VMware® SDDC and EUC Product Applicability Guide for the Criminal Justice Information Services (CJIS) Security Policy version 5.5

August 2016 Version 1.0

TECHNICAL WHITE PAPER

This is the first document in the compliance reference architecture for CJIS. You can find more information on the framework and download the additional documents from the CJIS compliance resources tab on VMware Solution Exchange here.

vmware®

Table of Contents

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Revision History

DATE	REV	AUTHOR	COMMENTS	REVIEWERS
August 2016	1.0	Jason Macallister		Internal SME, Coalfire; Technical SME – VMware; Legal – VMware and Coalfire; Branding - VMware

Design Subject Matter Experts

The following people provided key input into this design.

NAME	EMAIL ADDRESS	ROLE/Comments
Jason Macallister	jason.macallister@coalfire.com	Senior Consultant – Cloud and Virtualization
Chris Krueger	chris.krueger@coalfire.com	Revision QA to Customer DRAFT Release
Anthony Dukes	adukes@vmware.com	Technology SME, VMware
Chris Davis	chrisdavis@vmware.com	Security and Compliance SME, VMware

Trademarks and Other Intellectual Property Notices

The VMware products and solutions discussed in this document are protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their companies.

Solution Area	Key Products
Software-Defined Compute	VMware ESXi™, VMware vCenter™, VMware vCenter Server™, VMware vCenter™ Server Standard™, VMware vCenter™ Single Sign-On, VMware vCenter™ Server Appliance™, VMware vCloud Suite®, VMware vSphere® Data Protection™, VMware Tools™, VMware vSphere® Distributed Resource Scheduler™, VMware vSphere® Distributed Power Management™, VMware vSphere® Enterprise Plus Edition™, VMware vSphere® Fault Tolerance, VMware vSphere® Flash Read Cache™, VMware vSphere® High Availability, VMware vSphere® Storage DRS™, VMware vSphere® Storage vMotion®, VMware vSphere® vMotion®, VMware vSphere® Web Client
Software-Defined Networking	VMware NSX®, VMware NSX® Manager™, VMware NSX® Edge™, VMware NSX® Controller™, VMware NSX® Services™, VMware NSX® Virtual Switch™, NSX Firewall, NSX Router, NSX Load Balancer, NSX Service Composer, VMware NSX® API™
Management and Automation	VMware vRealize® Suite Enterprise, VMware vRealize® Operations™, VMware vRealize® Operations Manager™, VMware vRealize® Hyperic®, VMware vRealize® Configuration Manager™, VMware vRealize® Infrastructure Navigator™, VMware vRealize® Log Insight™, VMware vRealize® Log Insight™ Content Pack for xxx, VMware vRealize® Operations Insight™, VMware vRealize® Orchestrator™, VMware vCenter™ Orchestrator Appliance™, VMware vRealize® Operations for Horizon®, VMware vRealize® Operations for Published Applications™, VMware vRealize® Operations Manager™ for Horizon®, VMware vRealize Automation™, VMware vRealize Business™, VMware vRealize® Operations Management Pack™ for xxx, VMware vSphere® Syslog Collector, VMware vSphere® Update Manager™, VMware vSphere® Update Manager Client™, VMware vSphere with Operations Management™
Disaster Recovery Automation	VMware vCenter™ Site Recovery Manager™, VMware vSphere® Replication™
End User Computing	VMware Workspace™ ONE™, VMware Horizon® Enterprise Edition, VMware Horizon® FLEX™, VMware View® Composer™, VMware View® Manager™, VMware Horizon® Client, VMware Workspace™ Suite, VMware Identity Manager™, VMware User Environment Manager™
Enterprise Mobility Management	AirWatch® by VMware, AirWatch® Connect™, AirWatch® Enterprise Mobility Management™, AirWatch® Mobile Device Management, AirWatch® Mobile Application Management, VMware AirWatch® Mobile Email Management, AirWatch® Secure Content Locker™, AirWatch® Mobile Browsing Management, AirWatch® Browse, AirWatch® Workspace™

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Executive Summary

VMware recognizes the following as critical areas that must be addressed by each criminal justice agency (CJA) and non-criminal justice agency (NCJA) that has access to and/or works with criminal justice information (CJI): security and compliance; the criticality and vulnerability of the assets needed to manage CJI impacting infrastructures; and the risks to which those assets are exposed. By standardizing an approach to compliance and expanding the approach to include partners, VMware provides its customers a proven solution that more fully addresses their compliance needs. This approach provides management, IT architects, administrators, and auditors a high degree of transparency into risks, solutions, and mitigation strategies for moving critical applications and data to the cloud in a secure and compliant manner in alignment with the objectives of the CJIS Security Policy to protect sources, transmission, storage, and generation of CJI. This is especially important when the outcomes for noncompliance are extremely critical due to the imposition of sanctions against offending entities, which may include termination of CJIS services. Other issues resulting from non-compliance may include data spillage, data compromise, loss of data integrity, and loss of trust for the agency where compromise occurs, all of which would likely negatively impact the mission of the agency.

For these reasons, VMware enlisted its audit partner, Coalfire Systems, to engage in a programmatic approach to evaluate VMware products and solutions for CJIS Security Policy requirements capabilities and document these capabilities into a set of reference architecture documents. This document presents Coalfire's evaluation of the different VMware applications available to organizations that use (or are considering using) VMware software-defined data center (SDDC) and end-user computing (EUC) environments to host or access CJI affecting critical cyber assets. Specifically, this document focuses on the SDDC and EUC solutions available. The software-defined data center is defined as a platform, which brings together best-in-class compute, storage, networking, security, and technical management, all virtualized and delivered as a service. A unified hybrid cloud lets you rapidly develop, automatically deliver, and manage all of your enterprise applications, no matter where they reside, from one unified platform. To that end, Coalfire highlights the specific CJIS Security Policy requirements that these applications address and/or support. The applications outlined in this Product Applicability Guide can be considered in evaluation of the initial sourcing of technologies to build a platform that helps CJA and NCJA adhere to CJIS Security Policy requirements.

For more information on these documents and the general approach to compliance issues, please review VMware Compliance Cyber Risk Solutions.

The controls selected for this paper are from the (Criminal Justice Information Services (CJIS) Security Policy Version 5.5, 2016). It has been reviewed and authored by our staff of cloud experts and CJIS Security Policy consultants in conjunction with VMware. The controls reviewed for scope in this whitepaper include all of the requirement priority Tier 1 and Tier 2 controls as determined by the presence of the word "shall" in the statement. Additional recommended controls were also chosen based on the relevance to the VMware technologies and solutions included in this whitepaper.

If you have any comments regarding this white paper, we welcome any feedback at vmware@coalfire.com or compliance-solutions@vmware.com.

It is Coalfire's opinion that the VMware software-defined data center (SDDC) and end-user computing (EUC) solutions may safely be used to address and/or support CJIS Security Policy version 5.5 requirements. From a high level, the VMware SDDC provides software-defined infrastructure, software-defined networking, and management and security technologies capable of supporting, adhering to, and/or addressing control objectives relevant to CJIS Security Policy Requirements to enable platform support of CJI. VMware EUC provides secure delivery capability of any application, to any device, anywhere. This is accomplished with an approach capable of meeting control requirements in support of the CJIS Security Policy. Furthermore, VMware's vast network of partners provide added value with technologies capable of being inserted seamlessly and holistically with the VMware solutions to address further requirements and enhance security.

Introduction

Most organizations begin the compliance process by mapping mandated accreditation requirements to their specific organizational needs and capabilities. Usually this difficult task can utilize significant time and resources. To streamline the process, VMware has established a single holistic approach that can be used to evaluate the VMware environment, partner solutions, and end-user tools. This Product Applicability Guide, the first in a series of white papers that make up the

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

reference architecture framework, maps CJIS Security Policy requirements to VMware's software-defined data center and end-user computing technology platforms.

Organizations can significantly reduce the complexity and cost of CJIS Security Policy compliance by replacing traditional non-integrated products with integrated solutions. As most organizations know, there is no single product or vendor that can meet all of an organization's needs. To further address this gap, VMware, together with the VMware partner ecosystem, delivers compliance-oriented integrated solutions, enabling compliance by automating the deployment, provisioning, and operation of regulated environments. VMware provides the solution reference architecture, CJIS Security Policy requirement-specific guidance, and software solutions that businesses require to achieve continuous compliance, along with breakthrough speed, efficiency, and agility for their deployments. These solutions directly address agency needs for:

- Cost and infrastructure efficiency
- Simplified management and reporting
- Infrastructure transparency
- Effective Cyber-Risk Management
- Ability to enable and maintain a secure and compliant environment

The VMware Compliance Reference Architecture framework provides a programmatic approach to map VMware and partner products to regulatory controls from an independent auditor perspective. The result is valuable guidance that incorporates best practices, design, configuration, and deployment with independent auditor oversight and validation. **Figure 1** illustrates the VMware Compliance Reference Architecture.

Figure 2 illustrates measures of capability with respect to security, confidentiality, and integrity that make up a trusted cloud implementation. The graphic illustrates the specific solution categories that can be addressed with VMware solutions and VMware's extensive partner ecosystem.

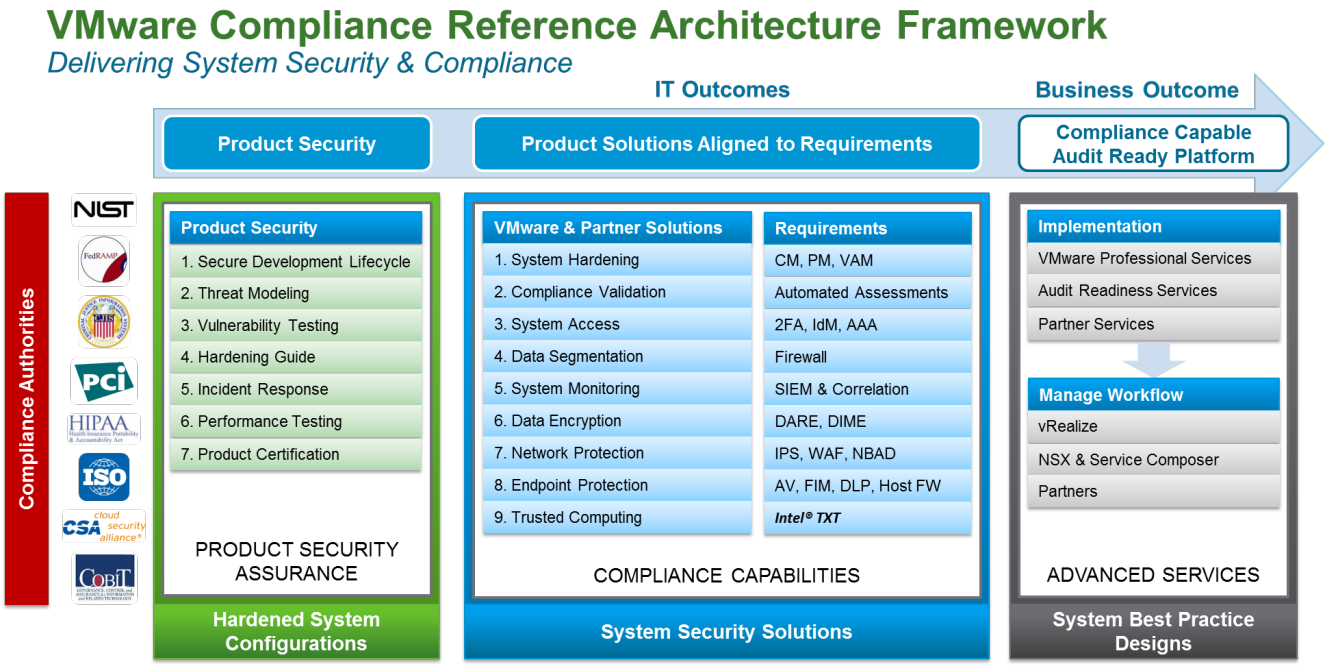

Figure 1: VMware Compliance Reference Architecture Framework

By addressing and implementing the security solutions within the framework of the regulated infrastructure, many of the technical control requirements for any particular regulation are addressed. By integrating these security solution components together in a cohesive manner, the outcome is a compliance-capable platform upon which the covered entity or business associate can overlay its business systems and data.

Figure 2 further illustrates the alignment of system security solutions with compliance frameworks and gives examples of VMware technologies and solutions that are capable of addressing the solution.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Compliance Solutions Crosswalk - Common Required Technical Security Solutions

	Common Required Technical Security Solutions	CJIS	FISMA MOD	PCI	NIST SP800-53A+	CJIS	Product Examples
System Hardening & Compliance Validation							
1	**Configuration Management**	●	●	●	SI-2, SA-10, CM-1/2/6, AC-7(2), AC-19	5.13.4 5.7.1 5.7.1.1	VMware vRealize Configuration Manager, AirWatch Enterprise Mobility Management
2	**Patch Management**	●	●	●	CM-2, SI-2	5.10.4.1	VMware vRealize Configuration Manager, VMware vSphere Update Manager
3	**Vulnerability Assessment and Management**	●	●	●	RA-5, RA-3, SA-14	5.1.2	vRealize Configuration Manager
4	**Penetration Testing**	●	●	●	CA-2	5.11.1.2 5.11.3	
System Access							
5	**Two Factor Authentication**	●	●	●	IA-2 (1), IA-4	5.6.1 5.6.2, 5.6.2.2 5.13.7, 5.13.7.1,2	VMware Identity Manager[1]
6	**Identity Management**	●	●	●	IA-2, IA-4	5.6.1 5.6.2.1.2 5.6.3 5.13.7, 5.13.7.1,2	VMware Identity Manager
7	**Access Management**	●	●	●	IA-5, AC-3	5.5 ALL 5.6.2.1 5.6.3	VMware Identity Manager
Data Segmentation							
8	**Network & Host Firewall**	●	●	●	SC-7	5.10.1 5.10.1.1	VMware NSX Logical Firewall
System Monitoring							
9	**Security Information Event Monitoring**	●	●	●	SI-4, AU-2/3/6/10/12	5.4.3 5.4.5 5.10.1.3	
10	**Database Monitoring**	○	▲	▲	SI-4		
Data Encryption & Protection							
11	**Data at Rest Encryption**	●	●	●	SC-12/13/28, IA-7	5.8.1 5.10.1.2 5.10.1.1.2 5.13.2	
12	**Data in Motion Encryption**	●	●	●	SC-9/12/13, IA-7	5.10.1.2 5.10.2	
13	**System Backup & Restore**	○	●	●	CP-9		VMware Data Protection
Network Protection							
14	**Intrusion Prevention System**	●	●	●	SI-3, SI-4	5.10.1.3 5.10.3.2	VMware NSX Platform Extensibility, vShield Endpoint
15	**Web Application Firewall**	▲	▲	▲	SI-3, SI-4, SC-7	5.10.3.2	VMware NSX Platform Extensibility, vShield Endpoint
Endpoint Protection							
16	**Antivirus & Malware Prevention**	●	●	●	SI-3	5.10.4.2 5.10.4.3	VMware NSX Platform Extensibility, vShield Endpoint
17	**File Integrity Monitoring**	○	●	●	SI-7		vRealize Configuration Manager
18	**Data Leakage Protection**	▲	▲	▲	AC-4	5.10.1	
Trusted Computing							
19	**Trusted Execution**	○	▲	▲			

Specifically discussed indicates that the technical security solution was specifically mentioned in a requirement ●

Not specifically discussed indicates that there was no specific mention of the solution; however, the solution may be inferred from the requirement ○

Possibly required indicates that the solution was specifically discussed, but is not considered a requirement. (Risk Reduction or Mitigation) ▲

Comments or suggestions: chrisdavis@vmware.com

Figure 2: Compliance Solutions Crosswalk

[1] Supports multi-factor authentication, but does not supply secondary factors for authentication.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Scope and Approach

Due to the CJIS Security Policy requirements' broad coverage of subjects relative to the protection of CJI, it is necessary to identify the subjects that are relevant to the combined subject matter of this Product Applicability Guide. The primary subjects include the CJIS Security Policy requirement topics and the VMware presented platform and solutions.

CJIS Security Policy Scope

The compliance framework scope of this Product Applicability Guide is the Criminal Justice Information Services (CJIS) Security Policy Version 5.5. To gain greater understanding of the requirements specified in the security policy, Coalfire refers to NIST Special Publication 800-53 Revision 4. The CJIS Security Policy requirements can be tied directly to NIST security guidelines. The NIST publications are useful for assisting CJAs and NCJAs with selecting the type of implementation that best suits their unique circumstances. For each of the CJIS Security Policy requirements, Coalfire identified controls from NIST Special Publication 800-53 Revision 4 that are in alignment. Using this foundation simplifies the process for determining the capability of VMware solutions to address controls necessary to meet the requirement. For VMware technologies, the relevant CJIS Security Policy requirements include:

Policy Area 4: Auditing and Accountability

Policy Area 5: Access Control

Policy Area 6: Identification and Authentication

Policy Area 7: Configuration Management

Policy Area 10: System and Communications Protection and Information Integrity

Policy Area 13: Mobile Devices

Reference architecture framework documents have been published by VMware for other compliance frameworks. If you are interested in learning more about VMware's approach to compliance with respect to additional regulatory frameworks, please review "VMware's Compliance & Cyber Risk Solutions" on the VMware Solution Exchange.

VMware Solution Scope

VMware provided a listing of VMware technologies to be included in scope for evaluation with regard to level of capability to support the CJIS Security Policy requirements. Included in scope for this assessment are VMware's software-defined data center (SDDC) stack and the VMware end-user computing (EUC) stack. The SDDC stack is the foundation for enterprise virtualization and cloud platforms. The EUC stack utilizes the best of software-defined data center and enables improved management and control over the delivery of the end-user experience. These technologies when taken together form the basis for a cohesive infrastructure platform solution. Both the SDDC and the EUC platforms are capable of being holistically and seamlessly extended with respect to private, public, and hybrid cloud models. The use of software-defined networking with NSX, as well as with Virtual SAN, improves this capability with respect to compliance by allowing the network and security to be stretched across an agency's environment. At a minimum, this capability can support disaster recovery initiatives and efficient regional distributions of workloads and workforce. The following is a listing of in-scope VMware technologies with a brief summary of each technology's purpose. More information about the technologies listed can be found at **https://www.vmware.com**.

