VMware® Product Applicability Guide for North American Electric Reliability Corporation: Critical Infrastructure Protection, Version 5 (NERC CIP v5)

Published February 2016
Updated October 2016

TECHNICAL WHITE PAPER

vmware®

Table of Contents

Executive Summary 5
Background 5
VMware SDDC Products and NERC CIP v5 5
Introduction 6
Scope and Approach 9
NERC CIP v5 Scope 9
VMware SDDC Solution Scope 9
Our Approach 13
VMware and NERC CIP v5 Requirements (Overview) 15
VMware Control Capabilities Detail (Per NERC CIP v5 Standard) 21
Summary 26
Appendix A (North American Electric Reliability Corporation Critical Infrastructure Protection, Version 5 (NERC CIP v5) Requirements) 27
Appendix B (What is Cloud) 27
Glossary of Terms 27
Bibliography 28
Acknowledgements 29
About Coalfire 29

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
December 2015	0.0	Chris Krueger	Initially Created	Internal SME, Coalfire
February 2016	0.1.2	Chris Krueger	SME Draft Candidate	Internal Coalfire; VMware SME and Compliance
April 2016	0.5	Chris Krueger	Legal/Branding	Legal
May 2016	1.0	Chris Krueger	Final	

Design Subject Matter Experts

The following people provided key input into this design.

NAME	EMAIL ADDRESS	ROLE/Comments
Jason Macallister	jason.macallister@coalfire.com	Review, Senior Consultant – Cloud and Virtualization
Bao Le	bao.le@coalfire.com	Practice Lead – NERC and Federal Practices
Chris Krueger	chris.krueger@coalfire.com	Principal Author, revision QA to Customer DRAFT Release
Anthony Dukes	adukes@vmware.com	VMware Solutions Architect, Compliance and Cyber Risk Solutions
Chris Davis	chrisdavis@vmware.com	VMware Sr. Manager, Compliance and Cyber Risk Solutions

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

Trademarks

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 vCloud Suite®
Software-Defined Networking	VMware NSX®, VMware NSX Edge™, NSX Firewall, NSX Router, NSX Load Balancer, NSX Service Composer
Management and Automation	VMware vRealize® Operations™, 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 vRealize® Operations for Horizon®, VMware vRealize® Operations for Published Applications™, VMware vRealize® Operations Manager™ for Horizon®, VMware vRealize Automation™, VMware vRealize Business™
Disaster Recovery Automation	VMware vCenter™ Site Recovery Manager™

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

Executive Summary

Background

VMware recognizes that security and compliance are critical areas that must be addressed by each covered entity in the operation of Bulk Electric Systems (BES) production, monitoring and distribution infrastructure, the criticality and vulnerability of the assets needed to manage BES impacting infrastructures, and the risks to which they 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 to the cloud in a secure and compliant manner. This is especially important when the consequences of noncompliance can be extremely critical due to the penalties imposed by the Federal Energy Regulating Commission (FERC) and accompanying Canadian governmental regulating agencies; not to mention, there is a high probability for collateral impact due to failure to protect the North American Power "grid" privacy, institutional trust and economics. FERC has mandated a single point of contact entity, specifically the North American Electric Reliability Corporation (NERC) as the international regulatory authority to monitor, educate, train, and certify organization participating in the "grid." This single entity has additional responsibility to evolve and manage the Reliability Risk program by standards development and oversight – including investigation of operational status, impact of outage and events, and the capacity to levy fines on "grid" participants for outages, breaches of the FERC approved standards and other compliance-related events. Further, the aim of the NERC Risk Management program is to avoid or prevent additional impacts from litigation, recompense and/or negative public relations.

For these reasons, VMware enlisted its audit partner, Coalfire Systems, to engage in a programmatic approach to evaluate VMware products and solutions for North American Electric Reliability Corporation Critical Infrastructure Protection, Version 5 (NERC CIP v5, or more simply CIP) (NERC, 2016) cybersecurity standards capabilities and document these capabilities into a set of reference architecture documents. This document presents Coalfire's assessment of different VMware applications available to organizations that use (or are considering using) software-defined data center (SDDC) environments to host or access NERC CIP critical cyber assets. Specifically, this document focuses on the VMware SDDC solutions available, and points out where additional, non-VMware vendor solutions may be required. The SDDC is defined as an architecture which brings together best-in-class compute, storage, networking virtualization and management offerings. Coalfire highlights the specific NERC CIP Version 5 standards that these applications address and/or support. These applications can be considered in evaluation of the initial sourcing or a systems refresh of technologies to build a NERC CIP v5 compliant environment.

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 North American Electric Reliability Corporation Critical Infrastructure Protection, Version 5 (NERC CIP v5). It has been reviewed and authored by our staff of North American Electric Reliability Corporation Critical Infrastructure Protection auditors in conjunction with VMware.

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

VMware SDDC Products and NERC CIP v5

It is Coalfire's opinion that the VMware software-defined data center (SDDC) products, when deployed in a holistic manner, paying particular attention to the details adherent to published best practices for securing the VMware hypervisor, network and control infrastructures, may safely be used to comply with the standards outlined in NERC CIP v5, and more specifically the mandated FERC rules subject to enforcement. Although the VMware SDDC does not provide the entire suite of required technologies to ensure compliance, it may be used in conjunction with third party (non-VMware) products, entity policies and procedures to achieve a compliance capable infrastructure.

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

Introduction

Most organizations begin the compliance process by mapping the mandated requirements to their specific organizational need and capability. This is usually a difficult task that can require significant amounts of time and resource. To streamline the process, VMware has developed and 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 whitepapers that make up the reference architecture framework, maps North American Electric Reliability Corporation Critical Infrastructure Protection, Version 5 (NERC CIP v5) to VMware's SDDC technology stack.

Organizations can significantly reduce the complexity and cost of NERC CIP 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 Compliance and Cyber Risk Solutions provide the solution reference architecture, NERC CIP specific guidance, and software solutions that businesses require to be able to achieve continuous compliance. VMware reference architecture framework combined with VMware hyper-converged solutions based on Intel architecture, enables IT to continually transform their data centers by speeding up Software Defined Infrastructures (SDI) and hybrid cloud deployments, enabling IT to advance innovation, optimizing system services in real-time, mobilizing workforce and customer interactions. These solutions improve security and control via secure compliance capable/audit ready solutions, lower equipment and operational costs, and 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 measures of capability with respect to security, confidentiality, and integrity that make up a trusted cloud implementation. The graphic illustrates the specific categories that can be addressed with VMware solutions and our extensive partner ecosystem.

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

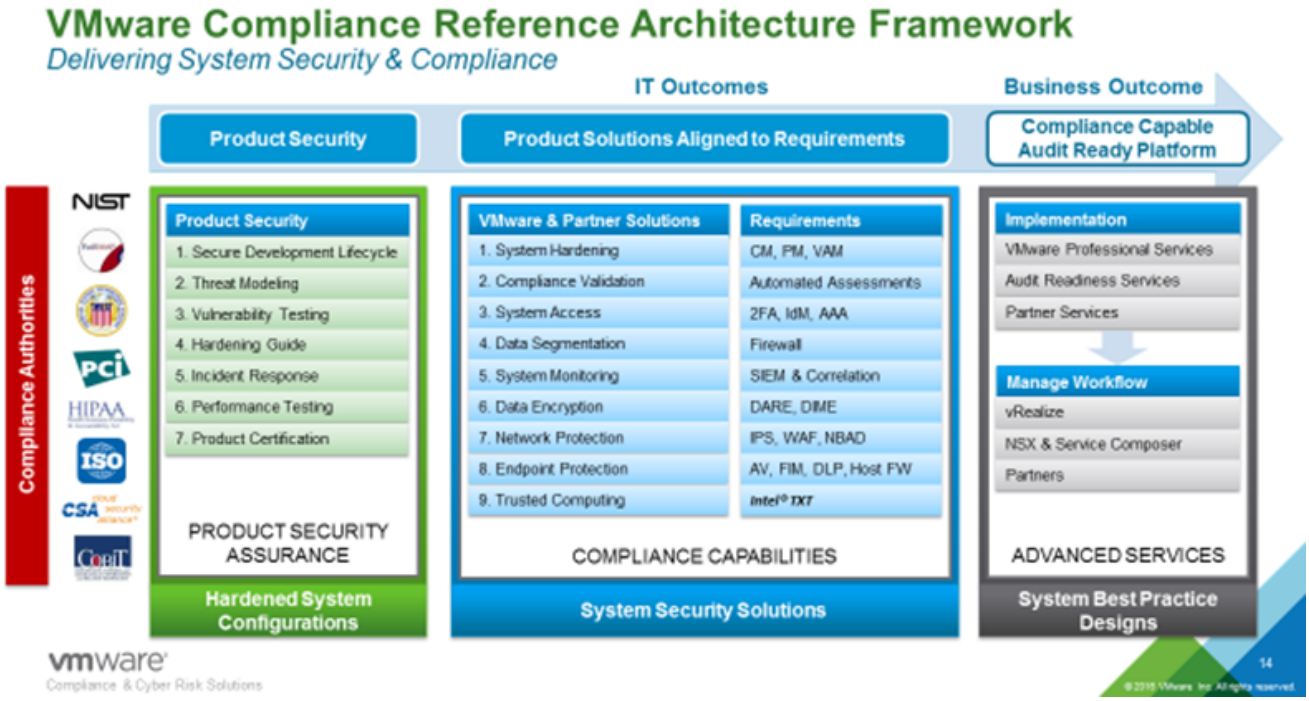
Compliance Solutions Crosswalk - Common **Required** Technical Security Solutions

The purpose of this worksheet is to list _required_ solutions that are part of a comprehensive security program.

