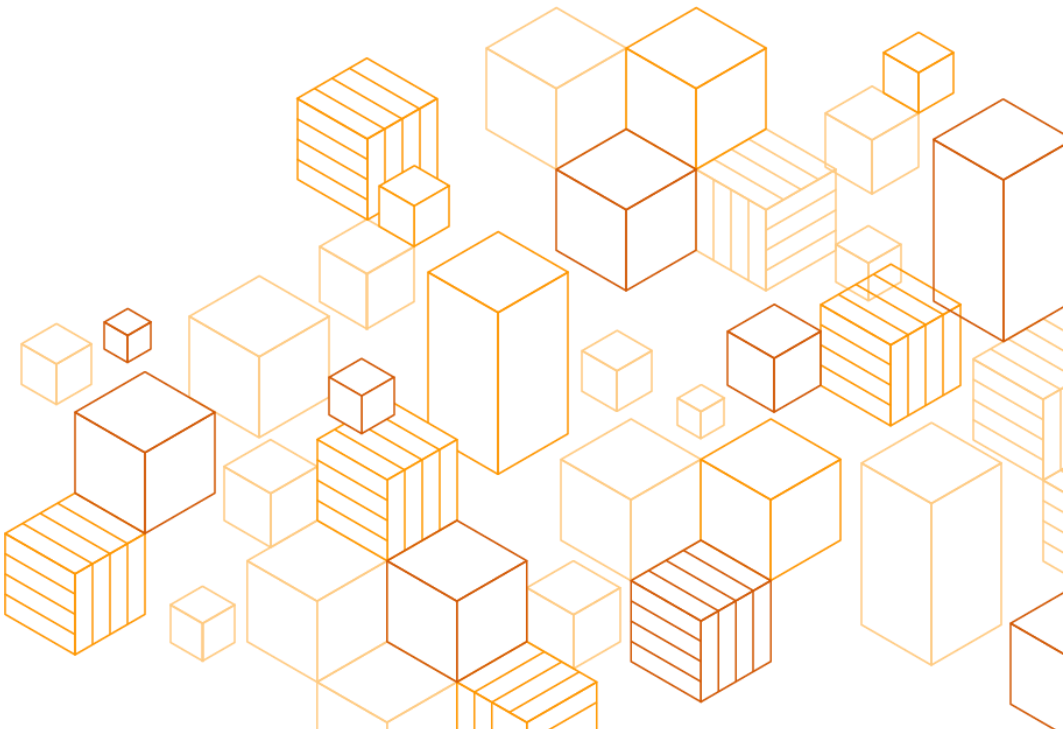
AWS User Guide to Support Compliance with North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards

November 2021



Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

About this Guide

This document describes how electric utility customers, also referred to as NERC Responsible Entities (Entities), can use AWS services to realize the benefits of cloud technology and support compliance requirements for the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards. This document explains core cloud security concepts as they apply to NERC CIP objectives,demonstrates how AWS services align to the NERC CIP requirements, and discusses how NERC Responsible Entities can plan their migration to the AWS Cloud.

Overview

This User Guide demonstrates how AWS provides a secure and reliable infrastructure, and how the wide range of AWS Cloud services can be used to support the security and reliability objectives of the NERC CIP standards. The following sections provide information on AWS services that can enable Entities to meet and sustain compliance with NERC CIP standards, how these services align with the NERC CIP standards, and considerations for Entities as they plan use of AWS Cloud services for data and systems within the regulated scope.

Background

AWS recognizes that our Power and Utility Entities are interested in leveraging cloud computing technology to meet their business objectives and the needs of their customers. Trends toward decentralization and decarbonization are changing the operational landscape of the electric grid. Cloud solutions are an important part of industry's transformative response to maintain reliable operations. IDC noted,

> "As the power and utility sector increases its digital capabilities, cloud offerings and services present companies with an attractive option for lowering overall IT and infrastructure costs while providing scalable and secure data storage with on-demand access."

As technology evolves in areas such as virtualization and cloud computing, Entities, regulators, and service providers are engaging to enable Responsible Entities to use new technologies and to meet their operational, security, and resiliency objectives. Regulators recognize the opportunities that cloud technology offers. They are moving forward to assess their role in cloud adoption and in enabling Entity cloud adoption in secure and compliant ways. In response to the Federal Energy Regulatory Commission's (FERC's) Notice of Inquiry (NOI) on cloud computing, NERC stated,

> *"The ERO Enterprise supports use of cloud computing for data storage of BCSI as the risks posed by third-party services for data storage listed below can be appropriately mitigated. …Furthermore, the ERO Enterprise could support use of cloud computing for BES reliability operating services if appropriate protections are in place to mitigate risks and vulnerabilities."*

The US electric sector is regulated by FERC, a federal independent agency that

regulates the interstate transmission of liquefied natural gas, oil and electricity, along with natural gas and hydropower projects. US electric sector Entities are subject to mandatory and enforceable security requirements to protect the reliability of the Bulk Electric System (BES).