VMware vCloud Suite - Enterprise

The following is a listing of the individual products and features available with the VMware vCloud Suite – Enterprise. The VMware vCloud Suite is the base suite of products that make up the VMware software-defined data center.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

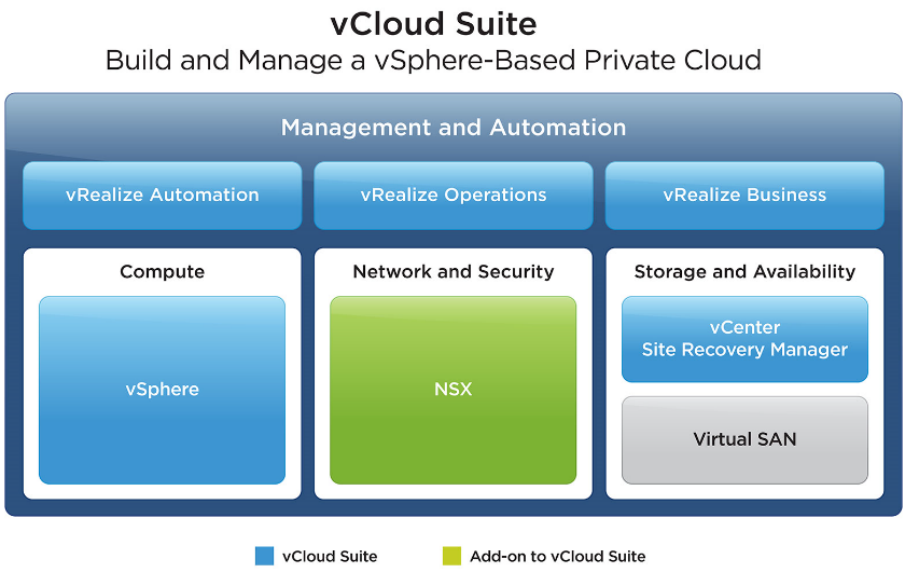

Figure 3: vCloud Suite[2]

VMware vSphere

VMware vSphere is the leading server virtualization platform with consistent management for virtual data centers. It is the core foundational building block of highly virtualized environments and cloud infrastructure, also referred to as the software-defined data center. The features listed below are relevant to CJIS Security Policy requirements. They provide capabilities that are pertinent to the Security Rule, including a secure platform architecture, management ease with integration for single pane of glass management, high availability, antivirus and anti-malware support, and configuration awareness and consistency.

- VMware ESXi
- VMware vSphere Storage APIs
- VMware vSphere High Availability
- VMware vSphere Fault Tolerance
- VMware vSphere Data Protection
- VMware vSphere Reliable Memory
- VMware vSphere Distributed Switch
- VMware vSphere Auto Deploy
- VMware vSphere Host Profiles

VMware vCenter Server

VMware vCenter Server provides a centralized and extensible platform for management of vSphere virtual infrastructure. IT administrators can help ensure security and availability, simplify day-to-day tasks, and reduce the complexity of managing a virtual infrastructure.

VMware Site Recovery Manager

[2] Virtual SAN is greyed out in this illustration depicting the vCloud Suite because Virtual SAN is licensed separately from the vCloud Suite. The Virtual SAN remains a useful component of the software-defined data center.

VMware Site Recovery Manager is a leading solution to enable application availability and mobility across sites in private cloud environments. It is the basis for fast and reliable IT disaster recovery. VMware Site Recovery Manager is an available extension to VMware vCenter, providing centralized management capability for disaster recovery, site migration, and non-disruptive testing capabilities to VMware customers. Site Recovery Manager is fully integrated with VMware vCenter Server and VMware vSphere Web Client. It works in conjunction with various replication solutions including VMware vSphere Replication to automate the process of migrating, recovering, testing, re-protecting, and failing back virtual machine workloads.

VMware vSphere Replication

VMware vSphere Replication is a hypervisor-based, asynchronous replication solution for vSphere virtual machines. It is fully integrated with VMware vCenter Server and the vSphere Web Client. VMware vSphere Replication delivers flexible, reliable, and cost-efficient replication to enable data protection and disaster recovery for all virtual machines in the infrastructure. Combined with VMware Site Recovery Manager, VMware vSphere Replication is capable of addressing general operational best practices for ensuring the availability of CJI with disaster recovery and business continuity in the event of long-term outages.

VMware vRealize Automation – Enterprise

VMware vRealize Automation improves agility by automating IT service delivery (applications, infrastructure, desktops, and any IT service to rapidly respond to business needs). It allows for improved control of the IT solutions by enabling personalized, business-relevant policies to enforce application deployment standards, setting resource quotas and enabling multiple service levels. VMware vRealize Automation allows for improvements in efficiency by improving IT delivery while lowering cost. With automation, IT is able to offer the business self-service deployment capabilities without sacrificing control, and thus helps to ensure that necessary security controls can be automatically applied to all newly deployed solutions. It further allows control for the covered entity beyond the private cloud with extensibility to multi-vendor, multi-cloud designs.

vRealize Suite – Enterprise

Part of the vRealize vCloud Suite, vRealize Operations provides intelligent operations management capability for the covered entity's and business associate's physical, virtual, and cloud infrastructure. It correlates data from applications to storage in a unified, easy-to-use management tool that provides control over performance, capacity, and configuration, with predictive analytics to drive proactive action and policy-based automation. A challenge that faces any organization desiring to determine risk is the lack of knowledge and insight into the infrastructure. The VMware vRealize Enterprise Suite includes:

- VMware vRealize Operations Manager
- VMware vRealize Hyperic
- VMware vRealize Configuration Manager
- VMware vRealize Infrastructure Navigator
- VMware vRealize Log Insight
- VMware vRealize Operations Insight
- VMware vRealize Orchestrator

VMware NSX

VMware NSX is the network virtualization platform for the software-defined data center. By bringing the operations model of a virtual machine to your data center network, you can transform the economics of network and security operations. NSX lets you treat your physical network as a pool of transport capacity, with network and security services attached to virtual machines with a policy-driven approach.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

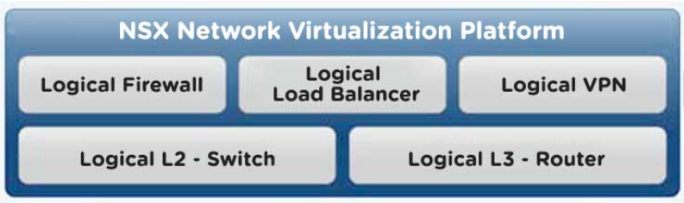

Figure 4: VMware NSX Platform for Advanced Networking and Security Services

Networking for the software-defined data center

VMware vSphere provides two software defined network platforms that form the basis of fault-tolerant switching for the SDDC: Standard vSwitch and Distributed vSwitch with hypervisor basic and fault-tolerant extended network services to facilitate a “network fabric.” The addition of VMware NSX brings routing, access-list based firewall features and VPN services to the Distributed vSwitch.

Agility and Streamlined Operations

As with the economies of scale created by initially using VMware vSphere technologies to promote agility and velocity for the server stack, VMware NSX does the same for networking and transit security. Virtual networking is enhanced with routing and firewall components that are as quick to deploy and easy to manage as VMs under vCenter.

Security and Micro-segmentation

NSX brings a complete set of firewall-based components to the Distributed vSwitch that extends the vital, regulatory compliance-ready tools to the vCloud environment. Through basic network segmentation, using the routing component of NSX, Layer 3 routing services may be introduced to create fundamental scope separation. NSX also includes VPN components to deliver data-in-motion encryption between elements of the network.

The powerful, per VM, firewall services supplied by NSX micro-segmentation can further enforce protected data scope with rich, access-list based rules, for fine-grained Layer 4-7 rules. Logging and management accompany the firewall services to complete the package.

Platform for advanced networking and security services

NSX is deployed at the hypervisor layer in the virtualized infrastructure, where it augments the ESXi virtualization engine by extending the Distributed vSwitch functionality with these platform services:

- Logical Switching
- NSX Gateway
- Logical Routing
- Logical Firewall
- Logical Load Balancer
- Logical VPN
- NSX API

NSX is a fundamental network enhancement from VMware. NSX is an important tool for achieving compliance with cloud security requirements and recommendations of the CJIS Security Policy.

VMware Validated Design for SDDC

The VMware Validated Design for SDDC provides a prescriptive and extensively-tested blueprint that can be followed to deploy and operate a private cloud using VMware’s SDDC technology. VMware’s SDDC technology is comprised of the vCloud Suite and NSX products listed in the previous sections. This comprehensive private cloud solution has been developed by VMware experts and rigorously tested and validated to help ensure both a successful deployment and efficient on-going operations. In addition, on-going interoperability testing ensures that the validated design remains valid as subsequent versions of the component products are released.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

A private cloud based on the VMware Validated Design provides the following benefits:

- **Faster Time to Value**: VMware Validated Design simplifies the design and implementation of the private cloud and streamlines “day-2” operations. Faster deployment of your data center and guidance for how to operate it allows customers to focus on solving real business problems faster.
- **Eliminates Risk and Instills Confidence:** VMware Validated Design is rigorously tested and continuously validated to help ensure interoperability and compatibility of all components. This instills confidence by eliminating risks associated with implementing a unique private cloud architecture.
- **Drives IT Agility:** VMware Validated Design provides an agile platform that is scalable and able to support both legacy and modern application types in support of a broad range of use-cases, enabling IT to become a competitive edge in today’s modern mobile cloud era.

VMware Validated Design includes the following as part of a set of supporting documentation and points of reference:

- Reference Architectures
- Detailed Design Guides
- Pre-Deployment Checklists
- Configuration Workbooks and Validation Workbooks
- Implementation Guides
- Operations Guides

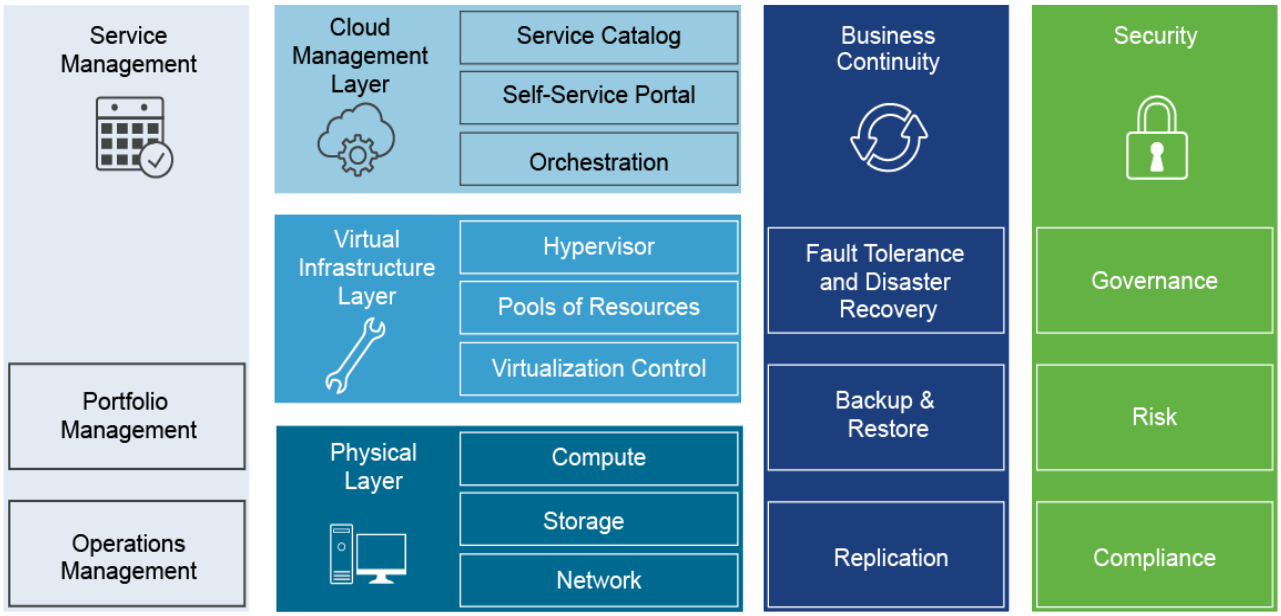

Figure 5: VMware Validated Design for SDDC

VMware Workspace ONE

VMware End-User computing products allow IT organizations to pro-actively deliver consistent and intuitive services to their customers. Driven by the demands of users for immediate access to applications and data from any device at any time, and from any location, services can be orchestrated to meet these demands without sacrificing compliance requirements. As a result, the user is able to work more efficiently in a manner that best suits his or her needs, while IT is able to manage that experience for confidentiality, integrity, and availability. VMware Workspace ONE combines end-user computing technologies such as VMware Horizon and AirWatch to unify the end-user experience for secure access to applications and

content from laptops, desktops, zero or thin-clients, and mobile devices and tablets. This allows IT to deliver the digital workspace as a service, much like catalogs of infrastructure services can be delivered with the software-defined data center.

Figure 6: VMware Workspace ONE

VMware Workspace ONE includes a unified app store for delivering a catalog of agency approved applications. This unified app store provides controlled access to a variety of types of applications including mobile apps, client-server apps, web apps, web sites and more. The apps are accessible through a catalog and is the central hub for end-user application delivery.

Workspace ONE also includes a single-sign on (SSO) capability, which is capable of integrating with basic Active Directory Federations SSO, SSO with Custom Policies, Device Trust Authentication, Touch ID on iOS, and device specific authentication provider integration.

VMware Horizon 7 Enterprise Edition

- vSphere for Desktop
- vCenter Server
- Horizon with View
- Horizon for Linux
- vRealize Orchestrator + Desktop Plugin
- vRealize Automation for Horizon
- vRealize Operations for Horizon
- User Environment Manager
- App Volumes
- NSX for vSphere Horizon Edition
- Identity Manager (vIDM)
    - VMware Identity Manager is an Identity as a Service (IDaaS) offering, providing application provisioning, self-service catalog, conditional access controls, and Single Sign-On (SSO) for SaaS, web, cloud, and

native mobile applications. Identity Manager delivers on consumer-grade expectations like one-touch access to apps. This delivery of applications can be optimized with AirWatch Conditional Access and backed by a self-service catalog with enterprise-class management and security.

VMware AirWatch Enterprise Mobility Manager

VMware AirWatch is a scalable enterprise mobility management platform that integrates with existing enterprise systems and allows you to manage almost all devices, regardless of type, platform, or ownership, from one central console. Included with AirWatch Enterprise Mobility Manager are the tools necessary to allow end users, regardless of their device, to securely interact with CJIS compliant workloads. The ability for administrators to manage and control the device helps to ensure the integrity of the device and security of the data that these devices are accessing.

- VMware AirWatch Container Management – provides complete separation of corporate and personal data on mobile devices, securing corporate resources and maintaining employee privacy. Enables standardization of enterprise security and data loss prevention strategies across mobile devices. Corporate containers keep corporate applications and data separate from personal applications and data on mobile devices.
- VMware AirWatch Mobile Device Management – this is the foundation of a comprehensive Enterprise Mobility Management (EMM) platform. AirWatch MDM provides a simplified, efficient way to view and manage a diverse fleet of devices from a central admin console. AirWatch MDM enables enrollment of mobile devices in your enterprise environment quickly, configure and update device settings over-the-air, and secure mobile devices without hindering the user experience.
- VMware AirWatch Mobile Applications Management – truly enables the concept of any application to any device. Provides the framework to help the agency support the complete app lifecycle. Beyond static app distribution, IT is able to source or develop apps, apply security policies, and deploy an app catalog, as well as analyze app metrics.
- VMware AirWatch Content Locker – enables secure mobile access to content anytime, anywhere. Protects your sensitive content in a corporate container and provides users with a central application to securely access, store, update, and distribute the latest documents from their mobile devices.
- VMware AirWatch Mobile Email Management (VMware Boxer) – a mobile email solution that helps keep corporate data secure and compliant. It delivers fast email sync and an intuitive user experience with secure mobile access to corporate-owned and BYO devices while respecting user privacy.
- VMware AirWatch Mobile Browsing Management – enables secure web browsing and provides organizations with the ability to configure customized settings to meet their unique business and end-user needs. Allows administrators to design and enforce secure browsing policies from a central admin console. AirWatch Browser is pre-configured to use app tunneling through the AirWatch Mobile Access Gateway to proxy access to internal resources in the agency's LAN. This is a secure point of entry for all compliant devices to access enterprise services.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

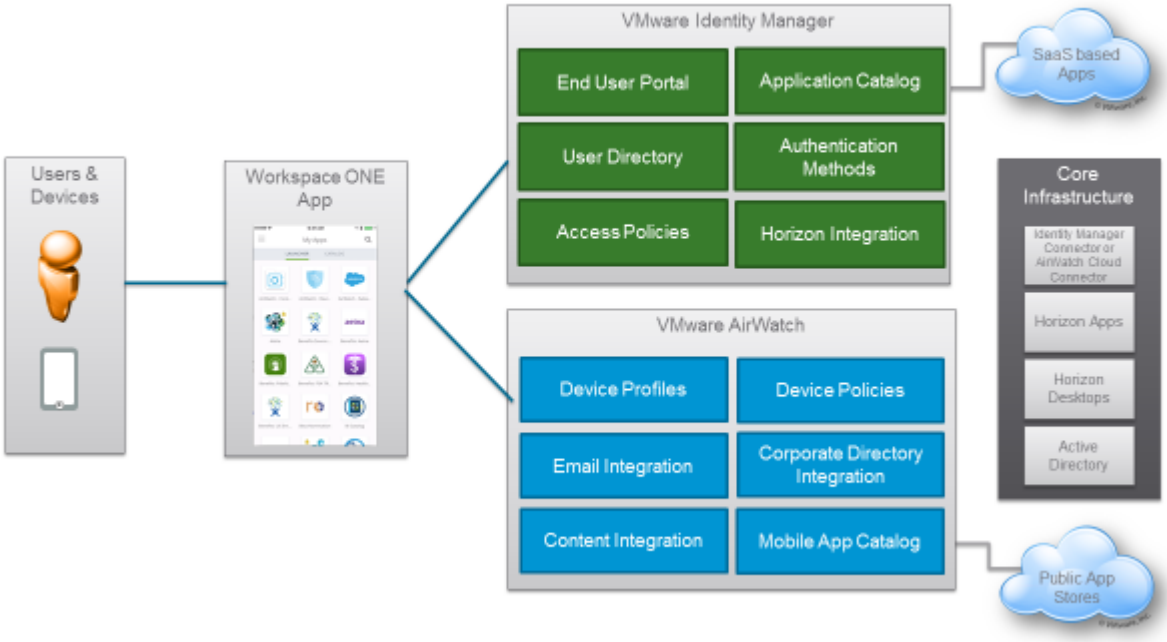

Figure 7: VMware Workspace ONE

Overall Design

The overall design of the VMware SDDC and EUC solutions has been considered for multiple purposes. Foremost, the design must support the function of the business. Secondly, the design must minimally meet security requirements for the impacted security framework. When deciding technologies to include in the design, these factors were considered.

EUC and mobility components were chosen for their ability to securely support end-user access to CJI data and application in a secure and controlled manner. This further accentuated the capabilities for secure access necessary to support agents in the field.

Software-defined data center components were chosen for the ability to achieve scalability and agility for the infrastructure necessary to support access to CJI.

Software-defined networking, a component of the SDDC, was included due to the ability to provide secure networking capability to both the infrastructure and the end-user compute environments.

The VMware Validated Design for SDDC has been utilized to take advantage of a rigorously tested and consistently reproducible architecture that provides additional operational benefits for customers.

The overall design is cohesive, comprehensive, and capable of being further enhanced by VMware partner solutions.