	Common Required Technical Security Solutions		ISO	PCI	HIPAA	SANS	CSA	FISMA LOW	FISMA MOD	FISMA HIGH	FedRAMP LOW	FedRAMP MOD	CJIS	PCI	NIST SP800-53A†	CJIS	HIPAA	Product Examp	Assumptions	On/Off Block††	TMT Project: Product	Scope?	On/Off Block	Notes
	System Hardening & Compliance Validation	CM, PM, VAM, PT																						
1	**Configuration Management**	*Protect infrastructure*	●	●	●	●	●	●	●	●	●	●	●	*2.1, 2.2*	*SI-2, SA-10, CM-1/2/6*	*5.7*				*Either/Both*	*Vision*	*Yes*	*On*	*Compliance Module*
2	**Patch Management**	*Protect infrastructure*	●	●	●	●	●	●	●	●	●	●	●	*6.1*	*CM-2, SI-2*	*5.10.4.1*				*Either/Both*	*Vision*	*Yes*	*On*	*RCM; etc*
3	**Vulnerability Assessment and Management**	*Identify and track vulnerabilities*	●	●	●	●	●	●	●	●	●	●	△	*6.2, 6.5, 6.6, 11.2*	*RA-5*	*5.1.1.2, 5.1.1.6*				*Either*	*Qualys; Intel Se*	*TBD*	*Both*	*Maybe we do, maybe not*
4	**Penetration Testing**	*Validate vulnerabilities*	●	●	●	●	●	●	●	●	●	●	△	*11.3*	*CA-2*	*5.1.1.2, 5.1.1.6*				*Either*	*Nope....*			
	System Access	2FA, IdM, IAM																						
5	**Two Factor Authentication**	*Authenticate users*	●	●	●	●	●	●	●	●	●	●	△	*8.3*	*IA-2 (1), IA-4*	*5.6.2.2*				*On*	*RSA*	*Yes*	*On*	*Administrative vs. Tenant Control; Possibly refer to SAA paper; ***MUST*** address multitenancy*
6	**Identity Management**	*Provision and deprovision users*	●	●	●	●	●	●	●	●	●	●	●	*8.1, 8.2, 8.5.1*	*IA-2, IA-4*	*5.5, 5.6*				*Either/Both*	*HyTrust; RSA Ai*	*Yes*	*Both*	*Administrative vs. Tenant Control; Possibly refer to SAA paper; ***MUST*** address multitenancy*
7	**Access Management**	*Identity interaction nonrepudiation*	●	●	●	●	●	●	●	●	●	●	●	*7, 8.5*	*IA-5, AC-3*	*5.4, 5.5, 5.6*				*On*	*HyTrust; RSA Ai*	*Yes*	*Both*	*Administrative vs. Tenant Control; Possibly refer to SAA paper; ***MUST*** address multitenancy*
	Data Segmentation	FW																						
8	**Network & Host Firewall**	*Segment and protect networks*	●	●	●	●	●	●	●	●	●	●	●	*1*	*SC-7*	*5.10.1.1, 5.10.3.2, 5.10.4.4*				*Either/Both*	*Cisco*	*Yes*	*Both*	*Cisco VSG; ASA, etc...*
	System Monitoring	SIEM, DBM																						
9	**Security Information Event Monitoring**	*Log and correlate environment data*	●	●	●	●	●	●	●	●	●	●	●	*10, A.1.3*	*SI-4, AU-2/3/6/10/12*	*5.4*				*Both*	*TBD*	*TBD*	*Both*	*RSA; Intel Security*
10	**Database Monitoring**	*Protect database environment*	△	△	△	△	△	△	△	△	△	△	△	*10, A.1.3*	*SI-4*	*5.4.1*				*Either*				
	Data Encryption & Protection	DARE, DIME, BD																						
11	**Data At Rest Encryption**	*Protect data*	●	●	●	●	●	●	●	●	●	●	△	*3.4, 3.5, 3.6*	*SC-12/13/28, IA-7*	*5.5.2.4, 5.10.1.2*				*On*	*EMC*	*TBD*	*On*	*Possibly just discuss in the paper... reference other notes, docs, etc*
12	Data In Motion Encryption	*Protect data*	●	●	●	●	●	●	●	●	●	●	△	*2.3, 4, 8.4*	*SC-9/12/13, IA-7*	*5.10.1.2*				*On*				
13	**System Backup & Restore**	*Systems survivability*	●	●	●	●	●	●	●	●	●	●	●	*12.9.1*	*CP-9*	*5.2.1.3*				*Both*	*EMC*	*TBD*	*Both*	*Avamar, Data Domain, VPLEX - Mike Barcelo discussions*
	Network Protection	IPS, WAF																						
14	**Intrusion Prevention System ‡**	*Identify attacks*	●	●	●	●	●	○	●	○	●	●		*11.4*	*SI-3, SI-4*	*5.10.1.3, 5.10.3.2*				*Either*	*Cisco*	*TBD*	*Both*	*SourceFire*
15	**Web Application Firewall***	*Protect user services*	△	△	△	△	△	△	△	△	△	△		*6.6*	*SI-3, SI-4, SC-7*	*5.10.4.3(3)*				*Either/Both*	*Intel Security*	*No*	*Off*	*Workspace VMs out of scope*
	Endpoint Protection	AV, FIM, DLP																						
16	**Endpoint Antivirus & Malware Prevention**	*Protect against malware*	●	●	●	●	●	●	●	●	●	●		*5*	*SI-3*	*5.10.4.3*				*On*	*Intel Security*	*No*	*On*	*Workspace VMs out of scope*
17	**File Integrity Monitoring**	*Identify changed files*	●	●	●	●	●	○	●	○	●	●		*11.5*	*SI-7*					*On*	*Intel Security*	*No*	*On*	*Workspace VMs out of scope*
18	**Data Leakage Protection****	*Identify sensitive data*	○	△	△	○	○	○	△	○	△	△			*AC-4*					*Either/Both*	*RSA*	*No*	*On*	
	Trusted Computing	–																						
19	**Trusted Execution**	*Intel® TXT*	△	△	△	△	△	△	△	△	△	△									*Trapezoid*	*Yes*	*On*	
	Additional Technologies	–																						
21	**Spam Protection**	*Protect against malware*											●			*5.10.4.3*								
22	**Denial of Service Protection**	*Protect against DoS attacks*																						

* Specifically discussed in some; implied control in others. Highly recommended if Internet is primary use case.
** Not _specifically_ called out in any authority. However, often used as a control for healthcare and financial verticals.
† Sampling of controls that apply. May be others that reference the solution as well.
†† Yes. Requires additional discussion.
‡ Compliance requirements *typically* specifically call out network IPS

● Specifically discussed
○ Not specifically discussed
△ Possibly required (use case, risk)



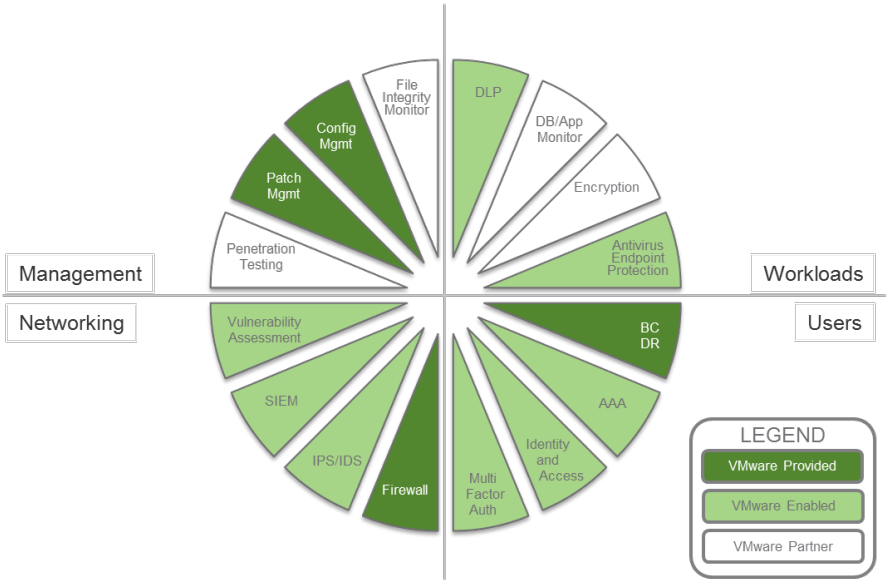


Figure 1: VMware + Partner Product Capabilities for a Trusted Cloud

Scope and Approach

As the not-for-profit international regulatory authority whose mission is to assure the reliability of the bulk power system in North America, NERC develops and enforces Reliability Standards; annually assesses seasonal and log-term reliability; monitors the bulk power system; and, educates, trains and certifies industry personnel. NERC is the private sector regulatory authority which, under the oversight of the United States Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada, is chartered to direct, measure, mandate and regulate the cyber security systems used by users, owners and operators of the bulk power system for more than 334 million people in North America.