In 2006, FERC certified the North American Electric Reliability Corporation (NERC) as the Electric Reliability Organization (ERO) with authority to develop Critical Infrastructure Protection (CIP) cybersecurity reliability standards, which are written to ensure the security and reliability of grid planning and operations. Entities with assets or operations that meet the defined Bulk Electric System scope are mandated to comply with the NERC CIP standards for the data, assets, and systems in-scope of the standards.

Through Reliability Technical Conferences, FERC promoted discussion of how standards can evolve to best leverage the benefits of a cloud environment effectively and securely for utility planning and operations.

FERC Staff report, FERC Commission Open Meeting, November 21, 2019

Cloud/Managed Security Service Provider*: This focus area acknowledges that as Entities explore how to deploy cloud and managed security service providers, it is critical that they do so in a secure manner. If implemented properly, the use of a trusted third party to perform common tasks and services can yield security benefits by allowing the Entity to focus on more complex issues in house and to optimize their security resources. However, more research needs to be conducted to determine if the most critical systems, such as those used for real-time operations, could be used in the cloud.*

In February 2020, they followed up with a Notice of Inquiry on Virtualization and Cloud Computing which collected input from interested stakeholders and trade organizations. At the end of 2020, FERC continued by directing NERC to submit an informational filing on the potential benefits and risks of virtualization and computing use to be submitted by the end of 2021.

"[T]here is general agreement in the NOI comments that the voluntary use of virtualization and cloud computing could provide significant benefits to users, owners and operators of the Bulk-Power System so long as the risks associated with these technologies are carefully addressed."

Work to understand and support cloud adoption exists within CIP drafting teams, which are following the Standards Development Process to assess and propose language

revisions, where appropriate. Industry approved revisions to CIP-004 and CIP-011 to enable and clarify use of BES Cyber System Information (BCSI) in the cloud in alignment with a NERC Practice Guidance that supports CIP auditors in assessing BCSI in the cloud in advance of the requirement revisions. The revisions are pending FERC approval.

Technical stakeholder working groups are also evaluating the use of cloud services relative to the requirement language and evidence obligations, and writing guidance to address how Responsible Entities can demonstrate compliance with the CIP standards when using cloud services. In June 2019, NERC endorsed guidance to rely on a third party's independent assessment as an acceptable means of identifying and assessing risk. (See NATF CIP-013-1 Implementation Guidance).

Security, Shared Responsibility and Inheriting Controls

Cloud security is a shared responsibility. The Shared Responsibility Model is fundamental to understanding the respective roles of the Entity and AWS in the context of the cloud security principles. AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. The Entity is responsible for the security of its data and systems in the cloud. This means that Entities retain control of the security program they choose to implement to protect their own content, applications, systems and networks, no differently than they would for applications in an on-site data center.

AWS operates, manages, and controls the IT components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate.

The division of responsibility depends on the functions performed by the cloud workloads and the services selected. Understanding the responsibility assignments between the Entity and AWS is an important part of the cloud adoption process. Entities also must consider that if they choose to leverage other third-party solutions to support their cloud environment, the shared responsibility model between the third-party and the customer may differ from the AWS Shared Responsibility model and may place additional security responsibilities on the Entity.