Coalfire's Approach

The CJIS Security Policy Solutions Applicability Matrix, found in the sections following, map specific requirements of the CJIS Security Policy to VMware's solutions suites, their component technologies, and partner technologies. All Tier 1 and Tier 2 requirements were reviewable relative to applicability. The requirements are identified by the use of "shall" in the policy statement; as an example, "virtual machines that are Internet facing **shall** be physically separate from virtual machines that process CJI internally or be separated by a virtual firewall." Additional consideration was given for policy recommendations inasmuch as there was alignment potential for VMware solutions. The recommendations are identified with the use of "should"; for instance, "the firewall in a virtual environment **should** be configured to ensure only allowed protocols will transact."

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Understanding the CJIS Security Policy requirements and how they align with NIST 800-53 Revision 4 controls helps to align control capability of a given technology with the policy requirement. The inferences, drawn upon by this common understanding, support cases where, for each policy requirement, VMware technology: (i) is fully capable of supporting control enablement; (ii) is partially capable of supporting control enablement; (iii) provides support for administrative control enablement; (iv) aligns with control requirements; or (v) does not support control enablement.

For the purpose of this white paper, when the VMware technology is designed to specifically address a control capability (e.g., VMware NSX, NSX distributed firewall, micro-segmentation, AirWatch Mobile Device Management) and that control capability aligns with a CJIS Security Policy requirement, it is determined to be fully capable of supporting said requirement.

Likewise, VMware technology that is determined to partially support control enablement will likely require additional partner technologies to fully support the enablement of controls to support the policy requirement. VMware NSX with service insertion from partner solutions to provide intrusion detection/protection, application firewall, or antivirus is a good example of such case.

There may be cases where an administrative action or process is the primary means for providing control or addressing a policy requirement. At the same time, a technological solution may be available to inform or aid the administrative process. For example, policy requirement 5.4.3 states that audit review/analysis shall be conducted at a minimum once a week. This requires the responsible designated personnel to perform an administrative action. Technology may inform this process by producing weekly-generated audit reports for the personnel to review; however, the designated personnel must perform analysis of the reports to meet the control requirement. This is an example where the VMware technology is determined to support an administrative control enablement.

When the VMware technology is capable of meeting control objectives on its own behalf for common controls that should be applicable to all systems with access or adjacency to CJI, the technology is considered to be in alignment with the policy requirements. An example of these common controls include, but are not limited to, role-based authentication for local administrative consoles, identity and authentication requirements for local system or application accounts, and audit log generation. An example of those systems that may be adjacent to CJI where access is not directly available, but security is still paramount, includes hardware hosts, software based host systems, management systems, and monitoring systems.

Finally, where a control can only be addressed by an administrative, non-technical process or control, the technology in this white paper does not support the control requirement. An example is information exchange agreements, which are only capable of being addressed by the agency and/or external parties, which VMware nor partner technology can address. For this guide, the assessor characterizes the policy as supported by “Other Support”.

For all of the above cases, additional considerations may be necessary for increasing the effectiveness of a control to address a security policy. These may include, for example, technical training, proper implementation of the technology by the agency, ongoing support and maintenance of the technology, and any additional administrative or operational procedures or processes that may be required.

Coalfire and VMware acknowledge that the CJIS Security Policy requirements are a minimum set of requirements necessary to meet a compliance objective. It is incumbent upon any CJA, NCJA, or other entity to assess risk relative to its own organization and determine additional policies, procedures, and necessary controls to feasibly enhance the security of the organization, business, and data being protected. As technology advances and a greater awareness of security risks and vulnerabilities become evident, the necessity and capability to implement greater controls becomes more practicable.

In general, **Figure 8**, which illustrates VMware’s complete approach to compliance, represents a regulation-agnostic approach to compliance, which we feel is an excellent overview of the relationship of the authoritative source through audit business process and potential compliance outcome:

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

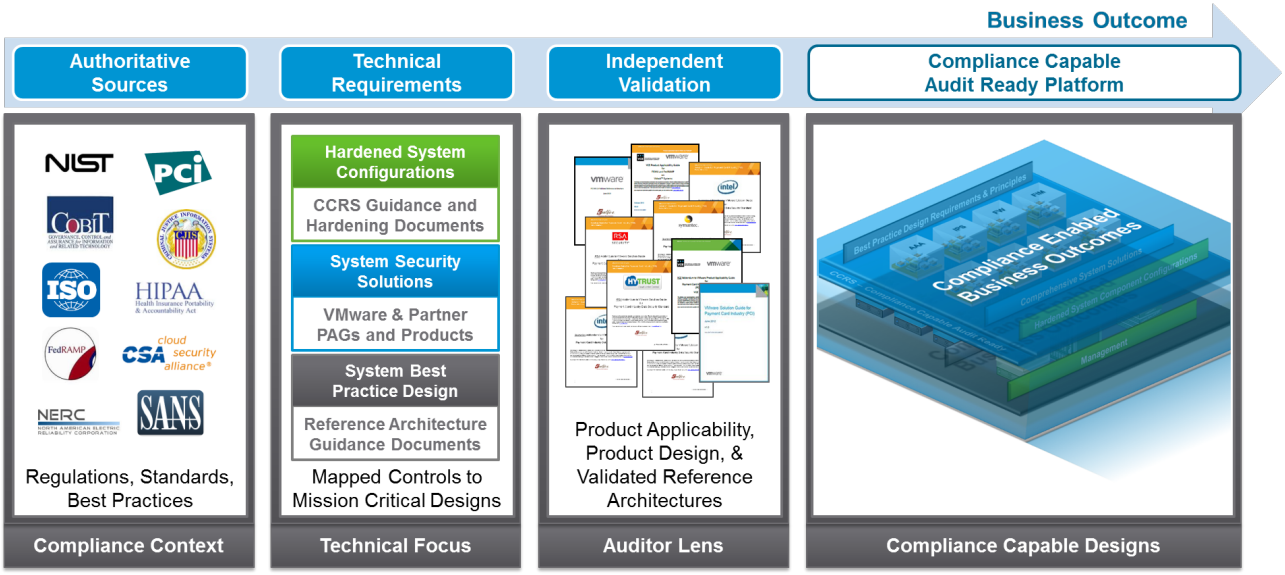

Figure 8: VMware's Compliance Reference Architecture Framework

This compliance approach applied to the software-defined data center and end-user computing stack of VMware technologies are integrated to formulate a total solution for criminal justice agencies and non-criminal justice agencies looking to utilize cloud and virtualization as the foundation for their infrastructure. The comprehensive layering of these technologies is represented in **Figure 9**.

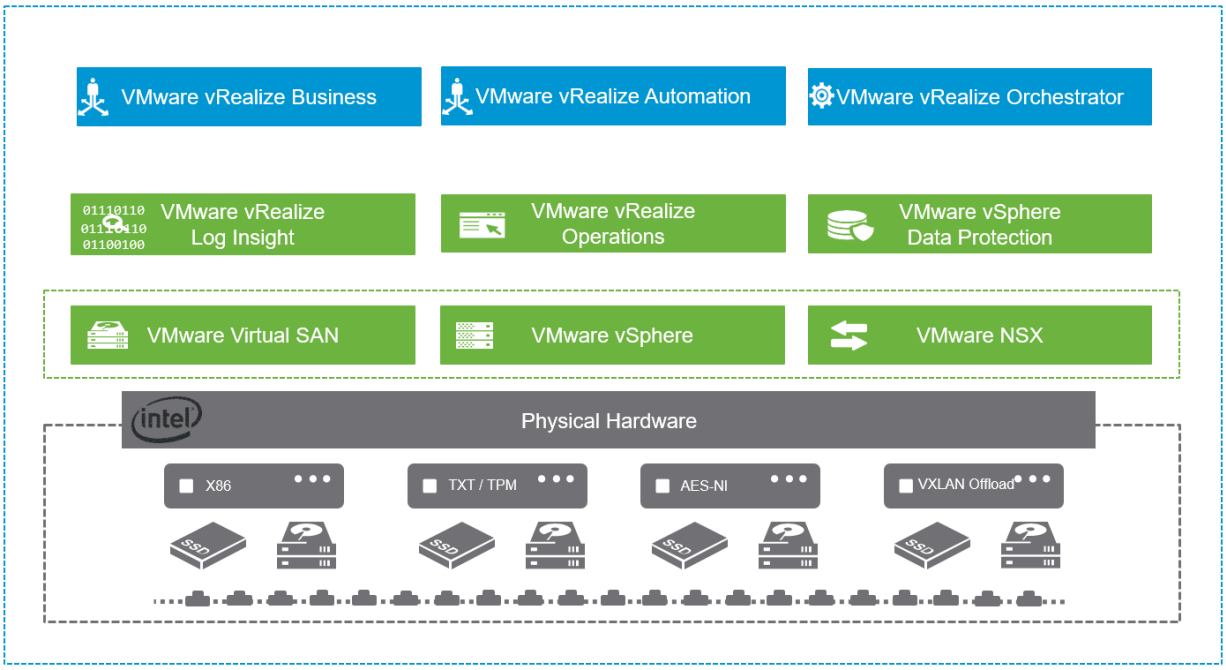

Figure 9: VMware SDDC Product Stack Layering

VMware and CJIS Security Policy Requirements (Overview)

VMware has created a CJIS Security Policy requirement matrix to assist CJAs and NCJAs with understanding how VMware technologies align with and support the CJIS Security Policy. This includes both Tier 1 and Tier 2 priority requirements, as well as recommended policies that align with VMware solutions. The requirement matrix presents Coalfire's assessment of the degree of compliance attainability that VMware platform and platform management technologies combined with partner technologies can provide. The remaining requirements and recommendations are addressable by CJA, NCJA, FBI, or other relevant entities tools, policies, procedures, standards, practices, and training. While every cloud is unique, VMware believes that a majority of requirements can be addressed by VMware and Partner solutions.

CJIS Security Policy		Products
Policy Area 4	Audit and Accountability	All products with audit logging capability align with audit and accountability requirements with respect to log generation and the content and events to be captured. VMware vRealize Log Insight and Partner Solutions may enhance support for audit and accountability requirements.
Policy Area 5	Access Control	All products with local system or application access capabilities align with access control policies.
Policy Area 6	Identification and Authentication	All products with local system or application access capabilities align with identification and authentication policies. In many cases, additional technologies will be required, such as with AA, to fully institute controls in keeping with the policy requirements.
Policy Area 7	Configuration Management	VMware vRealize Configuration Manager
Policy Area 10	System and Communication Protection and Integrity	VMware NSX, VMware ESXi, VMware vCenter, VMware vSphere Data Protection, VMware vRealize Operations, VMware vRealize Automation, VMware vRealize Orchestrator, VMware Workspace ONE, VMware Horizon Enterprise, VMware Horizon Flex, VMware Mirage
Policy Area 13	Mobile Devices	VMware NSX for vSphere Horizon Edition, VMware Horizon Enterprise, VMware Horizon Flex, VMware Mirage, VMware User Environment Manager, vRealize Operations for Horizon and vRealize Operations for Published Apps, VMware Identity Manager, AirWatch Enterprise Mobility Manager, AirWatch Mobile Device Manager, AirWatch Mobile Email Management, AirWatch Container Management, AirWatch Mobile Application Management, AirWatch Mobile Content Management, AirWatch Mobile Browsing Management

Table 1: VMware Solutions Applicability to CJIS Security Policy – Policy Areas

For a high-level view, Table 1 matches up VMware technology capabilities to fully or partially support or address requirements found in the CJIS Security Policy.Table 2 breaks out the CJIS Security Policy requirements by topic. The table summarizes the CJIS Security Policy requirements that are applicable to VMware technologies. The definition of the assertion of applicability to the topics is found in the approach section above. These assertions are:

Fully Supports – VMware technology designed to address control relative to policy requirement.

Partially Supports – VMware technology along with partner solution addresses control relative to policy requirement.

Administrative Support – VMware technology may be capable of informing administrative action or control with regard to policy requirement.

Aligns – VMware technology can meet the control objective for itself and/or does not hinder or subvert the policy requirement.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Other Support – Due to the nature of policy requirement statements, VMware and partner technologies do not specifically address these requirements. Only administrative procedures or actions of non-VMware or partner solution can address these policy requirements.

CSP v5.5 Area	Requirement Topic	Applicability to VMware Technologies
5.1	**Policy Area 1: Information Exchange Agreements**	Other Support
5.2	**Policy Area 2: Security Awareness Training**	Other Support
5.3	**Policy Area 3: Incident Response**	Other Support
5.4	**Policy Area 4: Auditing and Accountability**	
5.4.1	Auditable Events and Content (Information Systems)	Administrative Support
5.4.1.1	Events	Aligns
5.4.1.1.1	Content	Aligns
5.4.2	Response to Audit Processing Failures	Partially Supports
5.4.3	Audit Monitoring, Analysis, and Reporting	Partially Supports
5.4.4	Time Stamps	Aligns
5.4.5	Protection of Audit Information	Partially Supports
5.4.6	Audit Record Retention	Partially Supports
5.4.7	Logging NCIC and III Transactions	Other Support
5.5	**Policy Area 5: Access Control**	
5.5.1	Account Management	Aligns
5.5.2	Access Enforcement	Aligns
5.5.2.1	Least Privilege	Administrative Support
5.5.2.2	System Access Control	Aligns
5.5.2.3	Access Control Criteria	Aligns
5.5.2.4	Access Control Mechanisms	Aligns
5.5.3	Unsuccessful Login Attempts	Aligns
5.5.4	System Use Notification	Aligns
5.5.5	Session Lock	Aligns
5.5.6	Remote Access	Administrative Support
5.5.6.1	Personally Owned Information Systems	Administrative Support
5.5.6.2	Publicly Accessible Computers	Administrative Support
5.6	**Policy Area 6: Identification and Authentication**	
5.6.1	Identification Policy and Procedures	Other Support
5.6.1.1	Use of Originating Agency Identifiers in Transactions and Information Exchanges	Other Support
5.6.2	Authentication Policy and Procedures	Administrative Support
5.6.2.1	Standard Authenticators	Aligns

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

CSP v5.5 Area	Requirement Topic	Applicability to VMware Technologies
5.6.2.1.1	Password	Aligns
5.6.2.1.2	Personal Identification Number (PIN)	Aligns
5.6.2.2	Advanced Authentication	Partially Supports
5.6.2.2.1	Advanced Authentication Policy and Rationale	Partially Supports
5.6.2.2.2	Advanced Authentication Decision Tree	Partially Supports
5.6.3	Identifier and Authenticator Management	Other Support
5.6.3.1	Identifier Management	Other Support
5.6.3.2	Authenticator Management	Partially Supports
5.6.4	Assertions	Other Support
5.7	**Policy Area 7: Configuration Management**	
5.7.1.1	Least Functionality	Administrative Support
5.8	**Policy Area 8: Media Protection**	Other Support
5.9	**Policy Area 9: Physical Protection**	Other Support
5.10	**Policy Area 10: System and Communications Protection and Information Integrity**	
5.10.1	Information Flow Enforcement	Fully Supports
5.10.1.1	Boundary Protection	Fully Supports
5.10.1.2	Encryption	Partially Supports
5.10.1.3	Intrusion Detection Tools and Techniques	Partially Supports
5.10.1.4	Voice over Internet Protocol	Other Support
5.10.1.5	Cloud Computing	Other Support[3]
5.10.2	Facsimile Transmission of CJI	Other Support
5.10.3	Partitioning and Virtualization	Fully Supports
5.10.3.1	Partitioning	Fully Supports
5.10.3.2	Virtualization	Fully Supports
5.10.4	System and Information Integrity Policy and Procedures	
5.10.4.1	Patch Management	Fully Supports
5.10.4.2	Malicious Code Protection	Partially Supports
5.10.4.3	Spam and Spyware Protection	Partially Supports
5.10.4.4	Security Alerts and Advisories	Other Support
5.10.4.5	Information Input Restrictions	Other Support
5.11	**Policy Area 11: Formal Audits**	Other Support

[3] This control is pertinent to agreements with cloud service providers, whereby the cloud service provider shall not use any metadata generated from CJI.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

CSP v5.5 Area	Requirement Topic	Applicability to VMware Technologies
5.12	**Policy Area 12: Personnel Security**	Other Support
5.13	**Policy Area 13: Mobile Devices**	
5.13.1	Wireless Communications Technologies	Other Support
5.13.1.1	802.11 Wireless Protocols	Other Support
5.13.1.2	Cellular Devices	Other Support[4]
5.13.1.2.1	Cellular Service Abroad	Administrative Support
5.13.1.2.2	Voice Transmissions Over Cellular Devices	Other Support
5.13.1.3	Bluetooth	Fully Supports
5.13.1.4	Mobile Hotspots	Fully Supports
5.13.2	Mobile Device Management (MDM)	Fully Supports
5.13.3	Wireless Device Risk Management	Fully Supports
5.13.4	System Integrity	Fully Supports
5.13.4.1	Patching/Updates	Fully Supports
5.13.4.2	Malicious Code Protection	Fully Supports
5.13.4.3	Personal Firewall	Fully Supports
5.13.5	Incident Response	Administrative Support
5.13.6	Access Control	Administrative Support
5.13.7	Identification and Authentication	Administrative Support
5.13.7.1	Local Device Authentication	Fully Supports
5.13.7.2	Advanced Authentication	Partially Supports
5.13.7.2.1	Compensating Controls	Administrative Support
5.13.7.3	Device Certificates	Partially Supports

Table 2: CJIS Security Policy and VMware Applicability Mapping

There may be multiple policy statements represented in each requirement found in Table 2, the assessor assigned applicability assertion for the table above, not on the ability to address all policy statements in a given topic, but on the primary objective of the topic and relationship of the technologies assessed to address. Greater detail is found in the following sections.

Figure 10 diagrams the percent of coverage for CJIS Security Policy requirements that are addressable by VMware and VMware Partner technologies. VMware and partner capabilities are primarily aligned to technical requirements. The remaining gaps in capabilities, represented in blue in this diagram, may be filled by the CJA or NCJA through agency policies, processes, training, applications, and tools. These means include, but are not limited to, information exchange agreements, policies, documented procedures, training, infrastructure diagrams and documentation, management structure, control processes, physical security measures, personnel hiring practices, management procedures, and other CJA or NCJA defined control techniques.