The scope of NERC oversight is vast – it includes Cyber Information Technology assets (cyber systems) that reside at a variety of North American Bulk Electric System (BES) contributors, as well as the physical, manpower, governance, economic and logistical components that are used to provide North American electrical power. NERC acts as a single point of contact for the relationship between FERC and the BES providers, and operates bi-directionally with stakeholders from both communities.

Due to the NERC CIP v5's broad coverage of subjects relative to the Responsible Entity, 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 NERC Critical Infrastructure Protection topics and the VMware software-defined data center (SDDC) platform and solutions.

NERC CIP v5 Scope

NERC CIP v5 is a body of ten standards that address Critical Cyber Infrastructure technologies, policies and procedures in a way that promotes (while not guaranteeing) a sound approach to risk avoidance for the Bulk Electric Systems providers to the North American power "grid." While not specifically mandating a particular risk avoidance framework or underlying specific standard, much of NERC CIP is compatible with the National Institute of Standards and Technology (NIST) Security and Privacy Controls for Federal Information Systems and Organizations (see NIST Special Publication 800-53 Revision 4) initiatives and philosophy.

The prescriptive methods present in other regulations, such as the Payment Card Industry Data Security Standard (PCI DSS), where specific guidance is provided on "how to secure", are absent from the requirements section of CIP standards. Instead, the NERC CIP standards contain a section on Requirements and Measures, where specific outcome-based "shall" directives are stated and means to evaluate compliance with the "shall" directives are enumerated. The NERC CIP standards also contain a section titled Guidelines and Technical Basis which provides additional insights on how the "shall" directives may be arrived at. This additional information augments the requirements and measurement sections with insight that can direct the IT and InfoSec architects to concrete outcomes. The Guidelines… sections of each standard often provide similar details to what PCI DSS requirements specifically direct.

Coalfire has elected to put emphasis on both the Requirements and Measures and Guidelines and Technical Basis sections of the specific NERC CIP v5 standards, and to use these sections in combination to define what we will refer to hereafter as "requirements" or "controls" for the purposes of this Product Applicability Guide (PAG). Also, please be advised, this is our interpretation and not necessarily followed by all members of the audit community. We do not aim to mislead with this interpretation, but instead to seek to use the terms "control" and "requirement" in closer alignment with how they are meant in the Information Security community, without specific bias of NERC CIP regulatory meaning. From this point forward in this Product Applicability Guide, we will use "control" and "requirement" to mean the general InfoSec term, and the capitalized "Requirement(s)" to mean specifically a NERC CIP Requirement, per se. Similarly, we will use "Guideline(s)" and "Technical Basis (Bases)" to reflect NERC CIP elements from the Guidelines and Technical Basis section of the standards.

Sourcing the entire policy framework, we start with identification of North American Electric Reliability Corporation Critical Infrastructure Protection, Version 5 (NERC CIP v5) topics that are applicable to information technology that make up common infrastructure used for the storage, processing, transmission and destruction of electronic data.

VMware SDDC Solution Scope

This Product Applicability Guide (PAG) is focused on the VMware software-defined data center (SDDC), which is presented and described in the Creating a VMware Software-Defined Data Center – Reference Architecture Version 1.5 (VMware, Inc., 2014) document. This technical white paper was created to convey details of the logical architecture and reflect nuances of the physical implementation.

VMware vCloud Suite - Enterprise

VMware vCloud Suite is an integrated bundle of VMware products that bring together vSphere, VMware vRealize cloud management and, optionally in the Enterprise packaging, VMware Site Recovery Manager (SRM) to deliver a vSphere-based private cloud. It is bundled and priced to deliver maximum value at time of purchase. With use of vCloud Suite, VMware claims dramatic improvements in efficiency, agility and control of the virtual IT environment. See figure 2 for an overview of vCloud Suite components and roles.

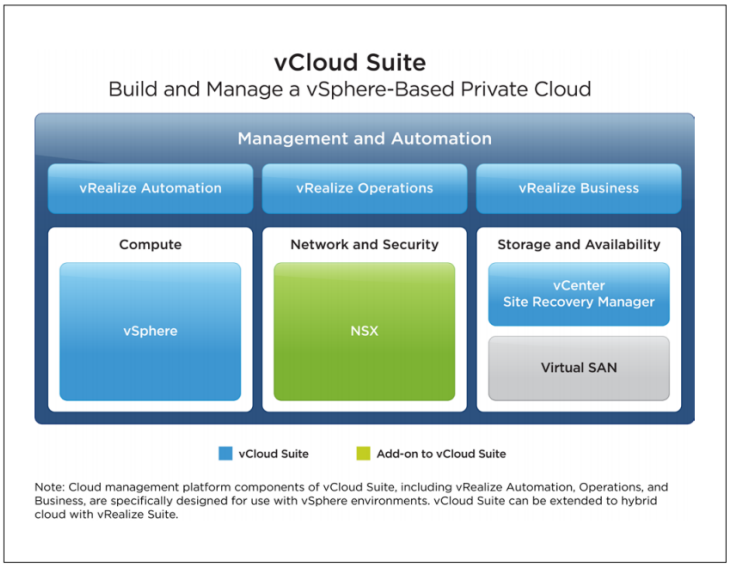


Figure 2 - vCloud Suite

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. VMware vSphere is a suite of products with the following key components:

- VMware vSphere Hypervisor Architecture (ESXi)
- VMware vSphere Storage, OpenStack, Management and Control APIs
- VMware vSphere High Availability
- VMware vSphere Fault Tolerance
- VMware vSphere Data Protection
- VMware vShield Endpoint
- 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 ensure security and availability, simplify day-to-day tasks, and reduce complexity of managing a virtual infrastructure.

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

VMware vCenter Site Recovery Manager Enterprise

Disaster Recovery Automation is delivered by the vCenter Site Recovery Manager (SRM) Enterprise component of vCloud Suite. SRM helps the solution architect design scalable, testable and manageable fault-resilient data centers which do not require the traditional hand-built N+1 designs – designs which customarily require complex operational plans and do not easily tolerate failure event simulation. SRM uses the inherent flexibility of virtual machines, storage and networking, along with "runbook" operation automation to make Disaster Recovery feasible and cost-effective.

VMware vRealize Business for vSphere

VMware addresses the following business goals of a SDDC operation with vRealize Business for vSphere: perform business unit aware cost analysis; generate and manage information to make informed decisions on provisioning and operations of cloud resources, including storage, network and compute resources; and support costing of non-ESXi physical servers managed by the vCloud suite.

VMware vRealize Automation Enterprise

Used to automate the service delivery process to private and hybrid cloud infrastructures, vRealize Automation Enterprise augments the vCloud products with service management, multiple-endpoint/vendor provisioning and policy-based tools for DevOps integration. Via a tight integration between vRealize Automation and other elements of the vSphere suite, on-demand network and resource creation can be automated for rapid and consistent delivery of customer workload deploys.

VMware vRealize Operations Enterprise

To manage the vSphere infrastructure, increase performance, improve efficiency and support a policy-driven management paradigm, vRealize Operations Enterprise delivers a comprehensive suite of control and visualization tools to the Responsible Entity. This toolset may be used to harden vSphere hypervisors and to granularly manage the guest VM Operating System for standard upkeep and for regulatory compliance. Via use of OS-level regulatory compliance-management packs, comprehensive controls may be deployed fleet-wide for greater efficiency. For deployed client applications, pre-supplied and customized monitoring can keep the pulse of the service delivery through visualization and alert mechanisms.

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.

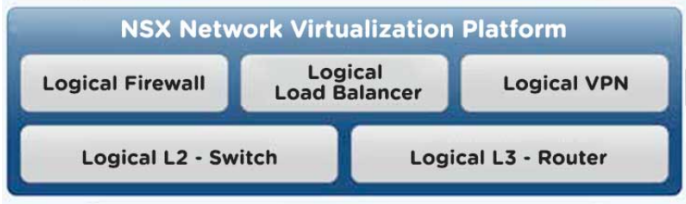


Figure 3 - VMware NSX Platform for Advanced Networking

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 promoting 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 VM's under vCenter.

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

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 enforced 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 for NERC CIP Cyber security architectures subject to compliance requirements.

