data including financial, legal, audit records, documents, "gold images" of software and data, archives, system backups, disaster recovery, data integrity, governance compliance, records retention and other applications requiring immutable data and system integrity.

# CJIS Compliance Overview

In addition to the CJIS Security Policies, the law enforcement community recognizes and adopts guidance from the National Institute of Standards and Technology (NIST) and other standards organizations. The technology described below has been selected by the NIST National Cybersecurity Center of Excellence (NCCoE) as a key building block for their Data Integrity Project. This technology protects systems from cyber-attacks that may render the system unbootable, and protects data from various types of intentional or accidental alteration and deletion as well as insider threats and viruses.

In addition to being part of the NIST Data Integrity Project, the Defense Information Systems Agency (DISA) has tested and validated these technologies, and they have produced a report entitled "Assessment Report GreenTec WORMdisk and CYBERdisk" that states: *"The GreenTec WORMdisk product allows for permanent unchangeable storage of data onto a hard disk medium. The CYBERdisk product allows for protection of a boot hard disk where the Master Boot Record (MBR) is unalterable. The two products perform as advertised."*

This technology has also been tested by Dell on their Generation 13 and 14 servers, and is available for demonstration in the Dell Solutions Center (DSC) in Reston, Virginia.

## Media Protection

Immutable storage guarantees the integrity of digital evidence, audit records, investigation records, case management files and other critical data, thereby ensuring that it cannot be altered, modified, sabotaged, manipulated or deleted. Placing data onto immutable storage provides assurance that the data has not been tampered with, and proves the authenticity and admissibility of the evidence in the courtroom.

WORMdisks™ are the only storage media that exceeds the CJIS requirements to securely store, retain and protect electronic records from disclosure, modification, sabotage, manipulation, alteration, deletion and re-formatting. WORMdisks™ use standard interfaces, file systems and file formats, are plug-and-play, perform as typical disks, are operating system and application compatible, and are available as a single USB attached enclosure, internal disk drives, network attached storage, and as rack mount servers, ranging from 500GB up to multiple Petabytes.

WORMdisks™ provide three types of media protection to support a variety of CJI use cases:

- **Temporary Protection** allows data to be written to the WORMdisk™ and write protected so applications may not alter, delete or add data, until it is un-protected by an authorized user. Once un-protected, you can again write more data.
- **Incremental Permanent Protection** allows data to be written with permanent protection for all data written up to that point. Additional data may be written and then incrementally protected again. When incremental protection is enforced, no modifications may be made to files written up to that point and no files may be deleted, changed or re-formatted.
- **Permanent Full Disk Protection** may be used at any time to protect contents of the entire physical disk from modification, alteration, deletion, modification and re-formatting.

## Critical Systems Protection

A vulnerable part of all systems is the operating system boot disk. Critical systems have been destroyed by common cyber-attacks that destroy or modify the sensitive Master Boot Record (MBR) and partition tables. These attacks have destroyed many thousands of systems that have crippled organizations like Sony Entertainment, Aramco Oil, banks, law enforcement agencies, hospitals and other organizations.

CYBERdisks™ are the only disk technology that permanently protects these sensitive areas of the OS boot disk and provides additional protections against other viruses and malicious code including firmware viruses that are not detectable with anti-virus scanning tools.

## Auditing and Accountability

An important component for CJIS compliance is the recording and retention of critical audit records. The last steps that a hacker performs when penetrating a system is to cover his tracks by deleting audit entries in the system log files. Once this is done, it is nearly impossible to determine the attack vector and discover where the hacker came from and what systems he has entered or damaged.

WORMdisks™ are the only storage media that provides an easy to use capability to permanently record and retain audit records for any retention period for full compliance to section 5.4 of the CJIS requirements.

# CJIS Policy Areas Addressed

Key CJIS policy areas that are addresses by GreenTec-USA and WORMdisk™ technologies are outlined in the following sections.

## Policy Area 2: Security Awareness Training

GreenTec-USA provides on-site, off-site, video-based and web-based training in each of the four categories security awareness categories including:

### Level One Security Awareness Training

Responsibilities and behavior for CJI usage and/or terminals, implications of noncompliance, incident response, visitor control, access to spaces, physical security policies and procedures.

### Level Two Security Awareness Training

Media protection and safeguarding procedures, usage, handling and marking of CJI, threats, vulnerabilities, risks of CJI, social engineering threats, dissemination and media destruction, proper handling of archived and backup media.