[4] This is only informational about the threats to Cellular Devices, but does not contain any requirement statements.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

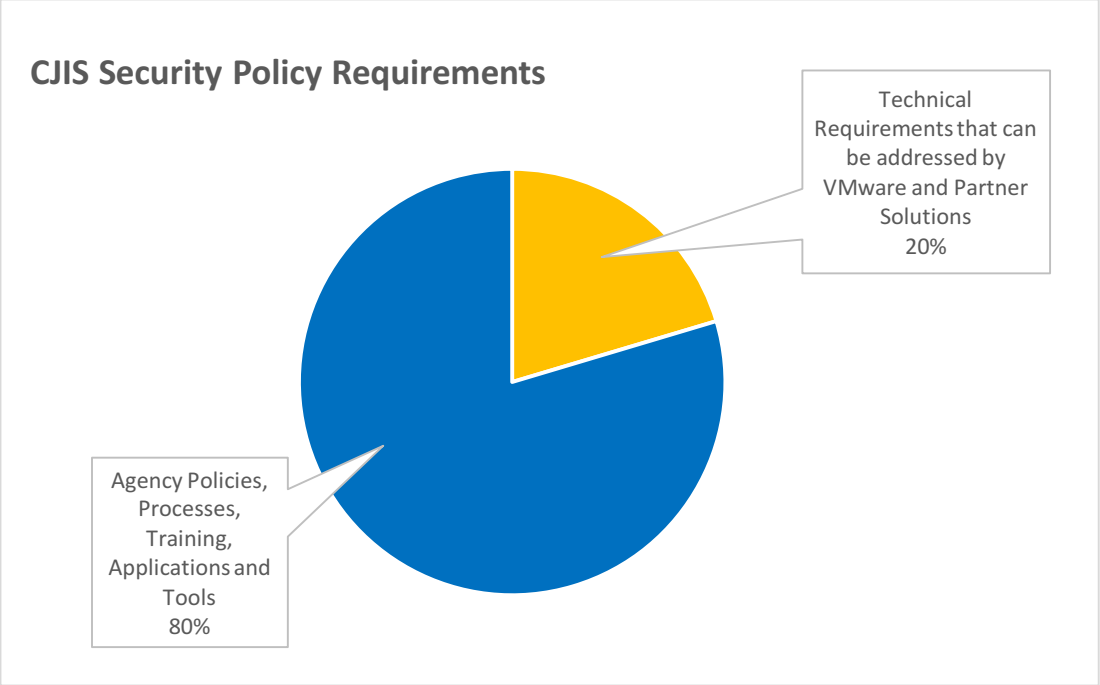

Figure 10: VMware and Partner Solution Coverage of CJIS Security Policy requirements

Table 3 illustrates a breakout of coverage by VMware Solutions, Partner Solutions, and the CJA or NCJA by CJIS Security Policy Areas. Primarily of note is the coverage capabilities in row three relevant to technical safeguards.

	CJIS Policy Areas	% Addressed by VMware Solutions	% Addressed by Partner Solutions	% Addressed by Agency
	1. Information Exchange Agreements	0	0	100
	2. Security Awareness Training	0	0	100
	3. Incident Response	0	0	100
	4. Audit and Accountability	10	30	60
	5. Access Control	15	15	70
	6. Identification and Authentication	5	20	75
	7. Configuration Management	25	20	70
	8. Media Protection	0	0	100
	9. Physical Protection	0	0	100
	10. Systems and Communications Protection and Information Integrity	45	45	10
	11. Formal Audits	0	0	100
	12. Personnel Security	0	0	100
	13. Mobile Devices	60	20	20

Table 3: CJIS Security Policy addressed by VMware, Partners and the Agency or Other

Additionally, VMware and partner solutions may be capable of meeting control requirements in alignment with further state, local, and agency specific regulations and/or policies. As these are likely varied and broad, they will not be covered in this document Likewise, an agency may be required to meet additional compliance frameworks and regulations such as HIPAA

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

or PCI. That being said, VMware is dedicated to security and compliance as illustrated in VMware's general approach to compliance.

VMware Control Capabilities Detail (By CJIS Security Policy Requirement Statement)

This section will only address the CJIS Security Requirements that are relevant to the VMware Solutions in scope for this assessment. It is assumed that requirements not covered in this section are addressable by other means. Furthermore, it is not assumed that any one technology could possibly meet all of the control requirements for any single CJIS Security Policy requirement. Where a technology is highlighted for capability to address or support a control objective, it is recommended that the CJA or NCJA evaluate any additional policies, procedures, standards, training, guidelines, and risk associated in order to more fully support controls necessary to address the CJIS Security Policy requirement.

Each policy statement addressed will include the policy statement taken from the CJIS Security Policy document. The policy statement is taken verbatim from the CJIS Security Policy. VMware Applicability will be a statement of how VMware technology can be used to enable controls to address the policy requirement. Additional considerations are the reflections of the assessor about implementation and/or other items for the reader of this document to consider. Relevant NIST 800-53 Controls is a list of controls taking from NIST SP 800-53 Revision 4 that align with the policy statement.

Policy Area 4: Auditing and Accountability

5.4.1 Auditable Events and Content (Information Systems)

CJIS Policy Statement: The agency's information system shall generate audit records for defined events. The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the source of the events, and the outcomes of the events.

VMware Capability

All VMware technologies in scope for this assessment that support interactive logon have the capability to align with the requirements of this policy statement. Additionally, all of the VMware solutions produce event logs that can be used for assessing the health and performance of the systems where abnormal operations may be an indicator of compromise. These logs can be configured to be collected and sent to a syslog server or security information and event management (SIEM) solution for further reporting, analysis, correlation, and alerting.

VMware vRealize Log Insight collects and analyzes all types of machine-generated log data, e.g., application logs, network traces, configuration files, messages, performance data, system state dumps, and more. It enables administrators to connect to everything in their environment, such as OS, apps, storage, and network devices, to provide a single location to collect, store, and analyze logs at scale. Log Insight features an intuitive interface to facilitate interactive searches and deep analytical queries for quick, actionable insights. Log Insight adds structure to unstructured log data. It delivers real-time monitoring, search, and log analytics. It has a dashboard for stored queries, reports, and alerts, enabling correlation of events across the entire IT environment.

While Log Insight is able to more quickly make sense of massive amount of unstructured data in the form of system, audit, and event logs, vRealize Operations collects information relative to structured data or metrics directly from applications, revealing historical and real time performance indicators. This can be useful for identifying issues within the environment, which allow the administrator or engineer to narrow the focus of remediation to the source of the issue and thus achieve timelier remediation and improved service levels. Integration of Log Insight findings with vRealize Operations can further enhance situation awareness, providing focused understanding of relevant event logs to structured metrics data. For improved situation awareness, the correlation of the information from vRealize Operations and vRealize Log Insight allows for improved inventory mapping where vSphere inventory items are directly tagged to events collected by log insight. With this tagging, alerting can be performed specifically with regard to the impacted object. These alerts from vRealize Log Insight are now capable of being visualized in the vRealize Operations console, producing a visual representation of the event correlated with the metric collected by vRealize Operations. Furthermore, the integration allows for the administrator to easily move between vRealize Operations and Log Insight and vice versa with respect to the object and or events that are being investigated.

Additional Considerations

Ultimately, it is up to the discretion of the agency as to which information systems are determined to produce logs for review. The statement of capability with regard to audit logging is simply an affirmation of the technologies ability to produce audit logs, should the agency determine that logs from a VMware technology in scope for their environment should be collected, reviewed, analyzed, and reported.

Relevant NIST 800-53 Controls: AC-9, AU-2, AU-2(3), AU-3, AU-3(1), AU-6, AU-6(1), AU-6(3), AU-12, CA-7

5.4.1.1 Events

CJIS Policy Statement: The following events shall be logged:

1. Successful and unsuccessful log-on attempts.
2. Successful and unsuccessful attempts to use:
    a. access permission on a user account, file, directory or other system resources;
    b. create permission on a user account, file, directory or other system resources;
    c. write permission on a user account, file, directory or other system resources;
    d. delete permission on a user account, file, directory or other system resources; and
    e. change permission on a user account, file, directory or other system resources.
3. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts.
5. Successful and unsuccessful attempts for users to:
    a. access the audit log file;
    b. modify the audit log file; and
    c. destroy the audit log file.

VMware Capability

Agencies typically utilize central account management solutions such as Microsoft Active Directory for handling identities and authentication. This solution will provide primary authentication for applications that are configured to be integrated with Active Directory. However, in most cases, these applications and technologies will additionally create events for access to the application either from the integrated directory solution or for local accounts, when local accounts are supported by the application. All VMware solutions that have interactive logon capability to a user interface are capable of logging the log-on attempt.

All VMware solutions are capable of logging activities relative to user account permission changes referenced to local application accounts; for instance, VMware Single Sign On (SSO) accounts. For all other authentication providers, the authentication provider will provide the logging mechanism on behalf of those accounts that it manages.

All VMware solutions that have local account creation capability or utilize local application or system accounts are capable of logging changes to passwords for those accounts. For all other authentication providers, the authentication provider will manage the logging mechanism, relative to password changes, on behalf of those accounts that it manages.

All VMware solutions that have audit logging facilities are capable of auditing attempts to access, modify, or destroy the audit logs created by that application or system.

Additional Consideration

For the purpose of simplification of identification, authentication and authorization. It is recommended to use a third party directory service provider such as Microsoft Active Directory. Within this solution, unique identities can be generated for each user. These users can be further added to security groups, also managed by the directory service. Within the application or system, these security groups can be tied to application roles for role-based authorization to perform duties within that application.

While most of the solutions from VMware can be integrated with a third party provider for identification and authentication, many also include the facilities to generate local user accounts. In this case, the requirements for audit logging should also apply to the local user account even if the local user account is not the primary means of access to the environment. The only exception to this might be if the local user accounts and the facilities to generate local user accounts are disabled.

Relevant NIST 800-53 Controls: AC-9, AU-2, AU-12, CA-7

5.4.1.1.1 Content

CJIS Policy Statement: The following content shall be included with every audited event:

1. Date and time of the event
2. The component of the information system (e.g., software component, hardware component) where the event occurred
3. The type of event
4. The user/subject identity shall be included with every audited event
5. Outcome (success or failure) of the event shall be included with every audited event

VMware Capability

Similar to the above statement with regard to the application or system requirement to generate audit logs, all VMware systems that generate audit and event logs are capable of meeting the requirement for this policy statement. The logs contain date and time of the event, the component of the information system where the event occurred, the type of event, the user/subject identity of the audited event, and the outcome (success or failure) of the event. When properly implemented, date and time are synchronized with an authoritative time source or are synched between components to ensure that log times match up for forensics.

Additional Considerations

This is a general statement of the VMware technology or solution capability. The determination of whether this capability will be required for formal audit and accountability activities is at the discretion of the agency.

Relevant NIST 800-53 Controls: AU-12

5.4.2 Response to Audit Process Failures

CJIS Policy Statement: The agency's information system shall provide alerts to appropriate agency officials in the event of an audit process failure.

VMware Capability

Most of the VMware technologies are incapable of monitoring and alerting on their own behalf in the event of an audit process failure. Third party solutions may be required to monitor services and daemons responsible for generating audit logs. Furthermore, disk space monitoring may be necessary to ensure that resources are sufficiently available to satisfy audit logging requirements. Many systems that generate logs have limited resources for long-term log retention. This can be problematic if there is a sudden increase in the number of logs being generated, which might cause logs to be overwritten. In this case, it is useful to have the logs that are generated by a system to be sent to a purpose built syslog facility or SIEM solution.

vRealize Log Insight delivers scalable log management with dashboards, analytics, and third party extensibility for operational visibility and faster troubleshooting. In addition to the broad range of analysis, correlation, and reporting capability, vRealize Log Insight is capable of monitoring the sources of logs that it collects or receives to determine whether the audit logging facilities are functioning properly. Failure to receive logs from a particular host may indicate a problem with that host's logging ability. Alerts can be configured to notify system administrators when logging for one of the configured hosts has failed. Moreover, vRealize Log Insight continuously monitors its own disk space and can be configured to generate alerts if the volume used to store log data is running low. The integration of Log Insight with vRealize Operations provides additional visibility to help troubleshoot and remediate issues.

Additional Considerations

Where feasible**,** when using a defense in depth approach to security, it is advisable to implement and integrate multiple solutions for validation of proper functionality. This strategy provides cross checking and redundancy.

Relevant NIST 800-53 Rev 4 Controls: AU-5, AU-5(2)

5.4.4 Time Stamps

CJIS Policy Statement: The agency's information system shall provide time stamps for use in audit record generation. The time stamp shall include the date and time values generated by the internal system clocks in the audit records. The agency shall synchronize internal system clocks on an annual basis.

VMware Capability

All VMware technologies and solutions discussed in this white paper that have audit logging capabilities are capable of using date and time values that are generated by internal system clocks and recording this time stamp in the audit records.

Additional Considerations

The policy requires that the agency synchronize internal system clocks on an annual basis. In order to reduce synchronization drift, where possible, systems should be configured to synchronize with a reliable pool of Network Time Protocol (NTP) servers. In the likely event that there are agency systems unable to communicate directly with a public pool of NTP servers, it is useful to establish internal agency NTP servers that can synchronize with a public NTP server pool. Those internal systems can then be configured to synchronize their time with the agency NTP server.

Relevant NIST 800-53 Controls: AU-8, AU-8(1)

5.4.5 Protection of Audit Information

CJIS Policy Statement: The agency's information system shall protect audit information and audit tools from modification, deletion, and unauthorized access.

VMware Capability

VMware vRealize Log Insight is the primary log management tool available from VMware. This tool, however, does not have built in protection mechanisms necessary to ensure that logs are protected from modification, deletion, and unauthorized access. If vRealize Log Insight is being utilized as a primary log management solution, it will be recommended to configure log insight for archiving of logs to a secure facility for the protection of those logs. Alternatively, through VMware's extensive partner ecosystem, the logs can also be collected by or received by a SIEM solution that has CJIS auditable capabilities for the integrity of logging.

Relevant NIST 800-53 Controls: AU-9, AU-9(4)

5.4.6 Audit Record Retention

CJIS Policy Statement: 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.

Additional Consideration

It is recommended to use an alternative solution for long-term audit record retention necessary to satisfy compliance requirements. While vRealize Log Insight is primarily used as a tool for troubleshooting existing or recent issues, it is not an ideal tool for long-term retention to be used as evidence to support audit or forensic investigations. VMware's partner ecosystem includes tools that are useful and able to be integrated with VMware solutions that are designed to meet this requirement. There multiple syslog and SIEM solutions available from partners in the partner network.

Relevant NIST 800-53 Controls: AU-4, AU-5(1), AU-9(2), AU-11

Policy Area 5: Access Control

5.5.2 Access Enforcement

CJIS Policy Statement: The information system shall enforce assigned authorizations for controlling access to the system and contained information. The information system controls shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed by agencies to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.

VMware Capability

Often the procedures for authorization or supervision of workforce members involve manual workflows that contain paper trails for request, approval, authorization, implementation, and supervision. These paper trails can be inclusive of online static forms, email requests, and paper forms, among other means. For many organizations, these procedural workflows can lack definition and are difficult to maintain and certify as they have developed organically over time. Finding records of request, authorization, and implementation and aligning these records into cohesive evidence of compliance can be cumbersome and time consuming. VMware vRealize Automation is capable of being configured to manage many organizationally standard workflow processes. Commonly, this is used for automating regular maintenance routines, regular incident response procedures and the like; however, the API is flexible and adaptable to allow for integration into other technical services such as user provisioning and management. The workflows can be orchestrated in such a way to match the workflow procedures defined by the organization and include steps such as request for access, acknowledgement of request, review of request, authorization of request, and implementation of authorized access. Through integration with other VMware and partner solutions, additional effort can be made to automate the generation of access reports that are necessary to perform personnel reviews.

Generally, all VMware technologies that allow user interaction are capable of being configured to support role-based authorizations for controlling activities that can be performed on the same technology. This is true for both end-user access and privileged user access. The VMware in-scope technologies provide built-in roles with associated assigned permissions. Typically, additional sample roles are available to aid management in the design and decision making process for the agency's particular use case. Custom roles are also capable of being created with specific assigned rights for interaction with the technology.

The VMware technologies in scope support configuration to enable least functionality and are configurable following VMware hardening guides to ensure that functionality of the solution both fits the purpose for which it was defined and does not allow any additional undesirable or unnecessary functionality for the agency's particular use case. The agency should work closely with the technology implementation team(s) to ensure that careful consideration for security and compliance are factored when making decisions to support least functionality and hardened configurations. For continuous support of hardening and compliance, VMware provides vRealize Configuration Manager as part of the Operations Suite.

Access authorization management also applies to authorization and access between devices on the network. Whether user devices, server devices, or workload tiers, restricting access by need prevents unintentional or intentional malicious access by or from those objects that do not meet the need to know requirement. Much as vRealize Automation can be developed to create workflows for user authorization, it can also be used in coordination with VMware NSX to ensure that when a device is deployed, it is deployed with the necessary security measures such as logical network segment, security group, logical firewall policies, and advanced security measures applied.

As it relates to end-user access to applications or data structures containing CJI, VMware Workspace ONE provides the means to restrict access based on organizationally defined access control matrices, as well as device access management controls. Workspace ONE can combine a number of different access capabilities supplied by its single sign-on capabilities. VMware Identity Manager supports dynamic access management by leveraging both identity and device management to enforce access decisions based on multiple criteria, including:

- Device compliance (state of the device including: rooted devices, presence of blacklisted applications, geolocation, OS patch level, and more)
- Authentication strength (Active Directory password, Kerberos, Certificate, and RSA SecureID)
- Network range, VLAN, Logical network
- Device Type (iOS, Android, Web Browser)
- Use of registered device certificates, managed timeouts, and PIN strength

Moreover, the catalog of available applications, including data and file repositories, can be dynamically restricted based on these and other criteria to ensure agency and CJIS procedural access rules are enforced and support expected patterns of behavior for end users.

To further control access, User Environment Manager, as part of the Workspace ONE offering, allows IT to centrally manage user profiles for use throughout the agencies platforms, giving the end-user a consistent experience across devices and

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

locations. Policies with respect to user digital work environment can be applied dynamically with access based on specific endpoint criteria. These related criteria may determine which networks or printers are accessible to an end user at any given time.

The cost and complexity of network configuration for desktop environments, using traditional centralized hardware-based approaches to networking and security, were restrictive. This resulted in organizations opting for flat network architectures. The assumption was, because these networks are on the “secure” side of organizational edge firewalls and security solutions, that they were secure enough. This reduces an approach for defense in depth by at least one factor on what is traditionally the weakest part of the organization’s infrastructure. By extending the functionality of VMware NSX for integration with Horizon VDI environments, these issues can more readily be addressed.

VMware NSX provides critical security and access control capabilities to the software-defined infrastructure components. Likewise, these same capabilities and integrations for network access control and security extend to virtual desktop infrastructure (VDI) networking. VMware NSX for Horizon allows policies to follow virtual desktops without the need for complex and time-consuming network provisioning. NSX allows for administration of network and security policies for users based on logical groupings, role, or tag. Policies are immediately attached to desktops as they are created and follow the desktop virtual machine irrespective of the underlying infrastructure. VMware NSX can reduce attack surface area with respect to East-West communications within a network. This can significantly reduce the probability for proliferation of malware, viruses, and security breaches, as each desktop is capable of being secured with network access policies applied as well as advanced security capabilities such as intrusion prevention, antivirus, malware, and next-gen security services. To secure virtual desktops and adjacent workloads within the data center, VMware NSX implements “micro-segmentation”, giving each desktop its own perimeter defense. This security uses NSX distributed firewalling capability to police traffic to and from each VM, eliminating unauthorized access between desktops and adjacent workloads. Additional virtualized network functions can be implemented for virtual desktops with NSX such as logical switching, routing, firewalling, and load balancing. Administrators can build virtual networks for VDI without the need for complex VLANs, ACLs, or hardware configuration syntax.

Additional Considerations

The agency should evaluate its needs relative to the options available with the technology to determine the best fit. Found within these technologies, with regard to authorization, is the means to enable separation of responsibility to the degree that it is feasible for the agency to improve accountability.