Intel TXT and AES-NI

Intel Trusted Execution Technology (Intel TXT) provides hardware-based security technologies to help build a solid foundation for security which enables IT to establish trusted pools of virtualized resources for stronger security and compliance in multi-tenant virtual and cloud environments. Built into Intel's silicon, these technologies address the increasing and evolving security threats across the virtual infrastructure. Intel TXT also can play a role in meeting government and industry regulations and data protection standards by providing a hardware-based method of verification useful in compliance efforts.

Intel Advanced Encryption Standard New Instructions (Intel AES-NI) accelerates the most compute-intensive steps of AES algorithms to significantly reduce the performance penalties of encryption. Supported in the VMware ESXi kernel, AES-NI accelerates encryption allowing you to encrypt / decrypt sensitive data and communications throughout your data center without the performance penalty of security.

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

Our Approach

We show an overview of the NERC CIP v5 Cyber Security Standards CIP-002 through CIP-011 which is in the following section. NERC CIP is a composite of technical requirements, which may be mapped against VMware SDDC and Partner technologies; and, a suite of policy requirements, which have no VMware SDDC direct requirement mapping, as they pertain to programs, personnel, procedures and policies.

Each CIP has a Section (B.) pertaining to Requirements and Measures, where the clear “shall” statements of what is required and how it may be evaluated for appropriate evidence is prescribed. CIP also contains Section (C.) which defines the Compliance Monitoring Process, and stating who enforces compliance, how evidence is retained, monitored and assessed. In Section C., tables enumerate the Violation Severity Levels (VSLs) on a per-requirement basis, which shows inadequate action to satisfy the requirement, and a ranking of the VSL as Lower, Moderate, High and Severe. The final two sections of each CIP are Guidelines and Technical Basis and Rationale where more detail and reasoning is provided to guide the responsible party with additional supporting information to make their tasks clear.

Our approach to interpreting these standards is based on an understanding the technical requirement policies, which are specifically restricted to CIP-005, CIP-007, CIP-009, CIP-010 and CIP-011, and focus on Electronic Security Perimeter(s), Systems Security Management, Recovery Plans for BES Cyber Systems, Configuration Change Management and Vulnerability and Information Protection, respectively. Where the Guidelines and Technical Basis section of a standard directs the responsible party toward NIST 800-53 and other guidance, we are interpreting the VMware and partner technical solutions in light of the requirement following that guidance. Where no such guidance is suggested, we will provide specific details of our cyber security “best practices,” as observed in a multitude of customer scenarios that we believe apply. Unlike HIPAA/Hytrust, FedRAMP and other regulations, NERC standards committees and the FERC subject to enforcement regulation has been devoid of the strong hand of NIST.

In general, the following figure illustrates 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:

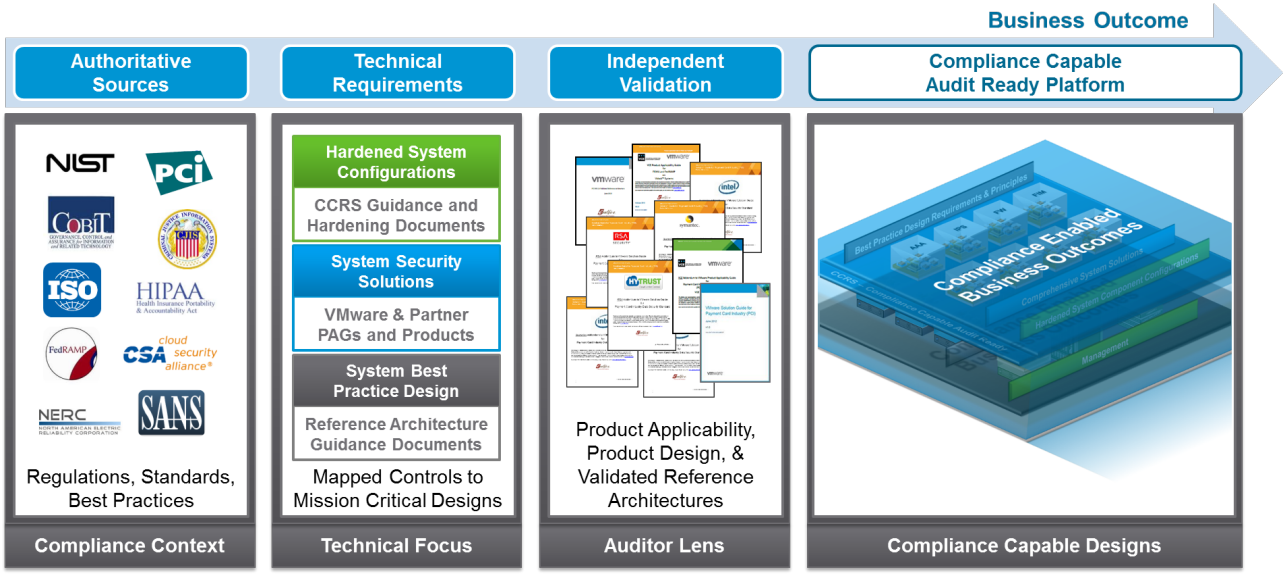


Figure 4 - VMware's complete approach to compliance

This compliance approach applies to the software-defined data center and end-user computing stack of VMware technologies which are integrated to formulate a total solution for the NERC CIP Responsible Entity. The comprehensive layering of these technologies is represented here:

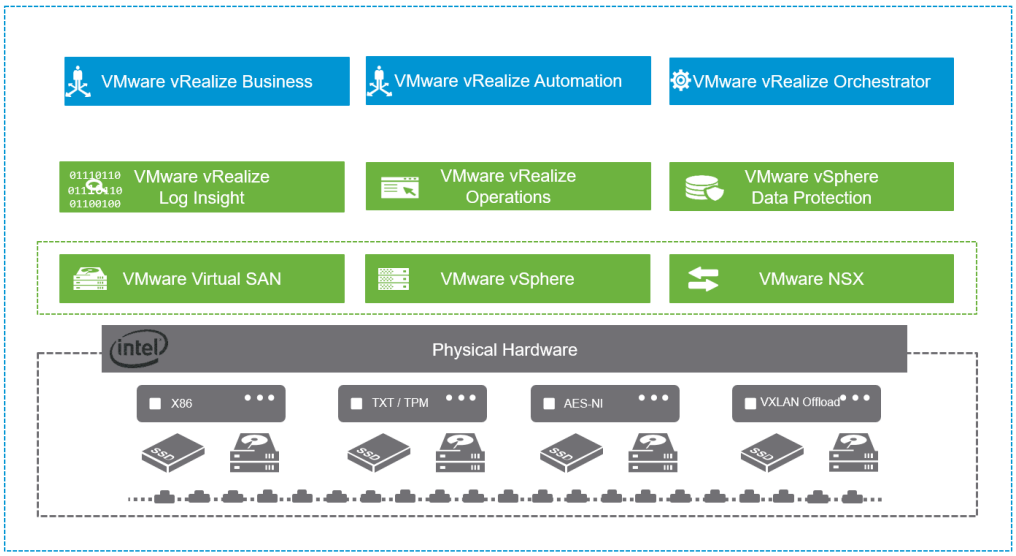


Figure 5 - VMware SDDC/EUC Product Stack Layering

VMware and NERC CIP v5 Requirements (Overview)

VMware has created a NERC CIP V5 Cyber Security requirement matrix to assist responsible entities with understanding how VMware technologies align with and support the CIP standards, requirements and guidance. The requirement matrix identifies the degree of compliance attainability for which VMware platform and platform management technologies combined with partner technologies can provide. The remaining standards are required or addressable by covered entities tools, policies, procedures, and training. While every cloud is unique, Coalfire believes that a majority of technical standards can be addressed by VMware and Partner solutions.

NERC CIP V5 CYBER SECURITY STANDARDS		PRODUCTS
CIP-002-5.1	BES Cyber System Categorization (non-technical)	none
CIP-003-5	Security Management Controls (non-technical)	none
CIP-004-5.1	Personnel & Training (non-technical)	none
CIP-005-5	Electronic Security Perimeter(s)	VMware vRealize Configuration Manager, VMware vRealize Log Insight, VMware vRealize Automation, VMware vSphere ESXi, VMware vCenter Server, VMware NSX
CIP-006-5	Physical Security of BES Cyber Systems (non-technical)	none
CIP-007-5	Systems Security Management	VMware vRealize Configuration Manager, VMware vRealize Log Insight, VMware vRealize Automation, VMware vSphere ESXi, VMware vCenter Server, VMware NSX, vSphere Data Protection
CIP-008-5	Incident Reporting and Response Planning (non-technical)	none
CIP-009-5	Recovery Plans for BES Cyber Systems	VMware vRealize Configuration Manager, VMware vRealize Log Insight, VMware vRealize Automation, VMware ESXi, VMware vCenter Server, VMware NSX, VMware vRealize Log Insight, VMware vRealize Configuration Manager, VMware vRealize Site Recovery Manager, VMware vRealize Workspace Suite
CIP-010-1 (new with V5)	Configuration Change Management and Vulnerability Assessments	VMware ESXi, VMware vCenter Server, VMware NSX, VMware vRealize Log Insight, VMware vRealize Configuration Manager, VMware vRealize Site Recovery Manager, VMware vRealize Workspace Suite, VMware User Environment Manager, VMware NSX for vSphere Horizon Edition, AirWatch Enterprise Mobility Management, VMware Identity Manager
CIP-011-1 (new with V5)	Information Protection	none

Table 1: VMware Solutions Applicability to NERC CIP V5 Standards

In Table 1, we present VMware technology which either fully or partially addresses the NERC CIP v5 standards on a per standard basis. Partner technologies are not included in this view.