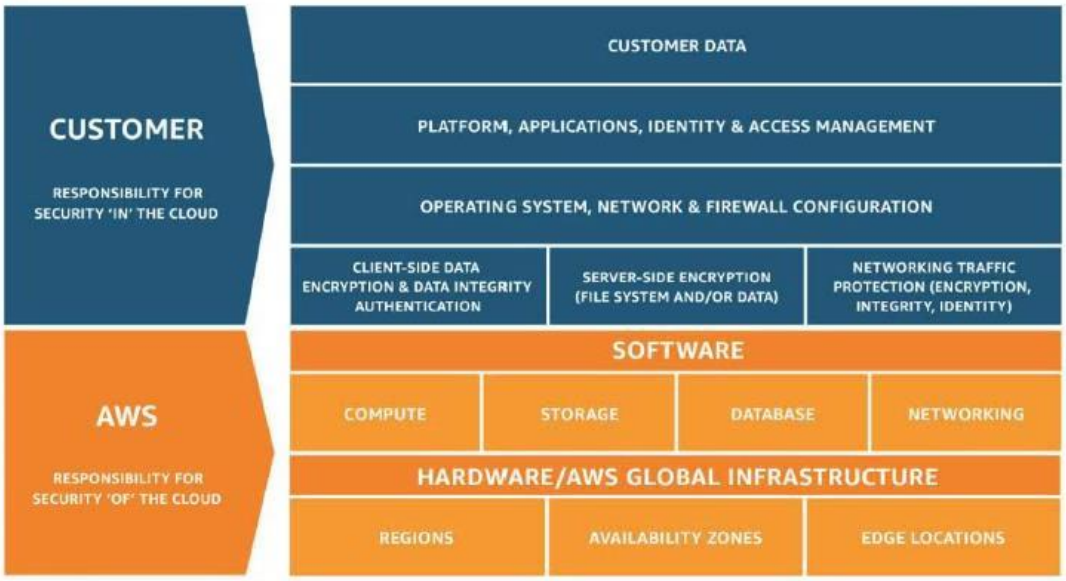


Figure 1: Shared *responsibility model*

In fulfilling CIP compliance, Entities are responsible for ensuring compliance with NERC CIP Standards. They manage security controls to fulfill CIP requirements like firewall configurations and networking traffic protection controls as applicable to their NERC CIP classified assets. AWS manages controls for the cloud infrastructure like the physical access control to AWS datacenters. Together, Entities and AWS share responsibility for performing security control activities.

Security OF the Cloud (AWS Responsibility)

To provide security of the cloud, AWS environments are continuously audited, and the infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and verticals, as described in the Security Assurance section. Entities can use these certifications to validate the implementation and effectiveness of AWS security controls, including internationally recognized security best practices and certifications. The AWS compliance program is based on the following actions:

- **Validate** that AWS services and facilities across the globe maintain a ubiquitous control environment that is operating effectively. The AWS control environment includes policies, processes, and control activities that leverage various aspects of the AWS overall control environment. The collective control environment encompasses the people, processes, and technology necessary toestablish and maintain an environment that supports the operating effectiveness of our control framework. AWS has integrated applicable cloud- specific controls identified by leading cloud computing industry bodies into the AWS control framework. AWS

monitors these industry groups to identify leadingpractices that can be implemented, and to better assist customers with managing their control environment.

- **Demonstrate** the AWS compliance posture to help customers verify compliance with industry and government requirements. AWS engages with external certifying bodies and independent auditors to provide customers with considerable information regarding the policies, processes, and controls established and operated by AWS. Customers can leverage this information toperform their control evaluation and verification procedures.
- **Monitor** that AWS provides a safe and secure environment and empowers its customers to secure their infrastructure through the use of thousands of security control requirements.

Compliance Programs

The AWS Compliance Program helps customers to understand the robust controls in place at AWS to maintain security and compliance in the cloud. By tying together governance-focused, audit-friendly service features with applicable compliance or audit standards, AWS Compliance Enablers build on traditional programs, helping customers to establish and operate in an AWS security control environment.

IT standards we comply with are broken out by Certifications and Attestations; Laws, Regulations and Privacy; and Alignments and Frameworks. Compliance certifications and attestations are assessed by a third-party, independent auditor and result in a certification, audit report, or attestation of compliance. AWS customers remain responsible for complying with applicable compliance laws, regulations and privacy programs. Compliance alignments and frameworks include published security or compliance requirements for a specific purpose, such as a specific industry or function.

AWS supports more security standards and compliance certifications than any other offering, including PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171, helping customers satisfy compliance requirements for virtually every regulatory agency around the globe.

AWS Artifact

Customers can review and download reports and details about more than 2,500 security controls on demand by using AWS Artifact, the self-service audit artifact retrieval portal available in the AWS Management Console.

The security objectives underlying the controls required by these security assurance

programs are consistent with the CIP security objectives, and are rigorously audited and certified on a regular basis by cloud security experts. Entities can help meet the CIP security objectives for cloud infrastructure through inherited controls managed by AWS and by leveraging AWS tools that empower users to secure their cloud environments.