There is a capability of automating workflows, including access authorization, establishment, and modification with regard to integration capabilities with Microsoft Active Directory; however, it is advisable that such an effort not be considered lightly. The design of the workflow should be consistent with the covered entities’ and business associates’ already established business processes. The architecture of the solution should be flexible to support future updates to the dependent components. The capability of vRealize Automation is not intended to be a replacement for administrative responsibility for this control. Rather, vRealize Automation is capable of enhancing the administrative process.

Moreover, it is essential to understand the applications, services, and data that are being served by and on behalf of the agency and to define boundaries both within the organization’s network and outside the organization’s network. With respect to boundaries, understanding of ports, protocols, services, access policies, authorization requirements, and more are important for understanding the proper implementation of technology to support the organization’s requirements.

Relevant NIST 800-53 Controls: AC-2, AC-2(1), AC-2(7), AC-3, AC-3(3), AC-3(4), AC-5, AC-6(1), AC-6(2), AC-12(1), SC-23(1), SC-23(3)

5.5.2.2 System Access Control

CJIS Policy Statement: Access control mechanisms to enable access to CJI shall be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects.

Access controls shall be in place and operation for all IT systems to:

(1) Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJIS, unless the agency grants authority based upon operational business needs. Agencies shall document the parameters of the operational business needs for multiple concurrent active sessions.

(2) Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.

VMware Capability

With respect to CJI access, VMware's end-user compute platform, VMware Workspace ONE, provides the means to limit access to CJI applications, desktops, volumes, file repositories, and files. The access determination through VMware Identity Manager is capable of being configured for conditional access. Determination of access is dynamically determined by criteria, which can be identity-based with regard to user and device or both. For devices, the basis of identity could be type, conditional upon existence of security keys, or meet criteria with regard to device configuration. Additionally, the criteria can be security-based with regard to geographic, logical, or network location or with respect to strength of authenticator. These restrictions can be applied to end users accessing via desktops, laptops, and mobile devices.

The configurable restrictions can include, among other things, prevention of multiple concurrent active sessions for each user identification. This can ensure an additional measure of protection for CJI in the event that the application that accesses CJI does not specifically have this built in policy restriction. Moreover, users can be configured in groups whereby individuals are assigned to security groups with approval for multiple concurrent sessions.

For the hardware and software platform that make up the software-defined data center, VMware and partner technologies integrate with and make use of Intel Trusted Execution Technology (TXT), a Trusted Platform Module, built into the hardware chipset to establish a root of trust. This root of trust can be measured at boot-up to ensure that the hosts have been unaltered with regard to hardware, firmware, or operating environment. Using a partner solution such as HyTrust CloudControl, virtual cloud security can ensure that untrusted hosts are not allowed to participate in production environments.

Furthermore, VMware software-defined data center solutions can be locked down with specific permissions granted on a per virtual machine basis to prevent administrators from adding, changing, or removing component devices to virtual machines, including both server infrastructure and virtual desktop infrastructure. A clean build or golden image can be the basis for new server virtual machines ensuring that the initial sourcing of a virtual machine meets agency build specifications. Likewise, a golden image can be used for deployment of virtual desktops as well as physical desktops and laptops.

VMware vRealize Operations can ensure through configuration management that the approved configuration of all devices is according to the agency specification and continues to be so.

Additional Consideration

VMware and its partners provide solutions that can help to initiate and maintain the integrity of the environment and restrict or control access to critical applications and data. This also requires careful planning, consideration, and coordination to ensure that the implementation of these technologies fully support and enable the controls to meet this policy requirement. Additional measures are recommended with respect to CJI applications that provide access to CJI, including files and records. The agency should consider the efficacy of such applications to enable its own control measures to extend or enhance the security of CJI beyond the platform.

Relevant NIST 800-53 Controls: AC-2, AC-2(4), AC-2(7), AC-5, AC-6, AC-6(5), AC-6(9), AC-10, RA-5(5)

5.5.2.3 Access Control Criteria

CJIS Policy Statement: Agencies shall control access to CJI based on one or more of the following:

(1) Job assignment or function (i.e., the role) of the user seeking access.

(2) Physical location.

(3) Logical location.

(4) Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside).

(5) Time-of-day and day-of-week/month restrictions.

5.5.2.4 Access Control Mechanisms

CJIS Policy Statement: When setting up access controls, agencies shall use one or more of the following mechanisms:

(1) Access Control Lists (ACLs). ACLs are a register of users (including groups, machines, processes) who have been given permission to use a particular object (system resource) and the types of access they have been permitted.

(2) Resource Restrictions. Access to specific functions is restricted by never allowing users to request information, functions, or other resources for which they do not have access. Three major types of resource restrictions are menus, database views, and network devices.

(3) Encryption. Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key. While encryption can provide strong access control, it is accompanied by the need for strong key management. Follow the guidance in Section 5.10.2 for encryption requirements if encryption of stored information is employed as an access enforcement mechanism.

(4) Application Level. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level to provide increased information security for the agency.

VMware Capability

VMware NSX is capable of enabling access restrictions according to a number of criteria. Utilizing micro-segmentation, a technology whereby network security is capable of being applied down to the virtual machine level, rule sets for access can be enabled to restrict access to resources based on user or device roles, as well as logical location and network address. With dynamic geotagging enabled for virtual machines, these restrictions can also be applied to physical location. The capability of NSX to support access controls is applicable to both the software-defined data center and end-user computing when integrated with Horizon with respect to VDI.

VMware NSX Edge Gateway provides SSL VPN-Plus to allow remote users access to private networks using an SSL client. Remote users can access servers and applications on the private network according to policy and rights assignments applied to and granted to the user respectively.

Additional controls can be enabled for the determination of sources for end user connections, whether within the boundaries of a secure environment, outside the boundaries of the secure environment, or remote from some other physical or geographic location. Based on location parameters, access controls can be enabled to ensure that devices and users can connect from trusted or authorized locations.

Through the use of integrated and combined components from AirWatch and VMware Identity Manager, VMware Workspace ONE can also apply defined requirements for access into technical control mechanisms to restrict end-user access to CJIS environments. The configuration enablement of VMware Workspace ONE can restrict access to CJI based on the following criteria:

- Job assignment or function as defined by an integrated directory services solution.
- Physical location as defined by geotagging for the user and device requesting access.
- Logical location as defined by the location of the device on the network.
- Network IP Address to determine if the user and the device are accessing from within the agency's secure boundaries or outside the secure boundary from the Internet.

Moreover, the access control mechanisms capable of being supported by VMware Workspace ONE include, but are not limited to:

- Access Control Lists – access authorizations can be defined by both device and user, whereby by the authorization or access granted is a dynamic and combined determination of the access controls authorized for the user and the device. Additionally, the solution can be configured in such a way that the device and/or user must meet additional criteria before being authorized.
- Resource Restrictions – beyond the resource restrictions that should be included in the CJI application, VMware Workspace ONE catalog can be pre-determined by set criteria. These criteria are used to define the catalog of applications, services, and data to which the end user can subscribe. This allows for the consumerization benefit of self-provisioning while limiting the applications and data on a need to know basis.
- Encryption – this control mechanism is more than likely related to the capability of unlocking encrypted data based on access rights with respect to authorization, whereby the decryption key is only provided to those who are authorized. This can be done through key management systems with respect to verified criteria. VMware Identity Manager can manage and integrate with certificates for authentication.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Additional Considerations

Where encryption is chosen as a means for establishing access, it will be necessary to implement a key management solution for the protection and distribution of encryption keys for use by end-users and end-user devices.

Relevant NIST 800-53 Controls: AC-2, AC-2(4), AC-2(7), AC-5, AC-6, AC-6(5), AC-6(9), AC-10, RA-5(5)

5.5.3 Unsuccessful Login Attempts

CJIS Policy Statement: Where technically feasible, the system shall enforce a limit of no more than five consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI). The system shall automatically lock the account/node for a 10-minute time period unless released by an administrator.

VMware Capability

All of the technologies in scope for this application rely on third party access management platform as its primary means of access management. Many of the VMware solutions, included in scope for this white paper, also have local system or application accounts, which can be configured to comply with unsuccessful logon attempt requirements.

Additional Considerations

When using third party access management solutions, such as Microsoft Active Directory, as the primary means of access, sometimes the local account management is overlooked. It is important not to overlook the local account management capabilities where they exist as they often provide a foothold or means for an attacker to gain access. This is especially important for sensitive infrastructure platform components on which much of an agency's critical data and applications sit. These local accounts should be monitored and managed with the same scrutiny of a directory service account.

Relevant NIST 800-53 Controls: AC-7, IA-5(1)

5.5.4 System Use Notification

CJIS Policy Statement: The information system shall display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules. The system use notification message shall, at a minimum, provide the following information:

(1) The user is accessing a restricted information system.

(2) System usage may be monitored, recorded, and subject to audit.

(3) Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.

(4) Use of the system indicates consent to monitoring and recording.

The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system.

Privacy and security policies shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly access systems:

(i) the system use information is available and, when appropriate, is displayed before granting access;

(ii) any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and

(iii) the notice given to public users of the information system include a description of the authorized use of the system.

VMware Capability

VMware technologies, which have interactive logon capability to a management console or application user interface, can be configured to enable system use notifications.

Relevant NIST 800-53 Controls: AC-8, AC-11(1), AC-22

5.5.5 Session Lock

CJIS Policy Statement: The information system shall prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Users shall directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. A session lock is not a substitute for logging out of the information system.

VMware Capability

All critical user interfaces for the VMware products in scope are configurable to allow for idle session timeout, whereby the idle session is disconnected and/or logged off. The amount of idle time that is permitted is configurable in most cases to address the policy requirement. After a session lock has been initiated, the user is required to present its authentication credentials to either re-login or re-establish connection to the existing running connection.

Additional Considerations

Some agencies may determine that the session lock on the device that is being used to provide access is sufficient. However, if it is feasible, session locks should be capable of being enabled at the application or user interface level as well. This guards against the possibility that one layer of protection has been compromised. It also ensures that session locks can be established regardless of the device being used, as in the case of permitted personally owned equipment that may not have the same policy requirements as organizationally controlled equipment. In this case, the separation of secure environments from non-secure device may be able to be established through remote desktops or application portals that provide this level of security.

Relevant NIST 800-53 Controls: AC-11

5.5.6 Remote Access

CJIS Policy Statement: The agency shall authorize, monitor, and control all methods of remote access to the information system. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency-controlled network (e.g., the Internet).

The agency shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The agency shall control all remote accesses through managed access control points.

VMware Capability

VMware NSX Edge Gateway provides SSL VPN-Plus to allow for remote users access to private networks using an SSL client. Remote users can access servers and applications securely on the private network according to policy and rights assignment applied and granted to each user, respectively.

Additional control is capable of being applied for remote access to secure private networks though VDI and virtual applications.

Additional Considerations

This control primarily pertains to temporary access that may be granted for the purpose of remote technical support. In this case, it is not intended to be a permanent connection. The lifespan of the connection is positively correlated to the security risk the connection presents. A longer life span for a remote connection presents opportunities for malicious users to hijack the connection. The connection should be monitored and controlled to ensure that the connection of the originating remote user supports non-repudiation. For privileged access granted to a remote support technician from a technology vendor, a greater level of scrutiny should be applied. In this case, it is possible to use a secure remote desktop, using VMware Horizon, to allow a remote user to establish connection to the secure environment. This also can allow agency personnel to shadow the work of the remote technician, ensuring that the work that is being performed as expected and commensurate with the work plan.

Relevant NIST 800-53 Controls: AC-17, AC-17(3), AC-17(4), AC-17(6)

5.5.6.1 Personally Owned Information Systems

CJIS Policy Statement: A personally owned information system shall not be authorized to access, process, store, or transmit CJI unless the agency has established and documented specific terms and conditions for personally owned information system usage. When personally owned mobile devices (i.e. bring your own device [BYOD]) are authorized, they shall be controlled in accordance with the requirements in Policy Area 13: Mobile Devices

VMware Capability

VMware provides the means to allow personally owned devices to be used in a secure manner. The technology available through VMware Horizon, VMware Workspace One, and AirWatch can ensure that the personally owned information system has no direct connection to CJI for processing, transmission, or storage. The remote desktop or application is obfuscated from the personally owned device and is containerized and separate from that of the accessing device.

Additional Considerations

This policy is administrative in that it requires the agency to make a determination of the circumstances for which a personally owned device can be used to access, process, store, or transmit CJI. VMware technology provides a means to ensure that personally owned devices can be used as a vehicle to remotely access these resources. In this case, the VMware technology informs the agency of measures and means that can be employed to support opportunities for BYOD. That being said, those personally owned devices when used for these purposes must be controlled in accordance with Policy Area 13: Mobile Devices. That control capability will be discussed further in following sections.

Relevant NIST 800-53 Controls: AC-17

Policy Area 6: Identification and Authentication

5.6.2.1.1 Password

CJIS Policy Statement: Agencies shall follow the secure password attributes, below, to authenticate an individual's unique ID. Passwords shall:

1. Be a minimum length of eight (8) characters on all systems.
2. Not be a dictionary word or proper name.
3. Not be the same as the User ID.
4. Expire within a maximum of 90 calendar days.
5. Not be identical to the previous ten (10) passwords.
6. Not be transmitted in the clear outside the secure location.
7. Not be displayed when entered.

5.6.2.1.2 Personal Identification Number (PIN)

CJIS Policy Statement: When agencies implement the use of a PIN as a standard authenticator, the PIN attributes shall follow the guidelines in Section 5.6.2.1.1 (password). When agencies utilize a PIN in conjunction with a certificate or token (e.g., key fob with rolling numbers) for the purpose of advanced authentication, agencies shall follow the PIN attributes described below. For example, a user certificate is installed on a smartphone for the purpose of advanced authentication (AA). As the user invokes that certificate, a PIN meeting the below attributes shall be used to access the certificate for the AA process.

1. Be a minimum of six (6) digits
2. Have no repeating digits (i.e., 112233)
3. Have no sequential patterns (i.e., 123456)
4. Not be the same as the User ID
5. Expire within a maximum of 365 calendar days
    a. If a PIN is used to access a soft certificate, which is the second factor of authentication, AND the first factor is a password that complies with the requirement in Section 5.6.2.1.1, then the 365-day expiration requirement can be waived by the CSO.
6. Not be identical to the previous three (3) PINs
7. Not be transmitted in the clear outside the secure location
8. Not be displayed when entered

EXCEPTION: When a PIN is used for local device authentication, the only requirement is that it be a minimum of six (6) digits.

VMware Capability

Access authorization and management including password policies are most likely to be managed by a third party access management or directory services solution. However, in cases where local accounts are present, the technology that

supports local account access should be capable of policy adherence. VMware technologies that provide local accounts for user or system access meet the configuration requirements necessary to support these policy statements.

VMware Identity Manager provides the following capabilities for user authentication and credential/token handling:

- Identity Manager integrates with AirWatch Enterprise Mobility Management (EMM) to enable the industry-first seamless SSO to native mobile apps using biometric, password, and multi-factor authentication
- Single Sign On capability using SAML assertions and authentication standards such as Active Directory password, Kerberos, Certificate, and RSA SecurID
- Single Sign-On access to systems and applications located across organizational boundaries using Active Directory Federated Services (AF DS)

VMware Identity Manager allows the agency to enforce strict identity and authenticator standards while at the same time simplifying the end-user's authentication experience.

Relevant NIST 800-53 Controls: IA-5, IA-5(1), IA-5(4)

5.6.2.2 Advanced Authentication

CJIS Policy Statement: Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as biometric systems, user-based digital certificates (e.g. public key infrastructure (PKI)), smart cards, software tokens, hardware tokens, paper (inert) tokens, out-of-band authenticators (retrieved via a separate communication service channel – e.g., authenticator is sent on demand via text message, phone call, etc.), or "Risk-based Authentication" that includes a software token element comprised of a number of factors, such as network information, user information, positive device identification (i.e. device forensics, user pattern analysis, and user binding), user profiling, and high-risk challenge/response questions. When user-based certificates are used for authentication purposes, they shall be specific to an individual user and not to a particular device, and they shall prohibit multiple users from utilizing the same certificate.

1. Require the user to "activate" that certificate for each use in some manner (e.g., passphrase or user-specific PIN).

5.6.2.2.1 Advanced Authentication Policy and Rationale

Policy Guidance: The requirement to use or not use AA is dependent upon the physical, personnel, and technical security controls associated with the user location and whether CJI is accessed directly or indirectly. AA shall not be required for users requesting access to CJI from within the perimeter of a physically secure location (Section 5.9), when the technical security controls have been met (Sections 5.5 and 5.10), or when the user has no ability to conduct transactional activities on state and national repositories, applications, or services (i.e. indirect access). Conversely, if the technical security controls have not been met, AA shall be required even if the request for CJI originates from within a physically secure location. Section 5.6.2.2.2 provides agencies with a decision tree to help guide AA decisions. The CSO will make the final determination of whether access is considered indirect. The intent of AA is to meet the standards of two-factor authentication. Two-factor authentication employs the use of two of the following three factors of authentication: something you know (e.g. password), something you have (e.g. hard token), something you are (e.g. biometric). The two authentication factors shall be unique (i.e. password/token or biometric/password but not password/password or token/token).

EXCEPTION:
AA shall be required when the requested service has built AA into its processes and requires a user to provide AA before granting access.

EXAMPLES:

a. A user, irrespective of his/her location, accesses the LEEP portal. The LEEP has AA built into its services and requires AA prior to granting access. AA is required.
b. A user, irrespective of their location, accesses a State's portal through which access to CJI is facilitated. The State portal has AA built into its processes and requires AA prior to granting access. AA is required.

5.6.2.2.2 Advanced Authentication Policy and Rationale

Policy Guidance Continued: The following AA Decision Tree, coupled with figures 9 and 10 below, assists decision makers in determining whether AA is required.

1. Can request's physical originating location be determined? If either (a) or (b) below are true, the answer to the above question is "yes". Proceed to question number 2.
    a. The IP address is attributed to a physical structure; or
    b. The mnemonic is attributed to a specific device assigned to a specific location that is a physical structure. If neither (a) or (b) above are true, then the answer is "no". Skip to question number 4.

2. Does request originate from within a physically secure location as described in Section 5.9.1? If either (a) or (b) below are true, the answer to the above question is "yes". Proceed to question number 3.
    a. The IP address is attributed to a physically secure location; or
    b. If a mnemonic is used, it is attributed to a specific device assigned to a specific physically secure location. If neither (a) or (b) above are true, then the answer is "no". Decision tree completed. AA required.

3. Are all required technical controls implemented at this location or at the controlling agency? If either (a) or (b) below are true, the answer to the above question is "yes". Decision tree completed. AA requirement waived.
    a. Appropriate technical controls listed in Sections 5.5 and 5.10 are implemented; or
    b. The controlling agency (i.e. parent agency or agency leveraged as conduit to CJI) extends its wide area network controls down to the requesting agency and the extended controls provide assurance equal or greater to the controls listed in Sections 5.5 and 5.10. If neither (a) or (b) above are true, then the answer is "no". Decision tree completed. AA required.