The following high level overview, presented here in Table 2, goes into additional detail on actual requirements, as stated in the standards. Again, VMware technology is reviewed for applicability; and, where the standard is either administrative,

organizational or policy oriented in scope, it will be noted that technology is “not applicable.” If the auditor’s opinion is that a VMware technology may be used to address the standard the term “supports” will be used in the Applicability… column. As with Table 1, partner technologies are not referenced in this material, and that relationship will be presented in the following sections of this document.

In the NERC CIP framework, the entirety of CIP-002, -003, -004, -006 and -008 are organizational and policy requirements, without any technical basis. They direct the Responsible Entity to create programs, define policies, manage non-technical physical access to Cyber assets, and create teams for incident response. Although these are critical to overall Cyber Systems security and they may have technical support supplied by VMware technologies, as a byproduct of how they may be implemented (Physical Access control often runs on Virtual Machines under ESXi, managed by vCenter, for example) the actual requirements of the standard neither provide a technical basis for a control, nor do the Guidelines and Technical Basis point out a likely technology. For this reason, these CIP standards have no applicable VMware technology, and we’ve briefly noted that in Tables 1 and 2.

REQUIREMENT	IMPLEMENTATION TOPIC	GUIDELINES AND TECHNICAL BASIS	APPLICABILITY TO VMWARE TECHNOLOGIES
CIP-002-5.1	**BES Cyber System Categorization**		
R1 and R2	Categorize and Identify BES Cyber Systems		Not Applicable
CIP-003-5	**Security Management Controls**		
R1, R2, R3 and R4	CIP Sr. Manager Approval, Policy Creation, Named CIP Sr. Manager identification and documentation, Process creation for management of deficiencies		Not Applicable
CIP-004-5.1	**Personnel & Training**		
R1, R2, R3, R4 and R5	Create, implement, document and staff a: Security Awareness Program; Cyber Security Training; Personnel Risk Assessment Program; Access Management Program; and, Document Access Program		Not Applicable
CIP-005-5	**Electronic Security Perimeter(s)**		
R1.1	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP	(paraphrased) Creation of different trust zones protected by EAP (firewall) as a primary defense layer	Supports
R1.2	All External Routable Connectivity must be through an identified Electronic Access Point (EAP)	Deployed EAP to protect trust zones with evidence to measure and validate presence (paraphrased). EAP should control inbound and outbound traffic.	Supports
R2.1	Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Use of an intermediate system (jump host) where EAP rules are only sufficient for access and control of jump host. Normal control system scrutiny applies to the jump host. (paraphrased)	Supports
R2.2	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	Additional information provided in NERC publication *Guidance for Secure Interactive Remote Access* (NERC, 2011)	Supports
R2.3	Require multi-factor authentication for all Interactive Remote Access sessions.	Combined multi-factor of something in possession of the user plus something known by the user	Supports
CIP-006-5	**Physical Security of BES Cyber Systems**		
R1, R2 and R3	Create, implement, document: Physical security plan; visitor control program; and, Physical Access Control System maintenance and testing programs.		Not Applicable
CIP-007-5	**Systems Security Management**		
R1	Ports and Services		
R1.1	Enable only needed ports as determined by the Responsible Entity. Disable not needed ports.	Positioned in-line in a non-bypassable manner.	Supports

REQUIREMENT	IMPLEMENTATION TOPIC	GUIDELINES AND TECHNICAL BASIS	APPLICABILITY TO VMWARE TECHNOLOGIES
R1.2	Protect against the use of unnecessary physical Input/out ports used for network connectivity, console commands or removable media.		Not Applicable
R2	Security Patch Management		
R2.1	Create a patch management process for tracking, valuating, and installing cyber security patches for applicable Cyber Assets. Tracking includes identification of sources.	Amalgam of National Vulnerability Database, OS and Control System vendors used as a source for the intelligence for patches, hotfixes and updates.	Supports
R2.2	Evaluate security patches every 35 calendar days.	Use judgement and Common Vulnerability Scoring System v2.	Supports
R2.3	Apply patches, or create/revise a dated mitigation plan (compensation) with a timeframe to complete these mitigations.	…the entity either installs the patch or documents (via mitigation plan) the alternative.	Supports
R2.4	Implement the mitigation plan from R2.3 within the timeframe, or revise the plan with CIP Senior Manager or delegate approval		Not Applicable
R3	Malicious Code Prevention		
R3.1	Deploy method(s) to deter, detect, or prevent malicious code.		Not Applicable
R3.2	Mitigate the threat of detected malicious code.	…traditional antivirus…automatically remove or quarantine…	Supports
R3.3	For methods identified in Part 3.1 that used signatures or patterns, have a process for update of the signatures or patterns, and address testing and installing.		Not Applicable
R4	Security Event Monitoring		
R4.1	Log Events at the BES Cyber System level or BES Asset level for identification of, and investigation of, Cyber Security Incidents for … detected successful and failed access/login attempts … Detected malicious code	Refer to NIST 800-92 and 800-137 for additional guidance…	Supports
R4.2	Generate alerts for security events … that include … Detected malicious code from part 4.1 and detected failure of part 4.1 event logging.		Not Applicable
R4.3	…retain applicable event logs identified in Part 4.1 for at least 90 days …		Not Applicable
R4.4	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.		Not Applicable
R5	System Access Control		
R5.1	Have a method(s) to enforce authentication of interactive user access, where technically feasible		Supports
R5.2	Identify and inventory all known enabled default or other generic account types…		Not Applicable
R5.3	Identify individuals who have authorized access to shared accounts		Not Applicable
R5.4	Change known default passwords	Remove published or known defaults.	Supports
R5.5	For password-only authentication for interactive user access, … enforce the following password parameters: ...1) length of 8 characters or feasible	… does not include read-only information access in which the configuration of the … Asset cannot	Supports

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

REQUIREMENT	IMPLEMENTATION TOPIC	GUIDELINES AND TECHNICAL BASIS	APPLICABILITY TO VMWARE TECHNOLOGIES
	maximum; and, …2) Minimum complexity that is the lesser of three or more different types of characters .. or the maximum complexity supported by the Cyber Asset.	change. Complexity rules are included in this section.	
R5.6	… enforce password changes or an obligation to change the password at least once every 15 calendar months.	…required where passwords are the only credential used to authenticate individuals.	Supports
R5.7	… limit the number of unsuccessful authentication attempts; or generate alerts after a threshold of unsuccessful authentication attempts.	… may be tailored to the operating environment over time to avoid unnecessary account lockouts.	Supports
CIP-008-5	**Incident Reporting and Response Planning**		
R1, R2 and R3	Document, Implement and Maintain a Cyber Security Incident Response Plan		Not Applicable
CIP-009-5	**Recovery Plans for BES Cyber Systems**		
R1	Create and Maintain one or multiple documented recovery plans that contain: Conditions for activation; Roles and responsibilities of responders; one or more process for the backup and storage of information required to recover…; one or more process to verify successful completion of the backup process…; and one or more process to preserve data…		Not Applicable
R2	Recovery Plan Implementation and Testing		
R2.1	Test each of the recovery plans referenced in Requirement R1 at least once every 15 months: By actual recovery; a paper drill or tabletop exercise; or, an operational exercise	Helpful and substantial details exist in this section to clarify this topic. Please see the actual Guidelines and Technical Basis Section 4, Requirements 1 and 2 for context.	Supports
R2.2	Test a representative sample of information used to recover BES Cyber System functionality every 15 months… An actual recovery … substitutes for this test.	The test must include steps for ensuring the information is usable and current. … can include testing a representative sample to make sure the information reflects the current configuration of the applicable Cyber Assets.	Supports
R2.3	Test each of the recovery plans … in Requirement R1 at least once every 36 calendar months through an operational exercise…An actual recovery may substitute…		Supports
R3	Recovery Plan Review, Update and Communication		Not Applicable
CIP-010-1	**Configuration Change Management and Vulnerability Assessments**		
R1	Each Responsible Entity shall implement, in a manner that identifies, assesses and corrects deficiencies, one or more documented processes that collective include each of the applicable requirement parts in CIP-010-1 Table R1 (follows)		
R1.1	Develop a baseline configuration…which shall include: Operating system(s) or firmware; and commercially available or open-source …; custom software installed; any logical network accessible ports; and, any security patches applied	Baseline configuration in CIP-010 consist of five different items: O/S firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. See additional examples in the Guidelines and Technical Basis Section for more detail.	Supports
R1.2	Authorize and document changes that deviate from the existing baseline configuration.		Not Applicable
R1.3	For a change that deviates from the existing baseline configuration, update the baseline … within 30 calendar days …		Not Applicable

