Aligning Certes Quantum Safe DPRM with CJIS Security Policy Version 6.0 for Agency Compliance

The Criminal Justice Information Services (CJIS) Security Policy Version 6.0, released on January 22, 2025, establishes rigorous standards for safeguarding Criminal Justice Information (CJI). Compliance is mandatory for entities accessing FBI CJIS systems, including criminal justice agencies (CJAs), noncriminal justice agencies (NCJAs), and contractors. The policy is structured into policy areas that correspond to NIST SP 800-53 control families, ensuring a holistic approach to CJI protection.

Certes' Data Protection and Risk Mitigation (DPRM) solution, built on four pillar, Data-Centric Security, Policy and Key Management, Layer 4 Payload Protection, and Unified Reporting is engineered to help agencies achieve CJIS compliance. This whitepaper explores how DPRM aligns with key CJIS policy areas: System and Communications Protection, Access Control, Audit and Accountability, Incident Response, and Cloud Service providers. Each section outlines how DPRM addresses specific controls, resolves agency challenges, and delivers benefits in terms of compliance, security, and operational efficiency in a FIPS Certified form.

Summary of Benefits to Agencies

Before delving into each policy area, here's a summary of benefits of how Certes DPRM supports agencies under CJIS Version 6.0:

- **Key Ownership:** Agency ownership of Centralized policy and key management to meet mandatory authentication and cryptographic standards across multiple policy areas.
- **Enhanced Data Security:** Encrypts CJI in transit, mitigating risks of interception or tampering, across trusted and untrusted networks from local to cloud.
- **Operational Efficiency:** Automates reporting and monitoring, reducing administrative overhead.

- **Architectural Flexibility:** Operates across diverse networks, supporting legacy and modern systems alike.
- **FIPS Quantum Safe Encryption:** DPRM provides quantum-safe data encryption, and quantum key distribution adhering to current NIST & FIPS standards.
- **Quick and Simple to Deploy:** As a bump in the wire the Certes Enforcement Point is simple to deploy into existing architectures without complex changes needing to be designed in.

These advantages make DPRM a strategic asset for agencies navigating CJIS requirements as demonstrated by multiple agencies using Certes to protect CJI over shared networks.

Policy Area: System and Communications Protection

This analysis evaluates DPRM's alignment with CJIS obligations for agencies, addressing the important sections which Agencies usually struggle with during an audit.

Overview

The System and Communications Protection policy area ensures CJI's confidentiality, integrity, and availability during transmission. Key controls include:

- **SC-8: Transmission Confidentiality and Integrity:** Requires cryptographic protection for CJI to prevent unauthorized changes or access.
- **SC-12 : Cryptographic Key Establishment and Management:** Mandates that crypto key generation, distribution, storage, access and destruction is controlled by the agency.
- **SC-13: Cryptographic Protection:** Mandates cryptographic mechanisms to safeguard CJI transmitted outside secure boundaries.

> **Compliance shouldn't come at the cost of complexity. Certes DPRM empowers agencies with control over their cryptographic keys, real-time auditing, and zero-trust network protection—delivering CJIS-aligned security that's as easy to deploy as it is powerful in practice.**
>
> *Simon Pamplin – CTO, Certes*

How DPRM Aligns and Solves Challenges

- **SC-8 and SC-13:** DPRM's Data-Centric Security and Layer 4 Payload Protection encrypt CJI at the data level within network packets using FIPS 140-3 compliant Quantum Safe 256-bit AES encryption. This ensures CJI remains secure across untrusted networks, addressing the challenge of maintaining security in diverse or complex infrastructures.

- **SC-12:** DPRM Customer Controlled Keys capability, gives an agency Administrator the ability to define part of the key material used for encryption. This means ONLY the agency can define what is protected giving them full control over management of the keys.

- **Related Controls:** DPRM enhances SC-7: Boundary Protection by encrypting data crossing network boundaries, reducing reliance on traditional perimeter defences like firewalls or VPNs.