4. Does request originate from an agency-controlled user device? If either (a) or (b) below are true, the answer to the above question is "yes". Proceed to question number 5.
    a. The static IP address or MAC address can be traced to registered device; or
    b. Certificates are issued to agency-managed devices only, and certificate exchange is allowed only between authentication server and agency issued devices. If neither (a) or (b) above are true, then the answer is "no". Decision tree completed. AA required.

5. Is the agency-managed user device associated with and located within a criminal justice conveyance? If any of the (a) (b), or (c) statements below are true, the answer to the above question is "yes". Proceed to Figure 9 Step 3.
    a. The static IP address or MAC address is associated with a device associated with a criminal justice conveyance; or
    b. The certificate presented is associated with a device associated with a criminal justice conveyance; or
    c. The mnemonic presented is associated with a specific device assigned and that device is attributed to a criminal justice conveyance. If none of the (a), (b), or (c) statements above are true, then the answer is "no". Skip to question number 7.

6. Is the user device an agency-issued and controlled smartphone or tablet? If both (a) and (b) below are true, the answer to the above question is "yes." Proceed to question number 7.
    a. The law enforcement agency issued the device to an individual; and
    b. The device is subject to administrative management control of the issuing agency. If either (a) or (b) above is false, then the answer is "no." Decision tree completed. AA required.

7. Does the agency-issued smartphone or tablet have CSO-approved AA compensating controls implemented? If (a) and (b) below are true, the answer to the above question is "yes." Decision tree completed. AA requirement is waived.
    a. An agency cannot meet a requirement due to legitimate technical or business constraints; and
    b. The CSO has given written approval permitting AA compensating controls to be implemented in lieu of the required AA control measures. If either (a) or (b) above is false, then the answer is "no." Decision tree completed. AA required.

VMware Capability

VMware technologies provide the means to support advanced authentication for access to resources within the environment. Though VMware does not provide its own multi-factor authentication solutions, its technologies are capable of being integrated with third party two-factor authentication solutions. This includes VMware Horizon, VMware Workspace ONE, AirWatch Enterprise Mobility Manager, and improved identity management with VMware Identity Manager.

VMware Identity Manager provides the following capabilities for user authentication and credential/token handling when services may require higher strength, or 'step-up', authentication:

- Enforce Conditional Access to services-based managed and un-managed devices, device security posture, network location, and application types
- Requiring specific authentication types, including Active Directory password, Kerberos, Certificate, and RSA SecurID, based on Conditional Access requirements
- VMware NSX may be leveraged with VMware Identity Manager SSO and AirWatch per-app VPN to isolate and policy manage services deep within the data center

This allows the agency to define within VMware Identity Manager the conditions or criteria for which a higher level of authentication is required, including the need for additional factors for authentication.

Additional Considerations

While the application with direct access to CJI may include built in two-factor authentication capabilities, it may be advisable to ensure that multi-factor authentication is used for the infrastructure that supports that application. This provides an additional layer of protection, which can prevent a malicious user from gaining access to the infrastructure where he or she may be able to obtain more information about the environment, which may prove useful for further infiltration.

NIST 800-53 Relevant Controls: IA-2(1), IA-2(2), IA-2(3), IA-2(4), IA-2(11), IA-2(13), IA-3(1), IA-5(2), IA-5(11), MA-4, SC-37, SC-37(1)

Policy Area 7: Configuration Management

There are a number of general capabilities that can be addressed with regard to configuration management beyond those requirements specified in the CJIS Security Policy. VMware vRealize Configuration Management is capable of establishing a baseline configuration whereupon deviations can be detected and designated personal notified with built in response mechanisms. This can enable a consistent and ongoing confirmation of compliance to an agency established standard. Moreover, vRealize Configuration Manager can check the components of the systems environment against best practices for hardening and securing according to common compliance frameworks.

To ensure the continued adherence to policy and the protection of the systems, vRealize Configuration Manager can implement configuration changes to address security vulnerabilities, thus establishing an updated operational baseline. Through integration with other VMware technologies, agents for Linux and Windows, and management packs, vRealize Configuration Manager can be configured to manage security patches and updates for various system components.

5.7.1.1 Least Functionality

CJIS Policy Statement: The agency shall configure the application, service, or information system to provide only essential capabilities and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.

VMware Capability

VMware vRealize Configuration Manager can help assist an agency with decisions regarding implementation of least functionality throughout the organization. With built in hardening guides, management packs, and compliance configuration checks, the process for implementing and maintaining least functionality can be better supported. vRealize Configuration Manager is a system that provides capability to automate checklists for compliance and configuration to ensure adherence to the designed configuration. Moreover, to continually support compliance, it is able to address identified vulnerabilities by providing a mechanism to patch the vulnerable systems.

Policy Area 10: System and Communications Protection and Information Integrity

5.10.1 Information Flow Enforcement

CJIS Policy Statement: The network infrastructure shall control the flow of information between interconnected systems. Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent

accesses to that information. In other words, controlling how data moves from one place to the next in a secure manner. Examples of controls that are better expressed as flow control than access control (see Section 5.5) are:

1. Prevent CJI from being transmitted unencrypted across the public network.
2. Block outside traffic that claims to be from within the agency.
3. Do not pass any web requests to the public network that are not from the internal web proxy.

Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.

VMware Capability

VMware vSphere Distributed Switches (vDS) or VMware NSX logical switches are capable of being configured to assign ports on the virtual switch to a port group. The port group can be assigned to a specific network VLAN and/or private VLAN. Through this capability, virtual machine communications within a host or cluster of hosts can be limited. VMware NSX provides the means to further segment networks using logical network overlays or virtual extensible LANs (VXLANs). Using NSX Edge logical distributed router provides East-West distributed routing with tenant IP address space and data path isolation. These network segments can further be protected with additional security services.

VMware NSX is capable of enabling transmission security by enabling segmentation and micro-segmentation of networks. Policies are enabled to enforce restrictions to and from networks and network devices to prevent unauthorized access over the virtualized lines of transmission. These network access controls can be enforceable to network segments, applications, virtual machines, and/or users. As previously discussed, VMware NSX is also capable of being integrated with additional network security measures provided by VMware partners, such as intrusion prevention, intrusion detection, next generation firewalls, and antivirus and anti-malware solutions.

VMware NSX also supports multiple VPN-based access methods to the virtual environment. VPN can be enabled to support site-to-site connections as well as SSL VPN connections for end users into the environment. This site-to-site IPSEC solution can provide both authentication and encryption mechanisms to grant access to the cloud environment and then only to those segments of the environment that are authorized.

VMware Horizon and AirWatch Enterprise Mobility Manager enable containerized secure access to apps and data. Access to sensitive apps and data is only available within the confines of the secure container. In this case, users only need to be concerned with curious shoulder surfers and would be required to have controls in place to minimize this activity.

Relevant NIST 800-53 Controls: AC-4, AC-20, AC-20(1), CA-3, CA-9, IA-5(7), SC-7(4), SC-7(8), SC-7(11), SC-10, SC-15, SC-15(1)

5.10.1.1 Boundary Protection

CJIS Policy Statement: The agency shall:

1. Control access to networks processing CJI.
2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.
3. Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels). See Section 5.13.4.4 for guidance on personal firewalls.
4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.
5. Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device shall “fail closed” vs. “fail open”).
6. Allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces. Publicly accessible information systems residing on a virtual host shall follow the guidance in Section 5.10.3.2 to achieve separation.

VMware Capability

VMware NSX Edge provides network edge security and gateway services to isolate a virtualized network. You can install NSX Edge as either a logical (distributed) router or a services gateway. The NSX Edge logical (distributed) router provides East-West distributed routing with tenant IP addresses and data path isolation.

VMware NSX Edge gateway connects isolated, stub networks to shared (uplink) networks by providing common gateway services such as DHCP, VPN, NAT, dynamic routing, and Load Balancing. Common deployments of NSX Edge include the DMZ, VPN Extranets, and multi-tenant Cloud environments where the NSX Edge creates a virtual boundary for each tenant. For a single entity using the services in this manner, it can allow for segmentation or separation of resources for distinct business units, for example those CJI data environments and non-CJI data environments. When placed at the agencies physical boundary, the Edge gateway becomes an extra layer of boundary protection from the Internet.

Addition Edge Gateway Services are included as follows:

Dynamic Routing: Provides the necessary forwarding information between layer 2 broadcast domains, thereby allowing you to decrease layer 2 broadcast domains and improve network efficiency and scale. NSX extends intelligence to where the workloads reside for East-West routing. This allows more direct virtual machine to virtual machine communication without the costly or timely need to extend network hops. At the same time, NSX also provides North-South connectivity, thereby enabling access to public networks.

Firewall: Supported rules include IP 5-tuple configuration with IP and port ranges for stateful inspection of all protocols.

Network Address Translation: Separate controls for Source and Destination IP addresses, as well as port translation.

Dynamic Host Configuration Protocol: Configuration of IP pools, gateways, DNS servers, and search domains.

Site-to-Site Virtual Private Network (VPN): Uses standardized IPsec protocols to interoperate with all major VPN vendors.

L2 VPN: Provides the ability to stretch L2 network.

SSL VPN-Plus: SSL VPN-Plus enables remote users to connect securely to private networks behind the NSX Edge gateway.

Load Balancing: Simple and dynamically configurable virtual IP addresses and server groups.

High Availability: ensures an active NSX Edge on the network in case the primary NSX Edge virtual machine is unavailable.

VMware NSX Edge Services are capable of supporting syslog exports for all available services to remote servers for analysis, correlation, and reporting purposes.

This solution provides an efficient solution for not only protecting North-South traffic to and from public networks, but also protecting the network at key internal boundaries in support of inspection of East-West traffic.

Moreover, through a rich network of partners, VMware NSX provides an API that allows for insertion of services for advanced security capabilities, including Intrusion Detection/Protection, Application Firewall, and Antivirus and Antimalware solutions.

The ease of deployment of NSX as opposed to traditional physical networking models allows security to be applied day one. Moreover, NSX supports the mobility of workloads that is a hallmark of virtualization. Virtual machines that migrate in the infrastructure through VMotion are automatically and continuously protected.

Relevant NIST 800-53 Controls: AC-20, CA-3(1), CA-3(2), CA-3(5), PE-3(2), SC-5, SC-5(1), SC-5(2), SC-7, SC-7(3), SC-7(4), SC-7(5), SC-7(7), SC-7(8), SC-7(11), SC-7(12), SC-7(13), SC-7(14), SC-7(18), SC-24

5.10.1.3 Intrusion Detection Tools and Techniques

Policy Statement: The agency shall implement network-based and/or host-based intrusion detection tools.

The CSA/SIB shall, in addition:

1. Monitor inbound and outbound communications for unusual or unauthorized activities.
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.

3. Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.

VMware Capability

VMware NSX allows for service insertion with the NSX distributed firewall or Edge Gateway to include advanced security services from VMware Partner solutions. This service insertion enables the distribution of IDS/IPS virtual appliances to any location within the virtual environment. It can be applied to workloads, resource groups, or individual virtual machines. Traffic is routed through the inspection engine in line with either the distributed firewall or Edge Gateway with minimal impact to performance.

Additional Considerations

The agency should determine appropriate locations for application of security within the environment, including where it may be necessary with respect to East-West communications to include IDS/IPS inspection.

Relevant NIST 800-53 Controls: SC-7(19), SI-4, SI-4(1), SI-4(2), SI-4(4), SI-4(5), SI-4(7), SI-4(9), SI-4(11), SI-4(12), SI-7, SI-7(1), SI-7(7)

5.10.3.1 Partitioning

CJIS Policy Statement: The application, service, or information system shall separate user functionality (including user interface services) from information system management functionality. The application, service, or information system shall physically or logically separate user interface services (e.g. public web pages) from information storage and management services (e.g. database management). Separation may be accomplished through the use of one or more of the following:

1. Different computers.
2. Different central processing units.
3. Different instances of the operating system.
4. Different network addresses.
5. Other methods approved by the FBI CJIS ISO.

VMware Capability

In most cases, the separation of functionality will be provided through the physical means described in this policy statement. A good design may include, at a minimum, the separation of compute resources each to facilitate management, application, and edge or DMZ environments respectively. Each of these resources can further be segmented by network wherein each environment represents a different LAN with routing and layer 4 – 7 inspection between them. This is a design that may be feasible for a CJIS environment. Additional capabilities of partitioning or separation can be supplied by VMware technologies. These capabilities extend not only to server infrastructures, but also to virtual desktop infrastructures.

Virtualization supplies a way to enable this separation with greater efficiency than traditional all hardware methods. By virtualizing CPU, Memory, Network, and layering on operating systems and applications on these constructs, workloads with different functions can co-exist on the same physical platform. These virtual resources are protected and separated from the other virtual resources through the virtual machine manager (VMM). In this way, the virtual resource does not have direct access to the physical processor or memory. This prevents any non-network communication between virtual machines.

VMware provides the means through the use of different network interfaces to separate management functionality from user functionality. Moreover, it provides the capability through logical switches, logical routers, and gateway services to separate various facets of the environment and control the interconnectivity of servers and workstations within the environment.

The physical storage that virtual machines use is further abstracted. This increases the efficiency with regard to the usage of storage while preventing unauthorized access to the storage. Nevertheless, it is ideal to ensure physical or minimally logical separation of storage networks from the other networks in the environment. This ensures the integrity and availability of the storage.

Relevant NIST 800-53 Controls: SC-2, SC-2(1), SC-3, SC-4, SC-32

5.10.3.2 Virtualization

Policy Statement: Virtualization refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments. Virtualized environments are authorized for criminal justice and noncriminal justice

activities. In addition to the security controls described in this Policy, the following additional controls shall be implemented in a virtual environment:

1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.
2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment.
3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) shall be physically separate from virtual machines (VMs) that process CJI internally or be separated by a virtual firewall.
4. Drivers that serve critical functions shall be stored within the specific VM they service. In other words, do not store these drivers within the hypervisor, or host operating system, for sharing. Each VM is to be treated as an independent system – secured as independently as possible.

The following additional technical security controls shall be applied in virtual environments where CJI is comingled with non-CJI:

1. Encrypt CJI when stored in a virtualized environment where CJI is commingled with non-CJI or segregate and store unencrypted CJI within its own secure VM.
2. Encrypt network traffic within the virtual environment.

The following are additional technical security control best practices and should be implemented wherever feasible:

1. Implement IDS and/or IPS monitoring within the virtual environment.
2. Virtually or physically firewall each VM within the virtual environment to ensure that only allowed protocols would transact.
3. Segregate the administrative duties for the host.

VMware Capability

VMware solutions meet or exceed the requirements of the CJIS Security Policy with regard to virtualization. As already discussed in previous sections, with regard to firewall protection between virtual machines, VMware NSX minimally provides a stateful firewall with Application Layer Gateway technology to protect the interconnectedness of virtual machines. Each virtual machine is capable of being configured by policy with a virtual firewall that sits between the network and the virtual machines network interface card.

By design, virtual machines are not allowed to have access to host files, firmware, BIOS, and drivers. These attributes of the host are capable of being protected using Intel TXT technology to ensure the host maintains its root of trust.

The maintenance of audit logs is capable of either being performed through log collection capabilities of vRealize Log Insight or further being shipped to a partner SIEM solution.

The design of a virtualized environment can include the separation of a DMZ environment onto a separate and distinct physical compute cluster. In this case, the DMZ environment can be isolated from a network perspective with virtual Edge Gateway services. Depending on the size of the environment and feasibility for this design, virtual machines as previously discussed can also be segmented from each other using virtual firewalls.

The distribution of virtual networking services to virtual machines allows each virtual machine to have its own security services and drivers applied. Additional drivers and/or services are available from VMware partners for layering on security directly on the virtual machines operating system.

Partner solutions also integrate with VMware solutions to provide both at rest and in-transit encryption capabilities. These solutions protect the volumes of virtual machines by encrypting the entire volume or the data contained therein.

Relevant NIST 800-53 Controls: SC-2, SC-4

5.10.4.1 Patch Management

CJIS Policy Statement: The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor)

shall develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs, and hot fixes. Local policies should include such items as:

1. Testing of appropriate patches before installation.
2. Rollback capabilities when installing patches, updates, etc.
3. Automatic updates without individual user intervention.
4. Centralized patch management.

Patch requirements discovered during security assessments, continuous monitoring, or incident response activities shall also be addressed expeditiously.

VMware Capability

vCenter Update Manager provides awareness of available patches from VMware for use with its products. vCenter Update Manager can provide insight to engineers and administrators as to the patch level of the infrastructure components relative to vendor available patches. Furthermore, patching can be automatically or manually scheduled to be performed in a guided manner to reduce or eliminate downtime during the patching cycle. This makes use of technologies such as VMware vMotion to migrate virtual machines to other available resources while a single or multiple hosts are being patched.

Patching of virtual machine drivers or VMware Tools, similarly, can be patched in a guided manner. The advantage of Update Manager is that virtual machines are capable of having a snapshot taken prior to the patch being applied. This allows for failback in the event that the updating or patching of VMware Tools causes issues.

vRealize Operations includes configuration management that is capable of supporting patching of Microsoft and Linux virtual machines with vendor specific patches. This also enables awareness for architects, engineers, and administrators as to the compliance level of the servers in the environment with respect to available vendor patches.

Relevant NIST 800-53 Controls: CM-3, CM-4, CM-4(1), RA-5, RA-5(1), RA-5(2), RA-5(3), SA-11, SA-11(1), SI-2, SI-2(2), SI-2(3)

5.10.4.2 Malicious Code Protection

CJIS Policy Statement: 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).

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.

VMware Capability

VMware NSX, additionally, provides APIs to allow VMware partners to develop software solutions to enhance security for the virtualized network. These security enhancements, which can be applied individually to virtual machines, include antivirus/anti-malware solutions, layer 4 - 7 next generation application firewalls, and intrusion detection/protection sensors. These seamlessly integrated solutions efficiently provide highly capable advanced protection techniques that make use of the portability and scalability inherent in virtualized and cloud solutions. This enables the same agility afforded the aforementioned virtual firewall to be extended to the advanced network protection measures.

Whereas NSX provides isolation capabilities at the network layer, VMware ESXi is designed to create secure isolation boundaries for virtual machines at the virtualization layer. Included in this secure isolation capability is secure instruction isolation, memory isolation, device isolation, and managed resource usage and network isolation. Each virtual machine is isolated from one another. While not specifically involved in guarding against malicious software attacks, the nature of the hypervisor's architecture reduces the surface area for attack and presents boundaries at critical areas to prevent impact to the hypervisor or the contained virtual machines.

These isolation techniques employed by vSphere for instructions, memory, I/O, resources, devices, and network are enhanced through extensions built into the hardware that are designed for x86 virtualization. The hypervisor uses these extensions to further improve security for the hosted virtual machines.

Extensions built into Intel Processors such as the Trusted Computing Group's Trusted Platform Module (TPM) or Intel Trusted Execution Technology (Intel TXT) managed by vSphere provide a trusted boot platform that verifies the physical hardware and hypervisor configuration during the boot sequence to ensure that the platform has not been compromised by malicious software or hardware tampering.