### Level Three Security Awareness Training

Information and system usage rules for laptops, handheld devices, desktops, servers, personally-owned systems and cloud-based systems, individual responsibilities, accountability and expected behavior, access controls, password usage and management, protection from viruses, worms, Trojan horses, and malicious code, proper handling of unknown e-mail, attachments and spam, web usage policies, activity monitoring, physical security risks to systems and data, physical and wireless security for handheld devices, encryption and

transmission of sensitive/confidential information, agency policies, procedures, and points of contact for assistance

### Level Four Security Awareness Training

System, security, network administrators and other information technology personnel to be trained on virus, worms, Trojan horses and malicious code protection policies and procedures including intrusion detection, anti-virus scanning, security, system and application patches and maintenance updates, system and data backup, storage access control policies and procedures and network infrastructure protections.

## Policy Area 4: Auditing and Accountability

Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior. Agencies shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.

| CJIS Requirement # | Description of Requirement | GreenTec-USA Solution |
|---|---|---|
| **5.4.5 Protection of Audit Information** | The agency's information system shall protect audit information and audit tools from modification, deletion and unauthorized access. | By having security protections build into the hardware-level with WORMdisks™, they uniquely protect audit information and audit tools, applications and executables from modification, deletion, sabotage, manipulation and unauthorized access. |
| **5.4.6 Audit Record Retention** | The agency shall retain audit records for at least one (1) year. Once the minimum retention time period has passed, the agency shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions. | WORMdisk technologies allow for varying user-defined retention periods and ensure that no data could have ever been altered, changes, sabotaged, manipulated or deleted throughout that retention period. Automated software tools allow the retention period to be specified in |

| | | |
|---|---|---|
| | | years, months, weeks, days or specific dates. When the retention period expires, a pop-up message is displayed and email alerts are sent to the administrator, who may dispose or extend the retention period. |

## Policy Area 8: Media Protection

Media protection policy and procedures shall be documented and implemented to ensure that access to digital and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media.

| CJIS Requirement # | Description of Requirement | GreenTec-USA Solution |
|---|---|---|
| **5.8.2.1 Digital Media during Transport** | Controls shall be in place to protect digital media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in Section 5.10.1.2 of this Policy, is the optimal control during transport; however, if encryption of the data isn't possible then each agency shall institute physical controls to ensure the security of the data. | WORMdisks are the only technology that provide both protection from modification, as well as protection from disclosure (encryption) for data, whether at rest, or in transport. Encryption alone does not protect data from deletion or modification. For example, encrypted data may be deleted or re-encrypted by crypto viruses like Ransomware. However, when using WORMdisks, data is protected from these vulnerabilities. |
| **5.8.3 Digital Media Sanitization and Disposal** | The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or | Expired WORMdisk digital media may be sanitized via a secure crypto erase, or degaussing, or be destroyed by shredding. Software tools generate and retain destruction certificates identifying witnesses of the |

| | | |
|---|---|---|
| | destruction is witnessed or carried out by authorized personnel. | sanitization or destruction by authorized personnel. |

## Policy Area 10: System and Communications Protection and Information Integrity

Examples of systems and communications safeguards range from boundary and transmission protection to securing an agency's virtualized environment. In addition, applications, services, or information systems must have the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information.

| CJIS Requirement # | Description of Requirement | GreenTec-USA Solution |
|---|---|---|
| **5.10.1.2 Encryption** | Commonly available encryption tools often use a key to unlock the cipher to allow data access; this key is called a passphrase. While similar to a password, a passphrase is not used for user authentication. Additionally, the passphrase contains stringent character requirements making it more secure and thus providing a higher level of confidence that the passphrase will not be compromised. | WORMdisks support various FIPS 140-2 compliant encryption technologies using strong passphrase technologies for secure data access. |
| **5.10.1.3 Intrusion Detection Tools and Techniques** | The agency shall implement network-based and/or host-based intrusion detection tools. The CSA/SIB shall, in addition:<br>1. Monitor inbound and outbound communications for unusual or unauthorized activities.<br>2. Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort.<br>3. Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks. | WORMdisks are the only disk drive technology that supports multiple types of real-time intrusion detection. 1). When data tampering is attempted, log entries are generated identifying the attempted intrusion, and the attempt is aborted. 2). At the electronic level, where a tamper detect is sensed if the device is disassembled and an attempt is made to substitute other components in an effort to bypass security controls. 3). A physical tamper resistant label makes it visually obvious that the device has been tampered with. |