Policy Area: Access Control

Overview

The Access Control policy area restricts CJI access to authorized individuals. Key controls include:

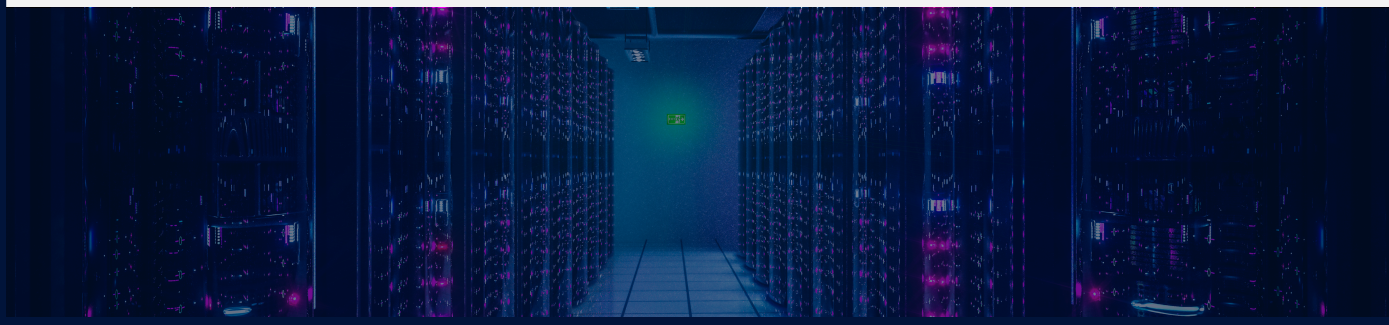
- **AC-6(1): Least Privilege:** Limits access to the minimum necessary for job functions.
- **AC-17: Remote Access**: Ensures secure remote access to CJI.

How DPRM Aligns and Solves Challenges

- **AC-6(1):** DPRM enforces role-based access to DPRM configuration, restricting access to administrators authorised to control and manage keys for that security function.
- **AC-17(2):** DPRM secures remote access by encrypting CJI in transit, overcoming vulnerabilities in remote operations without needing VPNs.

Benefits to Agencies

- Granular access controls minimize data exposure risks limiting system configuration to authorized individuals only.



Policy Area: Audit and Accountability

Overview

The Audit and Accountability policy area mandates logging and monitoring of security events. Key controls include:

- **AU-2: Event Logging:** Requires logging of security-relevant events.
- **AU-6: Audit Record Review, Analysis, and Reporting:** Demands regular audit record analysis.

How DPRM Aligns and Solves Challenges

- **AU-2:** DPRM's Unified Reporting logs all encryption activities, and system security events, providing a robust audit trail and addressing gaps in visibility.
- **AU-6:** DPRM integrates with SIEM systems for automated audit analysis and reporting, simplifying the review process.
- **Related Controls:** DPRM supports AU-12: Audit Record Generation by producing detailed logs compliant with CJIS standards.

Benefits to Agencies

- Comprehensive audit trails streamline compliance audits.
- Automated reporting reduces preparation time, boosting operational efficiency.

Policy Area: Incident Response

Overview

The Incident Response policy area focuses on detecting, reporting, and responding to security incidents. Key controls include:

- **IR-6:** Incident Reporting: Requires timely incident reporting to the CSO, SIB Chief, or Interface Agency Official.

How DPRM Aligns and Solves Challenges

- **IR-6:** DPRM offers real-time monitoring of protected CJI in transit, enabling industry standard SIEMS to report within CJIS timelines and overcoming delays in incident identification.
- **Related Controls: DPRM enhances IR-4:** Incident Handling with detailed logs and reports for effective investigation of encrypted traffic.

Benefits to Agencies

- Faster incident detection and response minimize CJI exposure.
- Automated reporting ensures compliance with reporting deadlines, avoiding penalties.

> **With the release of CJIS Security Policy Version 6.0, agencies face increasing pressure to safeguard criminal justice data against both today's threats and tomorrow's quantum risks. Certes DPRM is purpose-built to deliver on this mandate—ensuring complete data sovereignty, seamless compliance, and quantum-safe encryption without disrupting existing infrastructure.**
>
> *Paul German – CEO, Certes*

Policy Area: Cloud Service Providers

Overview

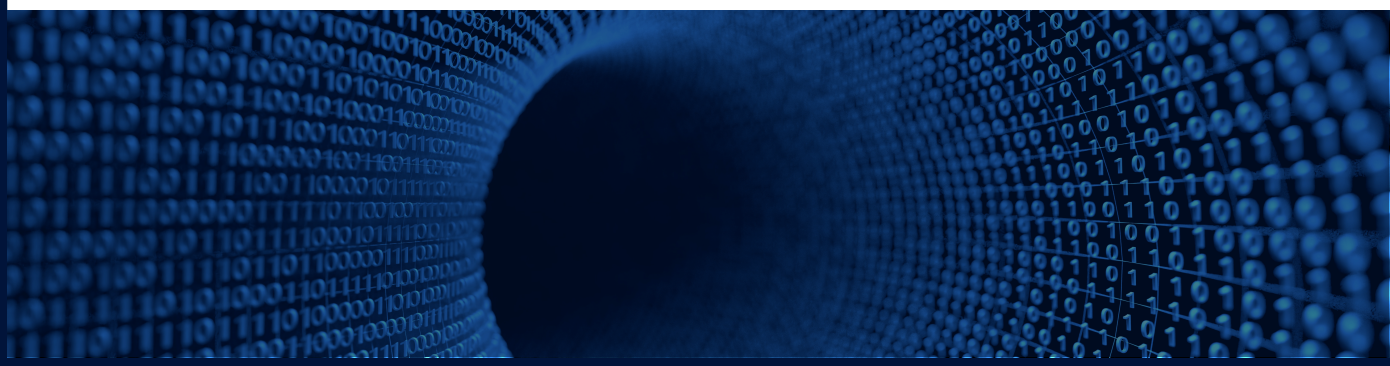
The G.3-4Cloud Utilization Services policy area mandates Encrypting CJI Data in a Cloud Environment with agency controlled keys. Certes Virtual Enforcement Points can be installed in Cloud Computing environments to protect Data in transit.