VMware vSphere uses address space layout randomization (ASLR) to randomize where core kernel modules are loaded into memory. The NX/XD CPU features enable the VMkernel to mark writeable areas of memory as non-executable. Both of these memory protection methods help protect the system from buffer overflow attacks in running code. Additional design consideration that were included in VMware vSphere allows for greater protection from denial of service attacks.

When vSphere hosts are managed by vCenter, vCenter provides the capability to enable lockdown mode to limit the access and functionality to the core of the virtualization infrastructure. Lockdown mode disables login and API functions from being executed directly on the ESXi server, forcing changes to be made through the vCenter interface, which also forces use of vSphere Single Sign-On. VMware vSphere CLI commands from an administration server or from a script cannot be run against the ESXi host in lockdown mode. All of the vSphere API privileges that are associated with root access have been disabled. The host access made available for vCenter to manage the host is provided with an obfuscated and protected vpxuser account. This enables and ensures tighter and more managed control of the ESXi hosts managed by vCenter.

Additionally, VMware NSX allows for service insertion of advanced security solutions from VMware's vast partner ecosystem. Among the services that can be included with NSX is antivirus, anti-malware, IDS/IPS, and Application Firewall. These technologies allow layering of additional measures to reduce the potential for infection, intrusion, or malicious activity. Moreover, as it is deployed within the infrastructure, it can help reduce the proliferation of attack within an environment.

For end-user devices and mobile devices that may be in use in a BYOD environment, AirWatch Enterprise Mobility Management provides tools for managing laptops, tablets, and smart phones to ensure that registered devices are properly protected. Among policies to which these devices must adhere are the inclusion of antivirus or anti-malware and endpoint or host-based firewalls. If these measures are not present on a registered device, AirWatch Mobile Device Management can deploy the covered entities' and business associates' chosen solution.

VMware vRealize Configuration Manager is capable of checking for the presence of required software such as antivirus, anti-malware, host-based intrusion detection/protection solutions, and reporting on non-compliant system. Software packages can be created for each required software and deployed automatically to non-compliant devices, ensuring that devices remain compliant and properly protected.

Additional Considerations

Additional design considerations should be made when deploying a virtualized environment to host or access CJI. Following VMware hardening guides and best practices is paramount to securing virtualized infrastructure. Out of the box deployment with default settings is typically not sufficient to ensure that the virtualization or cloud infrastructure has met satisfactory requirements for least privilege or least functionality. For example, the default host security profile for vSphere ESXi hosts for incoming and outgoing connections is all source and destination addresses for required TCP and UDP ports. For this reason, the organization should consider the configurable settings for inclusion or modification necessary to properly secure the infrastructure. The architecture and design considerations made available are useful in general for the protection of any critical information system or data. Examples of these considerations include, but are not limited to, physical separation of the hypervisor management network from that of the virtual machine or workload network and physical and VLAN separation of the vMotion network from the virtual machine network to prevent network snooping of virtual machine traffic.

The root account is necessary for the functions of ESXi. As a result, the root account cannot be removed and replaced with a differently named service account; however, the root account can adhere to password rules for complexity. It is strongly suggested that the root password for ESXi hosts and Linux Kernel-based virtual appliances be set using strong password complexity requirements. Moreover, it is advisable to change the root account password on a regular basis. VMware partner technologies provide solutions to help manage the root account and proxy access when the root account is needed for troubleshooting that ensures that logged changes are attributable to a named user. It is advisable for the ESXi hosts that are managed by vCenter to be placed in lockdown mode. Additional network segmentation with policy-based security should be applied to limit accessibility to the management interface of the ESXi host to only that which is necessary for regular operations. Where ESXi hosts are implemented as standalone hosts, it is advisable to vault the root account and setup local named user accounts for administrative activities.

Relevant NIST 800-53 Controls: MA-3(2), SI-3, SI-3(1), SI-3(2)

5.10.4.3 Spam and Spyware Protection

CJIS Policy Statement: The agency shall implement spam and spyware protection.

The agency shall:

1. Employ spam protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers).
2. Employ spyware protection at workstations, servers and mobile computing devices on the network.
3. Use the spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g. diskettes or compact disks), or other removable media as defined in this Policy.

VMware Capability

Similar to the previous policy, VMware partner solutions provide the means to ensure spyware and spam protection at various information system entry points.

Relevant NIST 800-53 Controls: SI-8, SI-8(1), SI-8(2)

Policy Area 13: Mobile Devices

5.13.1.2.1 Cellular Services Abroad

CJIS Policy Statement: When devices are authorized to access CJI outside the U.S., agencies shall perform an inspection to ensure that all controls are in place and functioning properly in accordance with the agency's policies prior to and after deployment outside of the U.S.

VMware Capability

VMware AirWatch Enterprise Mobility Manager (EMM) is capable of supporting inspection of devices to ensure that the device configuration adheres to the desired parameters. This includes software, patching, access settings, configuration parameters, and the presence of required security controls.

Additional Considerations

While AirWatch MDM can ensure adherence to agency policies with regard to device configurations, it may be necessary to perform a forensic analysis prior to and after travel to determine if there are any differences with the device that could indicate compromise occurred while the device was abroad. This additional inspection is performed by third party solutions or services.

Relevant NIST 800-53 Controls: AC-19, AC-19(5)

5.13.1.3 Bluetooth

CJIS Policy Statement: Bluetooth technology and associated devices are susceptible to general wireless networking threats (e.g. denial of service [DoS] attacks, eavesdropping, man-in-the-middle [MITM] attacks, message modification, and resource misappropriation), as well as specific Bluetooth-related attacks that target known vulnerabilities in Bluetooth implementations and specifications. Organizational security policy shall be used to dictate the use of Bluetooth and its associated devices based on the agency's operational and business processes.

VMware Capability

AirWatch MDM has the capability of disabling Bluetooth on a device prior to allowing the device to access organization applications and data. It is not capable of modifying or increasing the security of the Bluetooth protocols or communication. As a result, Bluetooth that is enabled on a device will continue to provide a measure of risk relative to inherent vulnerabilities.

Additional Considerations

The agency should measure the risk of compromise with the need for Bluetooth to perform agency-related tasks when determining the appropriate actions to take with regard to Bluetooth.

Relevant NIST 800-53 Controls: AC-18(5)

5.13.1.4 Mobile Hotspots

CJIS Policy Statement: Many mobile devices include the capability to function as a Wi-Fi hotspot that allows other devices to connect through the device to the Internet over the device's cellular network.

When an agency allows mobile devices that are approved to access or store CJI to function as a Wi-Fi hotspot connecting to the Internet, they shall be configured to:

1. Enable encryption on the hotspot
2. Change the hotspot's default SSID
    1. Ensure the hotspot SSID does not identify the device make/model or agency ownership
3. Create a wireless network password (pre-shared key)
4. Enable the hotspot's port filtering/blocking features if present
5. Only allow connections from agency controlled devices

Note: Refer to the requirements in Section 5.10.1.2 encryption for item #1. Refer to the requirements in Section 5.6.2.2.1 Password for item #3. Only password attributes #1, #2 and #3 are required.

OR

1. Have a MDM solution to provide the same security as identified in items 1 – 5 above.

VMware Capability

AirWatch Mobile Device Management can provide the security capabilities necessary to meet control requirements in alignment with this policy requirement.

Relevant NIST 800-53 Controls: AC-18, AC-18(1), AC-19, IA-5, IA-5(1), IA-5(4), SC-40, SI-4(14), SI-4(15)

5.13.2 Mobile Device Management

CJIS Policy Statement: Mobile Device Management (MDM) facilitates the implementation of sound security controls for mobile devices and allows for centralized oversight of configuration control, application usage, and device protection and recovery, if so desired by the agency.

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of full featured operating systems may not function properly on devices with limited feature operating systems. MDM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented.

Devices that have had any unauthorized changes made to them (including but not limited to being rooted or jailbroken) shall not be used to process, store, or transmit CJI data at any time. Agencies shall implement the following controls when allowing CJI access from devices running a limited feature operating system:

- Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.
- MDM with centralized administration configured and implemented to perform at least the:
    i. Remote locking of device
    ii. Remote wiping of device
    iii. Setting and locking device configuration
    iv. Detection of "rooted" and "jailbroken" devices
    v. Enforcement of folder or disk level encryption
    vi. Application of mandatory policy settings on the device
    vii. Detection of unauthorized configurations
    viii. Detection of unauthorized software or applications

ix. Ability to determine the location of agency controlled devices

x. Prevention of unpatched devices from accessing CJI or CJI systems

xi. Automatic device wiping after a specified number of failed access attempts

VMware Capability

AirWatch Mobile Device Management is capable of enabling controls necessary to achieve compliance for all the requirements in this policy statement. Additionally, the use of secure containers can ensure that CJI that is accessed from a mobile device is stored in a secure location and encrypted to meet necessary encryption standards supported by CJIS.

Relevant NIST 800-53 Controls: AC-19, AC-19(5)

5.13.3 Wireless Device Risk Mitigations

CJIS Policy Statement: Organizations shall, at a minimum, ensure that wireless devices:

1. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in Section 5.10.4.1.
2. Are configured for local device authentication (see Section 5.13.9.1).
3. Use advanced authentication or CSO approved compensating controls (as per Section 5.13.7.2.1).
4. Encrypt all CJI resident on the device.
5. Erase cached information, to include authenticators (see Section 5.6.2.1) in applications, when session is terminated.
6. Employ personal firewalls or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.
7. Employ malicious code protection or run a MDM system that facilitates the ability to provide anti-malware services from the agency level.

VMware Capability

VMware AirWatch MDM is also capable of providing the necessary controls to meet this requirement of CJIS Security Policy 5.13.3. AirWatch MDM verifies the patch level of the mobile device operating system to ensure that it is up to date. For some mobile device operating systems, AirWatch can ensure that the mobile update settings are enabled to automatically receive updates and can verify that the updates have been applied properly after updating.

For local authentication to the mobile device biometric, PIN or password can be enabled where the mobile device supports the authentication methods.

Relevant NIST 800-53 Controls: AC-19, AC-19(5)

5.13.4 System Integrity

5.13.4.1 Patching/Updates

CJIS Policy Statement: Based on the varying connection methods for mobile devices, an always-on connection cannot be guaranteed for patching and updating. Devices without always-on cellular connections may not be reachable for extended periods of time by the MDM or solution to either report status or initiate patching.

Agencies shall monitor mobile devices to ensure their patch and update state is current.

VMware Capability

AirWatch MDM is capable of monitoring mobile devices and reporting on the patching status of the mobile device. This allows the agency to assure that all mobile device resources are patched appropriately when accessing CJIS environments.

Additional Consideration

The agency may consider utilizing devices that have an always-on cellular connection. This is due to the nature of how devices are used in the field with respect to CJI. Additional consideration may be made as to the extent of CJI that may be allowed to be accessed offline, in the event that an extended outage occurs that could compromise an agent's ability to

access critical CJI in performance of duties.

Relevant NIST 800-53 Controls: CM-1, CM-2, CM-2(1), CM-2(3), CM-2(7), CM-3, CM-3(1), CM-3(2), CM-4, CM-4(1), RA-5, RA-5(1), RA-5(2), RA-5(3), SA-11, SA-11(1), SI-2, SI-2(2), SI-2(3)

5.13.4.2 Malicious Code Protection

CJIS Policy Statement: Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory to a central management console in a manner analogous to traditional virus scan detection of unauthorized software and can provide a high degree of confidence that only known software or applications are installed on the device.

Agencies that allow smartphones and tablets to access CJI shall have a process to approve the use of specific software or applications on the devices. Any device natively capable of performing these functions without a MDM solution is acceptable under this section.

VMware Capability

AirWatch MDM does not inherently include Antivirus or Antimalware protection; however, Airwatch MDM is capable of ensuring that the managed mobile device is running an approved antivirus or anti-malware solution. As part of this assurance, AirWatch MDM can enable distribution of an agency's antivirus or anti-malware solution to be installed on the mobile device.

Relevant NIST 800-53 Controls: MA-3(2), SI-3, SI-3(1), SI-3(2)

5.13.4.3 Personal Firewall

CJIS Policy Statement: For the purpose of this policy, a personal firewall is an application that controls network traffic to and from a user device, permitting or denying communications based on policy. A personal firewall shall be employed on all mobile devices that have a full-feature operating system (i.e. laptops or tablets with Windows or Linux/Unix operating systems). At a minimum, the personal firewall shall perform the following activities:

1. Manage program access to the Internet.
2. Block unsolicited requests to connect to the user device.
3. Filter incoming traffic by IP address or protocol.
4. Filter incoming traffic by destination ports.
5. Maintain an IP traffic log.

Mobile devices with limited feature operating systems (i.e. tablets, smartphones) may not support a personal firewall. However, these operating systems have a limited number of system services installed, carefully controlled network access, and, to a certain extent, perform functions similar to a personal firewall on a device with a full feature operating system. Appropriately configured MDM software is capable of controlling which applications are allowed on the device.

VMware Capability

Similar to antivirus and anti-malware solutions in the previous policy statement, AirWatch MDM does not inherently include firewall capabilities. AirWatch MDM is able to determine if an organization-approved firewall exists on the device. Similar to antivirus and anti-malware solutions, AirWatch MDM can be used to facilitate distribution of security solution to the mobile device. When this occurs, the state, status, and configuration of the mobile firewall solution would be managed by the agencies management facilities for said firewall solution.

Relevant NIST 800-53 Controls: SC-18, SC-18(1), SC-18(2), SC-18(3), SC-18(4)

5.13.5 Incident Response

CJIS Policy Statement: In addition to the requirements in Section 5.3 Incident Response, agencies shall develop additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface.

Special reporting procedures for mobile devices shall apply in any of the following situations:

1. Loss of device control. For example:
    a. Device known to be locked, minimal duration of loss
    b. Device lock state unknown, minimal duration of loss
    c. Device lock state unknown, extended duration of loss
    d. Device known to be unlocked, more than momentary duration of loss
2. Total loss of device
3. Device compromise
4. Device loss or compromise outside the United States

VMware Capability

Much of incident response in CJIS Security Policy focuses on awareness and notification when incidents occur. That being said, AirWatch MDM is able to provide status of mobile devices that may be lost, stolen, or otherwise compromised. Additional actions can be taken to further protect lost, stolen, or compromised mobile devices in an escalating fashion, including remote wiping.

Relevant NIST 800-53 Controls: IR-1, IR-2, IR-4, IR-8

5.13.7.1 Local Device Authentication

CJIS Policy Statement: When mobile devices are authorized for use in accessing CJI, local device authentication shall be used to unlock the device for use. The authenticator used shall meet the requirements in section 5.6.2.1 Standard Authenticators.

VMware Capability

VMware Workspace ONE with the integration of VMware Identity Manager and AirWatch Enterprise Mobility Management is capable of requiring local device authentication, using PIN, biometric, password, and two-factor authentication, for unlocking mobile devices with authenticator attributes in alignment with 5.6.2.1 Standard Authenticators.

Relevant NIST 800-53 Controls: IA-1, IA-2, IA-2(5)

5.13.7.2 Advanced Authentication

CJIS Policy Statement: When accessing CJI from an authorized mobile device, advanced authentication shall be used by the authorized user.

5.13.7.2.1 Compensating Controls

CJIS Policy Statement: CSO approved compensating controls to meet the AA requirement on agency-issued smartphones and tablets with limited feature operating systems are permitted. Compensating controls are temporary control measures that are implemented in lieu of the required AA control measures when an agency cannot meet a requirement due to legitimate technical or business constraints. Before CSOs consider approval of compensating controls, Mobile Device Management (MDM) shall be implemented per Section 5.13.2. The compensating controls shall:

1. Meet the intent of the CJIS Security Policy AA requirement
2. Provide a similar level of protection or security as the original AA requirement
3. Not rely upon the existing requirements for AA as compensating controls

Additionally, compensating controls may rely upon other, non-AA existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

The proposed compensating controls for AA are a combination of controls that provide acceptable assurance only the authorized user is authenticating and not an impersonator or (in the case of agency-issued device used by multiple users) controls that reduce the risk of exposure if information is accessed by an unauthorized party.

At least two of the following examples of AA compensating controls for agency-issued smartphones and tablets with limited feature operating systems shall be implemented to qualify for compensating control consideration:

- Possession of the agency-issued smartphone or tablet as an indication it is the authorized user
- Implemented password protection on the Mobile Device Management application and/or secure container where the authentication application is stored
- Enable remote device locking
- Enable remote data deletion
- Enable automatic data wipe after predetermined number of failed authentication attempts
- Remote device location (GPS) tracking
- Require CJIS Security Policy compliant password to access the device
- Use of device certificates as per Section 5.13.7.3 Device Certificates

VMware Capability

VMware Identity Manager along with AirWatch Enterprise Mobility Manager can manage the authentication process for users accessing CJI via mobile devices. Using conditional access criteria whereby one of the identified conditions is the mobile device operating system, the specified access in this case would require an additional factor for authentication.

While AirWatch Enterprise Mobility Manager supports the compensating controls criteria with respect to Advanced Authentication, VMware Workspace ONE should be capable of supporting Advanced Authentication for access to CJI from mobile devices.

Additional Considerations

The level of risk should be factored when determining the best course of action with regard to advanced authentication or the use of compensating controls.

Relevant NIST SP800-53 Controls: IA-2(1), IA-2(2), IA-2(3), IA-2(4), IA-2(11), IA-2(13), IA-3(1), IA-5(2), IA-5(11), MA-4, SC-37, SC-37(1), AC-19, IA-3, IA-3(4), PE-18, PE-18(1), PE-20

5.13.7.3 Device Certificates

CJIS Policy Statement: Device certificates are often used to uniquely identify mobile devices using part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI and may provide a critical layer of device identification or authentication in a larger scheme, a device certificate alone placed on the device shall not be considered valid proof that the device is being operated by an authorized user.

When certificates or cryptographic keys used to authenticate a mobile device are used in lieu of compensating controls for advanced authentication, they shall be:

1. Protected against being extracted from the device
2. Configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts
3. Configured to use a secure authenticator (i.e. password, PIN) to unlock the key for use

VMware Capability

AirWatch Enterprise Mobility Management mobile device management solution is capable of being configured to meet the requirements for compensating controls in lieu of advanced authentication as it pertains to using device certificates for device authentication. This includes protection of the keys on the device from being extracted. The ability to remote wipe a device or force a device wipe is based on a configurable number of unsuccessful login attempts. Finally, AirWatch MDM is capable of enforcing the use of a password or PIN on the device to unlock the key for use.