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

REQUIREMENT	IMPLEMENTATION TOPIC	GUIDELINES AND TECHNICAL BASIS	APPLICABILITY TO VMWARE TECHNOLOGIES
R1.4	For a change that deviates from the existing baseline configuration, determine cyber security controls in CIP-005 and CIP-007 that could be impacted; … verify that required cyber security controls determined in 1.4.1 are not adversely affected; and, document the results of the verification		Not Applicable
R1.5	Where technically feasible, for each change that deviates from the existing baseline configuration: Prior to implementing .. test the changes… ; and, document the results of the testing and … the difference between the test environment and the production environment, including a description of the measures used to account for any differences…	(see above R1.1)	Supports
R2	Configuration Monitoring		
R2.1	Monitor at least once every 35 calendar days for changes to the baseline configuration… Document and investigate detected unauthorized changes.		Not Applicable
R3	Vulnerability Assessments		
R3.1	At least once every 15 calendar months, conduct a paper or active vulnerability assessment		Not Applicable
R3.2	Where technically feasible, at least once every 36 calendar months: Perform an active vulnerability assessment in a production environment…; and, document the results…		Not Applicable
R3.3	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment…	The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification … is well documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.	Supports
R3.4	Document the results of R3.1, 3.2 and 3.3 and the action plan to remediate or mitigate vulnerabilities identified…		Not Applicable
CIP-011-1	**Information Protection**		
R1 and R2	Implement… one or more documented information protection program(s) that … include… Methods to identify information that meets the definition of BES Cyber System Information; … methods to … prevent the unauthorized retrieval of BES Cyber System Information from … data storage media; and methods to prevent unauthorized retrieval…		Not Applicable

Table 2: NERC CIP V5 Standards and VMware Applicability Mapping

Figure 5 below diagrams the percent of coverage for NERC CIP v5 standards that are addressable by VMware and VMware Partner technologies. VMware and partner capabilities are primarily aligned to technical standards. The remaining gaps in capabilities, represented in blue in this diagram, may be filled by the covered entity through other means.

Areas outside of technical controls covered by VMware and its' Partner technology, may be satisfied by a combination of business associate contracts and agreements, policies, documented procedures, training, infrastructure diagrams and documentation, management structure, control processes, physical security measures, personnel hiring practices,

management procedures and other Responsible Entity actions.

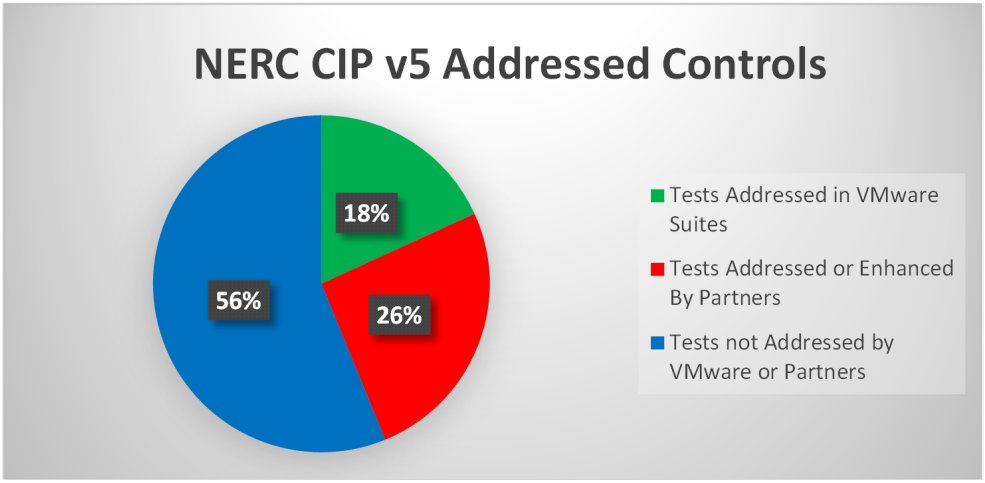


Figure 6

The following table 3 illustrates the NERC CIP V5 controls reviewed in this document and their support by VMware SDDC and partner technologies. For the purposes of counts in the tables below, the auditor defines a "control" as the detailed interpretation of a general requirement (for instance R1) at the specific sub-requirement level (e.g. R1.1) – meaning that a table that expands on the details of a general requirement with 5 entries, counts as 5 controls, one for each sub-requirement. For example, NERC CIP-003-5 has four (4) requirements, with a total of 15 sub-requirements (R1.1-9, R2.1-4, R3 and R4). We interpret that as 15 controls. This method of interpretation applies to technical and non-technical (process, policy, documentation, etc.) controls alike.

PIE CHART	NERC CIP V5 (AND INFORCE V3) STANDARDS	# NERC CIP V5 CONTROLS	CONTROLS ENABLED IN VMWARE'S SDDC SUITES	CONTROLS ENABLED OR ENHANCED WITH PARTNER SOLUTIONS	CONTROLS NOT ADDRESSED BY VMWARE OR PARTNERS
	**Non-Technical Standards** CIP-002, CIP-003, CIP-004, CIP-006 and CIP-008	60	0	0	60
	CIP-005-5 **Electronic Security Perimeter(s)**	5	5	5	0
	CIP-007-5 **System Security Management**	20	11	17	2
	CIP-009-5 **Recovery Plans for BES Cyber Systems**	4	3	2	1
	CIP-010-1 **Configuration Change Management and Vulnerability Assessments**	10	3	6	4
	CIP-011-1 **Information Protection**	2	0	1	1

Table 3: NERC CIP Controls enabled and not addressed by VMware and technology Partners

VMware Control Capabilities Detail (Per NERC CIP v5 Standard)

In this section Coalfire highlights the VMware SDDC solutions that have specific impacts on the NERC CIP v5 Standard requirements, as compiled above in the tables and charts. While not all controls have a solution with VMware technologies, those that do often receive only partial coverage of the requirement by the technology. The reader should assume that companion products in conjunction with Responsible Entity policies, procedures, methods and best practices are used to create the most complete and comprehensive compliance to meet the requirement.

CIP-005-5 Electronic Security Perimeter(s)

Requirement R1 Description: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1. Table R1 requires 2 controls: Residence within an ESP; and, all externally routable connectivity passes through an EAP.

VMware Capability: The primary focus of these controls is to secure the Responsible Entity's networks and specifically firewall and router-based security controls that are provided by several elements of the VMware SDDC ESXi hypervisor and NSX products. The software defined networking features of VMware ESXi deliver the essential "basic" networking used to create network segments which are potential boundaries for security zones, or the basic network that might be enclosed by an Electronic Security Perimeter (ESP). The VMware NSX product, by virtue of its Firewall object performing the duties of an Electronic Access Point, is combined with the basic ESXi networking to constrain the access that a network segment may have with a rule-based, access-list driven technology, satisfying the R1.1 and R1.2 control requirements.

The VMware NSX network toolset has further capacity to construct the required ESP/EAP control via the use of "micro-segmentation." In a micro-segmented network, the VMware ESXi Distributed vSwitch networking is enhanced with additional features that may be selectively applied to any of the Virtual Machines (VMs) by the inclusion of NSX on the hypervisor. Running as a built-in resource, NSX adds a "toolkit" of routing, VPN, VLAN, and security components that may be engaged on VMs which are centrally managed and monitored by vCenter and vRealize Suite administration. The "micro-segmentation" component is effectively a "firewall wrapper" that, once applied to a VM, enables packet inspection at Layer 2 through Layer 7, and firewall access rules to apply to incoming and outgoing traffic to/from the virtual machine. The unique aspect of NSX micro-segmentation is that it requires no host-based software to deliver this service and is entirely agnostic and transparent with respect to the operating system. It may be applied to insecure network architectures which may not have appropriate conventional segmentation to create the ESP, and is a terrific tool to achieve compliance without massive re-engineering of the BES networks.

Requirement R2 Description: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management. Table R2 specifies three controls: Use of an intermediate system; encryption that terminates at the intermediate system; and, multi-factor authentication for all Interactive Remote Access.

VMware Capability: VMware SDDC ESXi may be used to construct the intermediate system as a VM, and to logically connect it to the appropriate network within the ESP, protected by an EAP, as outlined in the section above. This use-case is typically referred to as a "jump host" is a mainstay of virtualization architectures, and fully satisfies requirement R2.1. Complete management of this host is supported by additional components in the vCloud SDDC suite, specifically: vCenter and vRealize Operations. Selection of the VM host operating system, configuration and tools is left entirely up to the Responsible Entity. The creation and support of jump host inventories, including rapid deploy and re-configuration technologies are supplied by vCenter through use of custom templates and the "deploy from template" features that are built-in.