How DPRM Aligns and Solves Challenges

- **Transmission Confidentiality and Integrity:** Cryptographic protection for all CJI Data to and from Cloud services prevent unauthorized visibility, changes or access.
- **Agency Controlled Cryptographic Key Establishment and Management:** Crypto key generation, distribution, storage, access and destruction is controlled by the agency.

Benefits to Agencies

- Agencies can benefit from using Cloud Services under their control with Data protected to and from the services.



Conclusion

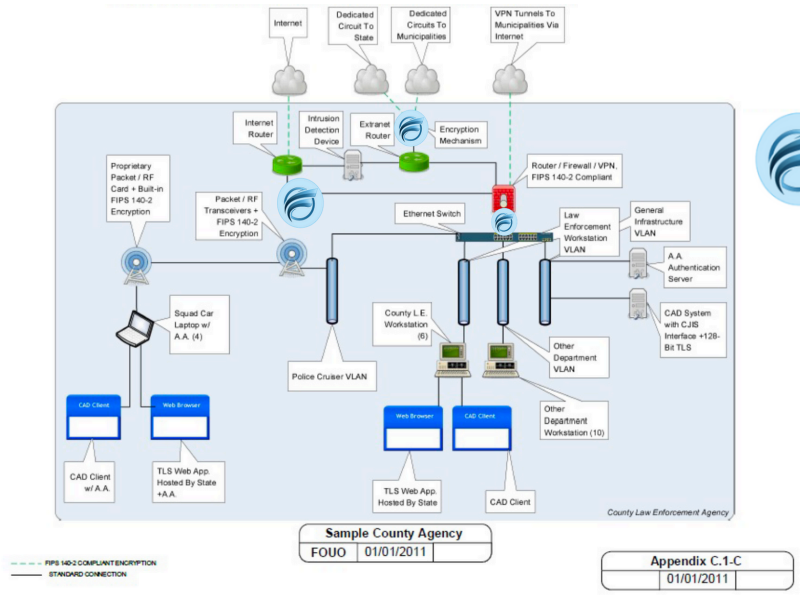
Certes DPRM aligns seamlessly with CJIS Version 6.0 policy areas, empowering agencies to deliver Quantum Safe protected CJI , while allowing agencies to meet their mandatory obligations under CJIS. By addressing controls in System and Communications Protection, Access Control, Audit and Accountability, Incident Response, and Cloud Services , DPRM delivers a data-centric, comprehensive solution.

Agencies can ensure compliance to CJIS Policy areas and benefit from:

- **Key Ownership:** Agency ownership of Centralized policy and key management to meet mandatory authentication and cryptographic standards across multiple policy areas.
- **Enhanced Data Security:** Encrypts CJI in transit, mitigating risks of interception or tampering, across trusted and untrusted networks from local to cloud.
- **Operational Efficiency:** Automates reporting and monitoring, reducing administrative overhead.
- **Architectural Flexibility:** Operates across diverse networks, supporting legacy and modern systems alike.
- **FIPS Quantum Safe Encryption :** DPRM provides quantum-safe data encryption, and quantum key distribution adhering to current NIST & FIPS standards.
- **Quick and Simple to Deploy :** As a bump in the wire the Certes Enforcement Point is simple to deploy into existing architectures without complex changes needing to be designed in.

For a customized evaluation of DPRM's fit for your agency, please contact Certes.

Conceptual Topology Diagram for a County L:aw Enforcement Agency



Certes FIPS 140-3 Enforcement Point

Contact Certes

300 Corporate Center Drive,
Suite 140 Pittsburgh, PA 15108

1 (888) 833-1142

sales@certes.ai