Relevant NIST SP800-53 Controls: AC-19, IA-3, IA-3(4)

Summary

There is no doubt that the transformation of business to the digital world presents exciting opportunities for industries around the world. This includes the capability of sharing information across multiple states and coordination with multiple law enforcement agencies including federal law enforcement. New businesses have emerged in recent years that have shifted the paradigm for how things are traditionally done. Among these transformations is the concept introduced by VMware of "One Cloud, Any Application, Any Device" architecture that can be used to meet a host of CJIS requirements. Some requirements can be met immediately upon implementation; others may require integration to fully meet the requirements. This architecture presents unique opportunities for improvements in how people interact with information. Improvements in speed and the availability of information can assist people in criminal justice with making informed decisions. Other available solutions include helping law enforcement agencies with identification, investigation, evidence collection, and forensic analysis in the field. This flexibility also presents the possibility for greater risk. It is not uncommon for security to follow in the footsteps of a brave new frontier as the awareness for the need of security paces behind the benefit for the new technology. Even with the benefits from accelerated innovation and mobile cloud applications, security of electronic protected health information is still of utmost concern. This product applicability guide identified ways in which VMware's software-defined data center and end-user computing platforms help to meet CJIS Policy requirements, govern risk, and support a responsible participation in ongoing innovation.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Bibliography

CJIS Information Security Officer. (2016, June 1). *Criminal Justice Information Services (CJIS) Security Policy Version 5.5.* (C. P. Board, Ed.) Retrieved from www.fbi.gov: https://www.fbi.gov/file-repository/cjis-security-policy-v5_5_20160601-2-1.pdf

Division, C. J. (2013). *2013 CJIS Annual Report.*

Appendix A: What is Cloud

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

http://www.vmware.com/files/pdf/VMware-Public-Cloud-Service-Definition.pdf

http://www.vmware.com/files/pdf/vcat/Private-VMware-vCloud-Service-Definition.pdf

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Appendix B: NIST Alignment

CJIS v5.5 to NIST

CSP v5.5 Area	Requirement Topic	NISTSP800-53 Alignment
5.1	**Policy Area 1: Information Exchange Agreements**	
5.1.1	Information Exchange	AC-21, CA-3, SA-2, SA-4, SA-4(1), SA-12(2)
5.1.1.1	Information Handling	AC-21, CM-9, CP-6, CP-7, IR-8, PL-2, PM-1
5.1.1.2	State and Federal Agency User Agreements	AC-21, CA-3, SA-2, SA-4, SA-4(1), SA-12(2)
5.1.1.3	Criminal Justice Agency User Agreements	AC-21, CA-3, SA-2, SA-4, SA-4(1), SA-12(2)
5.1.1.4	Inter-Agency and Management Control Agreements	AC-21, CA-3, SA-2, SA-4, SA-4(1), SA-12(2)
5.1.1.5	Private Contractor User Agreements and CJIS Security Addendum	AC-21, CA-3, SA-2, SA-4, SA-4(1), SA-12(2)
5.1.1.6	Agency User Agreements	AC-21, CA-3, SA-2, SA-4, SA-4(1), SA-12(2)
5.1.1.7	Outsourcing Standards for Channelers	PE-3, PS-1, PS-2, PS-3, PS-6, PS-7
5.1.1.8	Outsourcing Standards for Non-Channelers	AC-21, CA-3, SA-2, SA-4, SA-4(1), SA-12(2)
5.1.2	Monitoring, Review, and Delivery of Services	RA-3, SA-9, SA-9(1)
5.1.2.1	Managing Changes to Service Providers	RA-3
5.1.3	Secondary Dissemination	PS-3, PS-6, PS-7
5.1.4	Secondary Dissemination of Non-CHRI CJI	PS-3, PS-6, PS-7
5.2	**Policy Area 2: Security Awareness Training**	
5.2.1	Awareness Topics	AT-1, PL-4, PL-4(1)
5.2.1.1	Level One Security Awareness Training	AT-2, AT-3
5.2.1.2	Level Two Security Awareness Training	AT-2(2), AT-3, PL-4, PL-4(1)
5.2.1.3	Level Three Security Awareness Training	AT-2(2), AT-3, PL-4, PL-4(1)
5.2.1.4	Level Four Security Awareness Training	AT-3, CM-10
5.2.2	Security Training Records	AT-4, PL-4
5.3	**Policy Area 3: Incident Response**	
5.3.1	Reporting Information Security Events	IR-4(1), IR-6, IR-6(1), IR-6(2), IR-7, IR-7(1), IR-7(2), IR-8, PE-17
5.3.1.1.1	FBI CJIS Division Responsibilities	N/A
5.3.1.1.2	CSA ISO Responsibilities	N/A
5.3.2	Management of Security Incidents	IR-1, IR-8
5.3.2.1	Incident Handling	IR-4, IR-4(1), IR-4(3), IR-4(4), IR-8
5.3.2.2	Collection of Evidence	IR-4, IR-4(1), IR-4(3), IR-4(4), IR-8
5.3.3	Incident Response Training	IR-2, IR-3
5.3.4	Incident Monitoring	IR-5
5.4	**Policy Area 4: Auditing and Accountability**	
5.4.1	Auditable Events and Content (Information Systems)	AC-9, AU-2, AU-2(3), AU-3, AU-3(1), AU-6, AU-6(1), AU-6(3), AU-12, CA-7
5.4.1.1	Events	AC-9, AU-2, AU-12, CA-7
5.4.1.1.1	Content	AU-12
5.4.2	Response to Audit Processing Failures	AU-5, AU-5(2)
5.4.3	Audit Monitoring, Analysis, and Reporting	AU-6, AU-6(1), AU-6(3), AU-7, CA-7
5.4.4	Time Stamps	AU-8, AU-8(1)
5.4.5	Protection of Audit Information	AU-9, AU-9(4)

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

5.4.6	Audit Record Retention	AU-4, AU-5(1), AU-9(2), AU-11
5.4.7	Logging NCIC and III Transactions	AU-4, AU-11
5.5	**Policy Area 5: Access Control**	
5.5.1	Account Management	AC-2, AC-5, IR8
5.5.2	Access Enforcement	AC-2, AC-2(1), AC-2(7), AC-3, AC-3(3), AC-3(4), AC-5, AC-6(1), AC-6(2), AC-12(1), SC-23(1), SC-23(3)
5.5.2.1	Least Privilege	AC-2, AC-2(4), AC-2(7), AC-5, AC-6, AC-6(5), AC-6(9), AC-10, RA-5(5)
5.5.2.2	System Access Control	AC-2, AC-2(4), AC-2(7), AC-5, AC-6, AC-6(5), AC-6(9), AC-10, RA-5(5)
5.5.2.3	Access Control Criteria	AC-2, AC-2(4), AC-2(7), AC-5, AC-6, AC-6(5), AC-6(9), AC-10, RA-5(5)
5.5.2.4	Access Control Mechanisms	AC-2, AC-2(4), AC-2(7), AC-5, AC-6, AC-6(5), AC-6(9), AC-10, RA-5(5)
5.5.3	Unsuccessful Login Attempts	AC-7, IA-5(1)
5.5.4	System Use Notification	AC-8, AC-11(1), AC-22
5.5.5	Session Lock	AC-11
5.5.6	Remote Access	AC-17, AC-17(3), AC-17(4), AC-17(6)
5.5.6.1	Personally Owned Information Systems	AC-17
5.5.6.2	Publicly Accessible Computers	AC-17, AC-22
5.6	**Policy Area 6: Identification and Authentication**	
5.6.1	Identification Policy and Procedures	IA-1, IA-2, IA-2(5)
5.6.1.1	Use of Originating Agency Identifiers in Transactions and Information Exchanges	SC-16
5.6.2	Authentication Policy and Procedures	IA-1, IA-2, IA-2(8), IA-2(9), IA-3
5.6.2.1	Standard Authenticators	IA-5, IA-5(1), IA-5(5), IA-6
5.6.2.1.1	Password	IA-5, IA-5(1), IA-5(4)
5.6.2.1.2	Personal Identification Number (PIN)	IA-5, IA-5(1), IA-5(4)
5.6.2.2	Advanced Authentication	IA-2(1), IA-2(2), IA-2(3), IA-2(4), IA-2(11), IA-2(13), IA-3(1), IA-5(2), IA-5(11), MA-4, SC-37, SC-37(1)
5.6.2.2.1	Advanced Authentication Policy and Rationale	IA-2(1), IA-2(2), IA-2(3), IA-2(4), IA-2(11), IA-3(1), IA-5(2), IA-5(11), MA-4
5.6.2.2.2	Advanced Authentication Decision Tree	IA-2(1), IA-2(2), IA-2(3), IA-2(4), IA-2(11), IA-3(1), IA-5(2), IA-5(11), MA-4
5.6.3	Identifier and Authenticator Management	IA-4, IA-4(2), IA-4(4), IA-5, IA-5(8), IA-8
5.6.3.1	Identifier Management	AC-2(3), IA-4, IA-4(2), IA-4(4), IA-5(3), IA-5(8), IA-8
5.6.3.2	Authenticator Management	IA-5, IA-5(6), IA-5(8)
5.6.4	Assertions	IA-2(12), IA-8(1), IA-8(2), IA-8(3)
5.7	**Policy Area 7: Configuration Management**	
5.7.1	Access Restrictions for Changes	CM-3, CM-3(2), CM-4, CM-4(2), CM-5(5), CM-5(6), CM-6, CM-9, MA-2, MA-5, SA-10
5.7.1.1	Least Functionality	CM-2, CM-3, CM-6, CM-7, CM-7(1), CM-7(2), CM-7(3), CM-7(4), CM-7(5), CM-8(3), CM-10, CM-11, SA-4(9), SA-9(2)
5.7.1.2	Network Diagram	CA-3, CA-9, SC-7(4)
5.7.2	Security of Configuration Documentation	CM-2, CM-5, CM-5(1), CM-5(2), CM-8, CM-8(1), CM-9, SA-5
5.8	**Policy Area 8: Media Protection**	
5.8.1	Media Storage and Access	AC-20(2), CP-6, CP-7, MA-3(3), MP-2, MP-3, MP-4
5.8.2	Media Transport	MP-5
5.8.2.1	Digital Media in Transit	MP-5, MP-5(4)

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

5.8.2.2	Physical Media in Transit	MP-5
5.8.3	Digital Media Sanitization and Disposal	MA-2, MP-6, MP-6(1), MP-6(2), MP-6(3)
5.8.4	Disposal of Physical Media	MP-6
5.9	**Policy Area 9: Physical Protection**	
5.9.1	Physically Secure Location	PE-1
5.9.1.1	Security Perimeter	PE-1
5.9.1.2	Physical Access Authorizations	MA-4(7), MA-5, PE-2, PE-2(1)
5.9.1.3	Physical Access Control	PE-3, PE-3(3)
5.9.1.4	Access Control for Transmission Medium	PE-4
5.9.1.5	Access Control for Display Medium	PE-5
5.9.1.6	Monitoring Physical Access	PE-3, PE-5, PE-6, PE-6(1)
5.9.1.7	Visitor Control	PE-2(3), PE-3
5.9.1.8	Delivery and Removal	PE-8
5.9.2	Controlled Area	PE-2, PE-5
5.1	**Policy Area 10: System and Communications Protection and Information Integrity**	
5.10.1	Information Flow Enforcement	AC-4, AC-20, AC-20(1), CA-3, CA-9, IA-5(7), SC-7(4), SC-7(8), SC-7(11), SC-10, SC-15, SC-15(1)
5.10.1.1	Boundary Protection	AC-20, CA-3(1), CA-3(2), CA-3(5), PE-3(2), SC-5, SC-5(1), SC-5(2), SC-7, SC-7(3), SC-7(4), SC-7(5), SC-7(7), SC-7(8), SC-7(11), SC-7(12), SC-7(13), SC-7(14), SC-7(18), SC-24
5.10.1.2	Encryption	AC-17(2), IA-7, MA-4(6), SC-8, SC-8(1), SC-8(2), SC-11, SC-12, SC-12(1), SC-12(2), SC-12(3), SC-13, SC-17, SC-28, SC-28(1), SI-7(6)
5.10.1.3	Intrusion Detection Tools and Techniques	SC-7(19), SI-4, SI-4(1), SI-4(2), SI-4(4), SI-4(5), SI-4(7), SI- 4(9), SI-4(11), SI-4(12), SI-7, SI-7(1), SI-7(7)
5.10.1.4	Voice over Internet Protocol	SC-19
5.10.1.5	Cloud Computing	AC-17,AC-17(1),AC-17(2),AC-17(3),AC-17(4),AC-23,CP-1,CP-2(1),CP-2(3),CP-2(8),CP-6(1),CP-6(3),CP-7,CP-9,CP-10,CP-10(2),IA-1,IA-2,IR-1,IR-6,IR-8,IR-9,MA-1,MA-5,MA-5(4),MP-1,MP-2,MP-4,MP-5,MP-6,MP-7,MP-7(1),PE-1,PE-2,PE-3,PE-18,PL-1,PL-2,PL-2(3),PL-4,PL-4(1),PL-7,PL-8,PL-9,PS-1,PS-3,PS-7,SC-2,SC-2(1),SC-3,SC-4,SC-5,SC-5(1),SC-5(2),SC-5(3),SC-6,SC-7,SC-8,SC-9,SC-12,SC-13,SC-13(1),SC-16,SC-16(1),SC-20,SC-21,SC-22,SC-23,SC-28,SC-28(1),SC-28(2),SC-32,SC-36,SC-38,SC-43,SI-1
5.10.2	Facsimile Transmission of CJI	N/A
5.10.3	Partitioning and Virtualization	SC-2, SC-4
5.10.3.1	Partitioning	SC-2, SC-2(1), SC-3, SC-4, SC-32
5.10.3.2	Virtualization	SC-2, SC-4
5.10.4	System and Information Integrity Policy and Procedures	N/A
5.10.4.1	Patch Management	CM-3, CM-4, CM-4(1), RA-5, RA-5(1), RA-5(2), RA-5(3), SA-11, SA-11(1), SI-2, SI-2(2), SI-2(3)
5.10.4.2	Malicious Code Protection	MA-3(2), SI-3, SI-3(1), SI-3(2)
5.10.4.3	Spam and Spyware Protection	SI-8, SI-8(1), SI-8(2)
5.10.4.4	Security Alerts and Advisories	SI-5, SI-5(1), SI-11
5.10.4.5	Information Input Restrictions	SI-10, SI-12
5.11	**Policy Area 11: Formal Audits**	
5.11.1	Audits by the FBI CJIS Division	N/A
5.11.1.1	Triennial Compliance Audits by the FBI CJIS Division	CA-2, CA-7

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

5.11.1.2	Triennial Security Audits by the FBI CJIS Division	CA-2
5.11.2	Audits by the CSA	CA-2
5.11.3	Special Security Inquiries and Audits	CA-2(1), CA-3, CA-5, CA-6, CA-7(1), CM-3(4)
5.12	**Policy Area 12: Personnel Security**	
5.12.1	Personnel Security Policy and Procedures	N/A
5.12.1.1	Minimum Screening Requirements for Individuals Requiring Access to CJI	PS-2, PS-3, PS-3(1), PS-3(2), PS-3(3), PS-6, PS-6(2), PS-7
5.12.1.2	Personnel Screening for Contractors and Vendors	PS-2, PS-3, PS-7
5.12.2	Personnel Termination	PS-4
5.12.3	Personnel Transfer	PS-5
5.12.4	Personnel Sanctions	PS-8
5.13	**Policy Area 13: Mobile Devices**	
5.13.1	Wireless Communications Technologies	AC-18, SI-4(14), SI-4(15)
5.13.1.1	802.11 Wireless Protocols	AC-18(5), SI-4(15)
5.13.1.2	Cellular Devices	AC-19, AC-19(5)
5.13.1.2.1	Cellular Service Abroad	AC-19, AC-19(5)
5.13.1.2.2	Voice Transmissions Over Cellular Devices	AC-19, AC-19(5)
5.13.1.3	Bluetooth	AC-18(5)
5.13.1.4	Mobile Hotspots	AC-18, AC-18(1), AC-19, IA-5, IA-5(1), IA-5(4), SC-40, SI-4(14), SI-4(15)
5.13.2	Mobile Device Management (MDM)	AC-19, AC-19(5)
5.13.3	Wireless Device Risk Management	AC-19, AC-19(5)
5.13.4	System Integrity	CM-1, CM-2, CM-2(1), CM-2(3), CM-2(7), CM-3, CM-3(1), CM-3(2)
5.13.4.1	Patching/Updates	CM-3, CM-4, CM-4(1), RA-5, RA-5(1), RA-5(2), RA-5(3), SA-11, SA-11(1), SI-2, SI-2(2), SI-2(3)
5.13.4.2	Malicious Code Protection	MA-3(2), SI-3, SI-3(1), SI-3(2)
5.13.4.3	Personal Firewall	SC-18, SC-18(1), SC-18(2), SC-18(3), SC-18(4)
5.13.5	Incident Response	IR-1, IR-2, IR-4, IR-8
5.13.6	Access Control	AC-5, AC-6, AC-6(5), AC-6(9), AC-19, AC-19(5)
5.13.7	Identification and Authentication	IA-1, IA-2, IA-2(1), IA-2(2), IA-2(3), IA-2(4), IA-2(8), IA-2(9), IA-2(11), IA-3, IA-5(2), IA-5(11), MA-4, SC-37, SC-37(1)
5.13.7.1	Local Device Authentication	IA-1, IA-2, IA-2(5)
5.13.7.2	Advanced Authentication	IA-2(1), IA-2(2), IA-2(3), IA-2(4), IA-2(11), IA-2(13), IA-3(1), IA-5(2), IA-5(11), MA-4, SC-37, SC-37(1
5.13.7.2.1	Compensating Controls	AC-19, IA-3, IA-3(4), PE-18, PE-18(1), PE-20
5.13.7.3	Device Certificates	AC-19, IA-3, IA-3(4)

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Acknowledgements

VMware would like to recognize the efforts of the VMware Center for Policy & Compliance, VMware Partner Alliance, and the numerous VMware teams that contributed to this paper and to the establishment of the VMware Compliance Program. VMware would also like to recognize the Coalfire Systems Inc. VMware Team www.coalfire.com/Partners/VMware for their industry guidance. Coalfire®, a leading security and compliance advisory and audit firm, provided the guidance and control interpretation described herein.

The information provided by Coalfire Systems and contained in this document is for educational and informational purposes only. Coalfire Systems makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained herein.

About Coalfire

Coalfire (Coalfire Systems, Inc.) is the trusted leader in cybersecurity risk management and compliance services. Coalfire integrates advisory and technical assessments and recommendations to the corporate directors, executives, boards, and IT organizations for global brands and organizations in the technology, cloud, healthcare, retail, payments, and financial industries.

Coalfire's approach addresses each businesses' specific vulnerability challenges, developing a long-term strategy to prevent security breaches and data theft. With offices throughout the United State and Europe, Coalfire was recently named one of the top 20 Most Promising Risk Management Solution Providers. **www.coalfire.com**

Disclaimer

* VMware solutions are designed to help organizations address various regulatory compliance requirements. This document is intended to provide general guidance for organizations that are considering VMware solutions to help them address such requirements. VMware encourages any organization that is considering VMware solutions to engage appropriate legal, business, technical, and audit expertise within their specific organization for review of regulatory compliance requirements. It is the responsibility of each organization to determine what is required to meet any and all requirements. The information contained in this document is for educational and informational purposes only. This document is not intended to provide legal advice and is provided "AS IS". VMware makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained herein. Nothing that you read in this document should be used as a substitute for the advice of an actual Cyber Security auditor or competent legal counsel.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com