R2.2 controls may be satisfied by use of VMware NSX VPN encryption, applied to the VM directly. In conjunction with Firewall rules for Layer 2-7 access in and out, strong encryption of the access event is assured. If external firewall devices are desired, they may be supplied by partners and can be deployed in either physical, or Virtual Appliance (VMware VM that is purpose-built as a firewall) versions.

The requirement R2.3 for multi-factor authentication is supported throughout the VMware product suite, and may be enhanced through partner offerings.

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

NERC CIP005-5 Additional Guidance: The publication *Guidance for Secure Interactive Remote Access* (NERC, 2011) supplies a host of detail that is helpful to create a set of procedures used by the Responsible Entity to institute a routine method for using VMware SDDC technology to remain compliant with CIP-005-5 and all required controls. VMware hardening guides and best practice documentation, and a wealth of knowledge on the VMware Partner Exchange may also be useful.

VMware partner organizations also deliver a host of useful and valuable products and services to meet these requirements – for instance, firewall vendors, those traditionally with hardware products and considered the mainstays of networking technology providers have been providing Virtual Appliance VM's of many of their top products. These products are often priced substantially below that of their hardware counterparts, and are also typically feature identical.

Coalfire Additional Considerations: VMware solutions are dependent on Access Control capacities provided by integration with a 3rd party when using a third party Virtual Appliance.

Jump host configurations are subject to machine image baseline configuration management, as dictated by CIP-010-1 requirements R1.1, R1.4 and also subject to monitoring requirements stipulated in requirement R2.1. Jump hosts are typically subject to more scrutiny than a traditional VM, because they have the potential for external access. The auditor recommends strict image control, and even the use of "powered on upon need" procedures, where the jump host is maintained in the powered off state until an event requires its' activation.

CIP-007-5 Systems Security Management

Requirement R1 Description: Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R1 – Ports and Services*. Table R1 enumerates 2 controls: Enable only needed ports / Disable not needed ports; and, Protect against unnecessary use.

VMware Capability: Regarding Ports and Services (Requirement 1), VMware is considered to be a participant in control and allocation of network ports, and is usually working in parallel with existing network switches in the typical SDDC. Network switch integration to vSphere is via connectivity to the VMware ESXi hypervisors, where the ports on the ESXi server are connected directly to dedicated ports on the switch(es), ports which either reside on particular VLANs or have 802.1q trunk connectivity to allow the hypervisor to participate on multiple VLANs. VMware vCenter and vRealize Operations Management have authoritative control over all hypervisor and virtual machine use of networks ports; but, not typically of the configurations of the outboard network switches. So, in summary, virtual machine connections may be entirely under the control of vSphere, whilst the network switches themselves and their port allocation and control are managed elsewhere.

When NSX has been deployed on a vSphere SDDC, additional fine grained control of the ESXi hypervisor switch ports, as they are consumed by the virtual machines, is added to the basic Layer 2 delivery provided by VMware Distributed vSwitches. By virtue of the NSX components (firewall, load balancer, router, VLAN management, VPN, micro-segmentation, etc.) and the pervasive and transparent presence of NSX on a hypervisor, virtual machine networking may receive the architectural benefits of those additions to basic virtual switching. Please note that the firewall rules are bound to the VM and not a specific hypervisor/host, and any vMotion activities will keep the rules connected to the VM, regardless of where it is hosted. Requirement 1.1, is supported by these SDDC features.

Requirement R2 Description: Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R2 – Security Patch Management*.

VMware Capability: Security Patch Management specified in Requirements 2.1-2.3 is supported by both VMware vCenter Update Manager (UM) and partner products for the hypervisor system images, and optionally for the underlying operating systems. UM is merely a vehicle for administering the program defined in R2.1 and sustained in R2.2, while it is the actual agent used to apply patches to (primarily) VMware software. It is customary that third party partner product are relied upon to supply patches for network equipment, servers resident (and not) on ESXi, and other critical infrastructure.

Requirement R3 Description: Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R3 – Malicious Code Prevention*.,

VMware Capability: Requirement 3, Malicious Code Prevention, is principally provided by partner products, but is supported (R3.2) by vCenter vRealize Operations and vCenter activities which coordinate the containment process, and are used to automate (or manually perform) the shutting down and quarantining of the infected virtual machine. Follow-up use of VMware snapshot technologies may be used to re-deploy a pre-infection instance of a de-commissioned VM. Rapid recovery, in this manner, is a key strength of virtualized servers versus traditional bare-metal system deployments.

Requirement R4 Description: Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R4 – Security Event Monitoring*.

VMware Capability: R4.1, which requires logging of events pertaining to successful and failed logins, is supported on the entire suite of VMware products. Via traditional syslog services and integrated internal logging, VMware vCenter actions are treated with the intended safety of this requirement, and may work in concert with partner SIEM products to provide for a comprehensive view of events at the Responsible Entity.

Requirement R5 Description: Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R5 – System Access Controls*.

VMware Capability: Systems Access Control under Requirements R5.1, and 5.4-5.7is supported by VMware SDDC technologies. Integration with LDAP, Microsoft AD and internal VMware authentication systems fully supports enforcement, change control, required complexity, unsuccessful lockout and the logging and (through partner integration) generation of alerts.

NERC CIP007-5 Additional Guidance: In the Guidelines and Technical Basis section of this standard, a wealth of specific advice is provided. The reference under R1 1.1, makes specific mention of host based firewalls. VMware NSX is actually superior to host based firewalls, in that it deploys transparently, is invisible to the operating environment and is centrally managed. Anti-malware and patch management solutions provided by partner technologies, are relied upon, in conjunction with VMware SDDC features. Requirement R4 specifically references NIST 800-92 and 800-137 for additional guidance in security monitoring. Third party SIEM and logging solutions are also advised in the Guidelines… Integration with comprehensive authentication and access control components like Microsoft's Active Directory is widespread and supported when using VMware SDDC technology. Single point of control integration is favored by NERC guidelines.

Coalfire Additional Considerations: CIP-007-5 is the most comprehensive and targeted standard to address Systems Security in the NERC CIP portfolio. Much of what is required in this standard is very similar to other regulated frameworks, and much of what might be used in PCI-DSS, would likely apply to satisfy the CIP Requirements under this Standard. VMware hardening guides, the vRealize Operations Configuration Manager (VCM) compliance templates and other provided tools can also assist in meeting these objectives.

Partner products – particularly: networking switches and their management tools; Security Information and Event Management (SIEM) systems; Anti-virus and anti-malware software; Intruder Detection / Intruder Prevention systems; Patch and systems integrity checking / management software; change control; and, event logging systems – are invaluable and required companions to VMware SDDC NERC-CIP implementations.

CIP-009-5 Recovery Plans for BES Cyber Systems

Requirement R2 Description: Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.*

Requirement R1 of CIP-009-5 calls for the Responsible Entity to create a documented plan with specific conditions for activation, roles and responsibilities, backup and storage process(es), verification and preservation. This leaves the Responsible entity open to define the specifics of said plan. In our section on R2, we make some assumptions, based on NERC and InfoSec best practices, about what a "typical" plan might look like. We assume that the Recovery Plan for most Responsible Entities has these integral components:

- Systems Disaster Recovery Planning
- Critical Information and Data Backup and Recovery Planning
- Cyber System asset valuation and identification of critical systems
- Risk Analysis and Ranking
- Processes for Restoration to Service

Assuming these components are in place, NERC Responsible Entities would put emphasis on the Restoration to Service portion of their plan, and not just "meet the basic requirement" of backing up data (recognize that DR is more than just backups). This is the stance of evolved Information reliant entities in all business segments.

VMware Capability: VMware vRealize Site Recovery Manager (SRM) supplies a unique bundle of enhancement to the standard VMware vCenter / ESXi core – it provides for a comprehensive set of Disaster Recovery tools that let backup and redundant systems be developed and deployed quickly and with assurance. By replicating the VM context from one vCenter Data Center to a backup one, and then remaining in constant readiness to "cut over" to the redundant Center, SRM positions the Responsible Entity to be prompt and effective in the event of a failure.

Requirements R2.1, R2.2 and R2.3 call for test of the recovery plan, and VMware SRM has complete simulation of the fail-over and fail-back process, as part of its basic functionality.

In a non-SRM environment, manual and vRealize Automation events may be used to construct test scenarios, clone critical assets for testing, etc. So either by user of SRM or basic SDDC tools, this requirement may be met for Information systems.

Representative samples of the recovery data, called for in R2.2, are available through the VMware vCenter snapshot feature, and may also be delivered by similarly by Partner supplied storage systems and their data snapshot technologies. VMware vCenter snapshot actually exceed the base requirement of R2.2, by a snapshot including the entirety of the system, data, context, and operational state of the VM. This brings more utility to both testing and actual recovery, by packaging data plus machine details into a "moment in time" instance of the VM.

Periodic recovery on the …once every 15 months… and the mandated operational exercise every 36 months are supported by VMware and partner products used within the specific guidelines of the Responsible Entity's recovery plan.