Some of the assurance programs of particular interest to NERC regulated Entities are:

- **FedRAMP** – A U.S. government program for ensuring standards in security assessment, authorization, and continuous monitoring. AWS offers FedRAMP-compliant services that have been granted authorizations for high and moderate impact levels, have been assessed by an accredited independent Third-Party Assessment Organization (3PAO), and maintain the continuous monitoring requirements of FedRAMP. The continuous monitoring requirements are based on the National Institute of Standards and Technology Special Publication (NIST SP) 800-137 Information Security Continuous Monitoring for Federal Information Systems and Organizations as described in the FedRAMP Continuous Monitoring Strategy Guide. AWS Regions are FedRAMP authorized (four Regions comprising the AWS East-West Regions are FedRAMP Moderate; two GovCloud Regions are FedRAMP High). The authorized AWS services are posted under the service description for AWS on FedRAMP Marketplace.
- **SOC** – AWS Service Organization Control (SOC) Reports are independent,third-party examination reports that demonstrate how AWS addresses key compliance controls and objectives. The purpose of these reports is to helpEntities and their auditors understand the AWS controls established to support customers' operations and compliance. AWS issues SOC 1, SOC 2, and SOC 3 Reports twice per year, covering 6-month periods. New reports are released in mid-May and mid-November.

There are three types of AWS SOC Reports:

- **SOC 1** – Provides information about the AWS control environment that could be relevant to a customer's internal controls over financial reportingand as information for assessment and opinion of the effectiveness of internal controls over financial reporting (ICOFR).
- **SOC 2** – Provides customers and their service users that have a business need with an independent assessment of the AWS control environment thatis relevant to system security, availability, and confidentiality.
- **SOC 3** – Provides customers and their service users that have a business need with an independent assessment of the AWS control environment thatis relevant to system security, availability, and confidentiality, without disclosing AWS internal information.
- **ISO 27001** – ISO 27001 is a security management standard that specifies security

management best practices and comprehensive security controls following the ISO 27002 best practice guidance. The basis of this certification isthe development and implementation of a rigorous security program, including the development and implementation of an Information Security Management System which defines how AWS perpetually manages security in a holistic, comprehensive manner.

- **ISO 27017** – ISO 27017 provides guidance on the information security aspectsof cloud computing, recommending the implementation of cloud-specific information security controls that supplement the guidance of the ISO 27002 and ISO 27001 standards. This code of practice provides additional informationsecurity controls and implementation guidance specific to cloud service providers.
- **ISO 27018** – ISO 27018 is a code of practice that focuses on protection of personal data in the cloud. It is based on ISO information security standard 27002 and provides implementation guidance on ISO 27002 controls applicableto public cloud Personally Identifiable Information (PII). It also provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements, which is not addressed by the existing ISO 27002 control set.
- **NIST Cyber Security Framework** – Whether assessing a cloud service provider like AWS, establishing priorities for traditional technology purchases, ordetermining gaps in staffing and skills, the CSF can serve as the common ground to meet security and compliance objectives for the entire organization. Many technology providers have already mapped their services and products tothe NIST CSF, thereby streamlining assessments, acquisition, and compliance, and at a lower cost.

AWS is compliant with several security standards including SOC 1, 2, and3, and FedRAMP moderate and high. The security of AWS data centers isreviewed and audited as a part of these and many other compliance programs. Customers can download audit reports associated with these compliance programs by signing into the **AWS Management Console** and navigating to Artifact. These audit reports can be presented to customer's auditors as evidence of compliance/meeting standards.

An Entity's compliance team can incorporate AWS certifications, attestations, and audit standards into their own audit programs to help support their compliance with requirements. For more information about certifications and attestations from AWS, see the AWS Compliance Center.

Security IN the Cloud (Entity Responsibility)

Entities are responsible for security **in** the cloud and ensuring security for their regulated assets, including management of the guest operating system (such as installing updates and security patches) and other associated application software, as well as the configuration of the AWS provided security group firewall. For example, to satisfy requirements for account configuration, management and reviews for assets managed in the cloud, Entities can use services such as AWS Identity and Access Management (IAM) to configure and manage user access and privileges.

Entities should carefully consider the services they choose, as their responsibilities vary depending on the services they use, the integration of those services into their IT environments, and applicable laws and regulations. Entities are encouraged to use the AWS resources available to select and implement cloud services (see section on AWS Well-Architected Framework).

When using AWS services, Entities maintain control over their content and are responsible for managing the configuration of their security controls, including:

- Selection of the AWS services and security features used by the Entity.
- The country where their content is stored.
- The format and structure of their content and whether it is masked,anonymized, or encrypted.
- Whether their data is encrypted at rest or in transit and how keys are managed.
- Who has access to their content and how those access rights are granted, managed, and revoked.
- Defining availability requirements and building a resilient architecture to meet those requirements.