| | | |
|---|---|---|
| **5.10.3 Partitioning and Virtualization** | As resources grow scarce, agencies are increasing the centralization of applications, services, and system administration. Advanced software now provides the ability to create virtual machines that allows agencies to reduce the amount of hardware needed. Although the concepts of partitioning and virtualization have existed for a while, the need for securing the partitions and virtualized machines has evolved due to the increasing amount of distributed processing and federated information sources now available across the Internet. 06/01/2016 CJISD-ITS-DOC-08140-5.5 56 | WORMdisks™ provide an easy means to maintain a "Gold Image" of the virtualized system, partitions and required baseline data to be used for virtual machines. This ensures that no virus or malware could have been injected into the virtual machine image or partitions. |
| **5.10.4.2 Malicious Code Protection** | The agency shall implement malicious code protection that includes automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet shall implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available).<br><br>The agency shall employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network. The agency shall ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed. | WORMdisks™ provide the unique capability to ensure that no malicious code could have been inserted into system images. Viruses, worms, Trojan horses and firmware modification are all prevented by WORMdisks™. Further, damage to data cause by malicious code, crypto viruses, human error and insider threats are prevented with WORMdisks™. |

## Other Considerations for System and Data Protection and Information Integrity

Additional examples of capabilities above and beyond the CJIS requirements to ensure protection and safeguarding of systems and data are described below. Digital evidence needs to be protected to ensure establishment of chain of custody and that digital evidence cannot be sabotaged, modified, deleted, or altered in any way. Further, in cloud based environments it is critical to ensure that the original digital evidence may be presented in court. WORMdisks™ as edge-node storage provide a mapping of user data to one or more specific disks, allowing delivery of the original digital evidence saved to cloud-based deployments.

## Criminal Justice Information Services (CJIS) Compliance Solutions

| CJIS Application | Description of Requirement | GreenTec-USA Solution |
|---|---|---|
| Chain of Custody | When digital evidence is collected, it must be tracked for the seizure, custody, control, transfer, analysis, and disposition of evidence. When digital evidence is collected onto immutable storage, this helps prove the authenticity and admissibility of the evidence in the courtroom. | Due to being unalterable, WORMdisks™ provide a simplified chain-of-custody from the point of seizure, collection and preservation, thereby ensuring bulletproof data immutability regardless of handling, control or transfer limitations. |
| Original Digital Evidence | Presentation of Original Digital evidence is critical in a courtroom because digital evidence may be altered when it is copied. Establishment of the originality of the evidence ensures that it has not be tampered with or altered in any way. | WORMdisks™ ensure that digital evidence that has been collected cannot ever be altered, modified, deleted or re-formatted. Common use of hashing does not prevent digital evidence from be deleted, or from the disk being re-formatted. Further, modification of digital evidence and generation of a new hash value and replacement of the original hash value may lead to the conclusion that data was not modified, when in fact is was. |
| Detection of Data Attacks | Preemptive detection when attempts are made to modify or alter data and sensitive system areas of the OS disk drive. | When attempts are made to modify or alter data stored onto WORMdisks™, the attempt is detected and logged, thereby providing an alert of the hack attack. |

# Conclusions

CJIS requirements encompass a wide range of requirements spanning from policies and procedures for information exchange, security, dissemination, auditing and accountability, logging, validation, system use, training, monitoring, physical security, incident response, access controls, identification and authorization, configuration management, media storage and protection, information integrity, personnel security and mobile devices.

While many of these areas are policy and procedural driven and ay require specialized software or trained personnel to expend a significant amount of labor, the sections above describe some areas of CJIS compliance that may be easily addressed with simple automated technologies.

One example of a simplified automated solution is the use of CYBERdisks™ to provide system integrity protecting sensitive areas of the operating system from damage, thereby enabling the system to survive a cyber-attack on the MBR, partition tables and disk firmware. Use of a CYBERdisk™ is as simple as using any other common disk for the operating system, but continuous protection prevents damage and improves system integrity, reliability and availability.

Another example is the use of WORMdisks™ to protect data from sabotage, modification, alteration, deletion, re-formatting, ransomware, firmware viruses, human error and insider threats. WORMdisks™ behave like ordinary disks but provide continuous data protection, thereby allowing data to survive accidental or intentional attacks and hence improving data integrity, reliability and availability.

WORMdisks™ and CYBERdisks™ are available as single standalone internal or external USB disks, local or networked storage, rack mounted server solutions and also available in the cloud from any device including smart phones and body-worn cameras.

For further information, please email to info@greentec-usa.com or call (703) 880-8332.