NERC CIP009-5 Additional Guidance: Once again, Guidelines and Technical Basis illuminate the "how to" aspects of this standard. The plan created in Requirement 1 is supported by two documents that are helpful: *NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions* (NERC, 2011); and, the *National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010* (NIST, 2010). Although the Guidelines… focus primarily on the backup and recovery of information, the section on Requirement 2 targets the process side and suggests use of FEMA Homeland Security Exercise and Evaluation Program (HSEEP) protocols that may be helpful.

Coalfire Additional Considerations: CIP009-5, in the auditor's opinion, is very strong on policy and process requirement, while remaining somewhat weak on the comprehensive nature of information technology infrastructure recovery. The view that places specific emphasis on largely recovery of information is not in keeping with the more holistic approach that has evolved in other regulatory frameworks and is the "accepted wisdom" for IT planners. When using a virtualized infrastructure, such as VMware SDDC, the notion that "your systems are just data", does, however, play nicely into NERC's viewpoint. Taking that perspective, preservation and rapid recovery of data that constitutes the virtual machine, virtual network, etc., is well supported by VMware SRM and vSphere technologies and directly supports, in a cost-effective and efficient manner.

CIP-010-1 Configuration Change Management and Vulnerability Assessments

Requirement R1 Description: Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R1 – Configuration Change Management.*

VMware Capability: VMware supports Requirement 1.1 which stipulates that a baseline configuration must be developed, and which includes the operating system, custom software, logical port access and security patches. Two mechanisms are available in VMware SDDC to accomplish this: Using the Template features of vCenter, specifically the Customization Specification Manager tool; and, using vRealize Operations deployment tools. These tools actually go beyond the minimal requirement of baseline creation; and, can be used to create, maintain and deploy at will, an arsenal of system images. VMware also provides for virtual machine snapshot functions, which can capture a "moment in time" image of a system, along with transient state information, which may be useful for satisfaction of R1.1 and also useful in compliance with R1.5, which calls for "…test the changes…" when creating a deviated system image for an approved baseline image.

Metadata can be attached to the virtual machine images, templates and to the Customization Specification, which may serve as part of the required documentation base to support the change control process as images are iterated during their use life. These built-in features may also be augmented by use of partner product that are designed for traditional bare-metal system image management.

R1.1 also request that the base images have specific network access control applied to ports and services, such that only intended source/destination/port combinations required for cyber system function are enabled. The auditor believes that VMware NSX or host system firewall software is suitable for this requirement.

NERC CIP010-5 Additional Guidance: Guidelines and Technical Basis for Requirement 1 specifically mention that the operating systems are intended to be "locked down" by configuring five elements of each system as the baseline: Operating system, firmware, custom software, network port configuration and applied patches. Further, it is stipulated that un-necessary components of the installed system should be either removed or rendered inoperative by disabling.

The Standard Development Team (SDT), mentioned in this Guidelines… section under the heading *Cyber Security Controls*, that the Responsible Entity is not expected to track all changes related to CIP005 and CIP007 at a granular level as part of this requirement; but, standards CIP005 and CIP007 are sufficient without additional stipulation as a "change to baseline" under CIP010.

Test environments, as required under R1.5, are permitted to differ from the actual production environment, as it is often infeasible to have simulated control inputs that are as comprehensive or similar to live data inputs coming from reality. These are reasonable exceptions to strict testing protocols.

Coalfire Additional Considerations: The auditor appreciates the diversity and complexity of baseline change management for Cyber Systems at the Entity. The manual process, without viable image management tools, such as those provided by VMware SDDC technology, leaves the Responsible Entity potentially vulnerable. We believe in NERC, as in other regulated frameworks, breach is often the result of compromised images going undetected in the enterprise.

As virtual appliances become more widespread in NERC vendor product offerings (following the trend in the general IT and Process Control manufacturer space, providing virtual appliance versions of what was once physical hardware), we expect to see pre-packaged OVF (Open Virtualization Format – an installable package for a virtual appliance) products that come "ready to operate" with factory-configured "locked down" images. VMware is the de-facto standard for most virtual appliances worldwide.

Vulnerability Assessments, as required by R3.1, are not specifically supported by VMware SDDC products; but, a clever operations model, using cloned production machines, may be leveraged to test critical cyber systems duplicated in their exact production context; and, then subjecting them to systems assessment, while their production counterparts remain on-line. This operational model may be supported by scripted vRealize Operations vCM tasks, and could generate automated test reports, when used in conjunction with penetration/port scanning products from partners.

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

Summary

Although the BES providers are focused on a more specific mission than most other regulatory required businesses (e.g. HIPAA for Healthcare, PCI-DSS for payment card merchants, etc.) they will still receive substantial benefits from the use of virtualized technologies from VMware. The VMware SDDC products have revolutionized cost and reliability in those other market segments; and, as NERC CIP regulated responsible BES entities move towards a more technologically sophisticated Cyber infrastructure with the onset of “Smart Grid” initiatives in the near future, those same advantages of velocity, flexibility and significantly reduced DevOps costs may be securely used by BES providers. Based on the “through the eyes of the auditor” review by Coalfire Systems, Inc., this product applicability guide identified ways in which VMware’s software-defined data center and end-user computing platforms help to govern risk and support a responsible participation in ongoing and continuing innovation.

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

Appendix A (North American Electric Reliability Corporation Critical Infrastructure Protection, Version 5 (NERC CIP v5) Requirements)

Link(s) to North American Electric Reliability Corporation Critical Infrastructure Protection, Version 5 (NERC CIP v5) requirements may be found here: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

Appendix B (What is Cloud)

NIST has defined the "Cloud" after 15 revisions over a multiple of years. The link to that press-release and definition is:

http://www.nist.gov/itl/csd/cloud-102511.cfm

Glossary of Terms

The Reliability standards NERC CIP have been develop since the initial NERC Board of Trustees adopted the proposed guidance from FERC in early 2005. In the time following the the initial adoption and throught the five specific versions, much clarification and definition of terms used in the standard has ensued.

The FERC approval process requires that terminology be initially defined during the proposal process and added to the glossary so that when final approval orders are issued, the glossary contains the concise definition of any new term. The glossary is considered to be the authoratative single point of NERC definitions for adopted (by NERC), remanded (retired) and FERC approved terms.

The current and comprehensive set of NERC adopted and FERC approved terms are available at this URL: http://www.nerc.com/files/glossary_of_terms.pdf

The terms used in this VMware SDDC NERC CIP v5 PAG are:

Term (Abbreviation)	Meaning
Bulk Electric System (BES)	Transmission Elements operated at 100kV or higher and Real Power and Reactive Power resources connected at 100kV or higher. Not inclusive of facilities used in local distribution of electric energy, radial systems, customer side generating, local networks (LN) and reactive power devices installed for sole retail customer benefit.
Critical Infrastructure Protection (CIP)	Programmatic reference to the protection of essential BES Infrastructure that if compromised would affect the reliable delivery of customer power.
CIP Senior Manager	Responsible Entity's managerial staff authority with custodial oversight of the Critical Infrastructure.
Dial-up Connectivity	Using a modem device on a traditional POTS telephone line for data access.
Electronic Access Points (EAP)	A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.
Electronic Security Perimeter (ESP)	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.
External Routable Connectivity	Connections from a BES facility that have access to the Internet, or other private network outside of the Electronic Security Perimeter(s) of that facility.
Federal Energy Regulatory	Regulatory commission monitoring interstate aspects of the utilities industries

Commission (FERC)	(electrical power, natural gas, oil pipeline, and hydroelectric).
“grid”	Euphamism that collectively means all BES participants (Transmission Elements, Real Power, Reactive Power, etc.)
North American Electric Reliability Corporation (NERC)	The not-for-profit international regulatory authority to monitor, educate, train, and certify organization participating in the “grid.”
Protected Cyber Assets (PCA)	Critical cyber assets at medium impact or high impact BES Entities.
Responsible or Functional Entity	Organization to which the NERC CIP standards apply.
Standard Drafting Team (SDT)	NERC committee that has the duty of creating and proposing standards for fututre CIP (and other) standards. Typically internally created, ratified in the general committee actions of NERC and ultimately presented to FERC for consideration and subsequent possible enforcement.

Bibliography

NERC. (2011, July). *Guidance for Secure Interactive Remote Access.* Retrieved from http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf

NERC. (2011, September). *NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operational Functions.* Retrieved from NERC Web Site: http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf

NERC. (2016, February). *CIP Standards.* Retrieved from NERC Web Site: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

NIST. (2010, May). *Special Publications 800-34 revision 1.* Retrieved from NIST Web Site: http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

VMware, Inc. (2014). *Creating a VMware Software-Defined Data Center.* Retrieved from VMware, Inc. Web Site: http://www.vmware.com/files/pdf/techpaper/vmware-reference-architecture-creating-software-defined-data-center.pdf

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 North American Electric Reliability Corporation Critical Infrastructure Protection, Version 5 (NERC CIP v5) 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