Some NERC CIP requirements are addressed by Entity specific policies, plans or processes and are managed by the Responsible Entity, among them the asset classification process of CIP-002; the overarching policies required in CIP-003; and the incident response plans of CIP-008. Cloud services may be used to support performance of these controls, but Entities will follow their compliance program to meet these requirements and should update governing documents to accommodate cloud services, as appropriate.

Inherited Controls

Entities can inherit the controls that provide security **of** the cloud infrastructure. AWS infrastructure is architected to be flexible and secure and meet the security requirements for highly sensitive organizations such as military, global banks and the power & utility industry. As noted earlier, AWS infrastructure and services meet thousands of security requirements embodied within a multitude of security assurance

programs and are verified through audit and continuous monitoring. The same secure hardware and software that meets requirements for top-secret workloads is available to all AWS customers.

An example of a control that an Entity will inherit by deploying workloads into AWS is the restricted physical access controls AWS implemented for its datacenters. Physical access to all AWS data centers housing IT infrastructure components is restricted to authorized data center employees, vendors, and contractors working for AWS who require access in order to execute their jobs. Access to facilities is only permitted at controlled access points that require multi-factor authentication designed to prevent tailgating and to ensure that only authorized individuals enter an AWS data center. On a quarterly basis, access lists and authorization credentials of personnel with access to AWS data centers are reviewed by the respective data center Area Access Managers (AAM). In addition, due to the nature of cloud computing, customer data is not assigned to specific servers in datacenters and is protected from unauthorized logical access, enhancing physical security.

Please see the Appendix: AWS Services and Alignment to NERC CIP to review a table that details shared responsibilities and inherited controls, and illustrates how they apply by CIP standard and requirement.

AWS provides a wide range of information to customers about the AWS control environment through technical papers, reports, certifications, and other third-party attestations. This documentation helps customers to understand the controls in place, relevant to the AWS services they use, and how those controls have been validated. This information also helps customers account for and validate that controls in their extended IT environment are operating effectively. To learn more about meeting security and compliance goals using AWS infrastructure and services Best Practices for Security, Identity, & Compliance.

Resources for Entities

While Entities are responsible for securing their workloads in the cloud, AWS offers support and expertise in designing a secure cloud architecture that meets their needs. AWS has resources available to help Entities determine the architecture and security controls for their NERC CIP workloads.

AWS developed the Well-Architected Framework to assist customers in defining the best approaches to meet security and reliability objectives. The Well-Architected Framework is based on five pillars—operational excellence, security, reliability, performance efficiency, and cost optimization. The pillars provide a consistent approach

for Entities, customers, and partners to evaluate and implement architectures that can be standardized and replicated across workloads. Entities can use the AWS Well-Architected Tool to review the state of their workloads and compare them to the latest AWS architectural best practices. AWS Solutions Architects are available to provide guidance for making improvements in alignment with the Entity's business objectives, workloads, and goals.

The AWS Cloud Adoption Framework (AWS CAF) is designed to help Entities develop and execute efficient and effective plans for their cloud adoption journey. The guidance and best practices provided by the framework help customers build a comprehensive approach to cloud computing across their organization, and throughout their IT lifecycle. AWS CAF organizes guidance into six areas of focus, called perspectives. These perspectives cover distinct responsibilities owned or managed by functionally related stakeholders. In general, the Business, People, and Governance Perspectives focus on business capabilities; while the Platform, Security, and Operations Perspectives focus on technical capabilities. The AWS CAF breaks down the complicated process of planning into manageable areas of focus.

Entities can also engage with AWS Security Competency Partners to help elevate and enhance their security in the cloud. AWS Security Competency Partners specialize in delivering security-focused solutions for specific workloads and use cases including software-as-a-service (SaaS) products to help secure data with solutions available for a wide range of workloads and use cases.

Beyond the AWS Well-Architected Framework, AWS CAF, and AWS Security Competency Partners, there are many free resources available for customers to leverage during their cloud adoption journey, including whitepapers listed in the Additional Resources section of this paper, computer-based trainings and AWS Workshops.

Implementing Controls to Support Security and Compliance Objectives

Implementing solutions on AWS cloud provides Entities with a highly scalable and resilient infrastructure built with cloud security expertise. It enables Entities to provide governance at scale, enhance their security capabilities, demonstrate compliance requirements, and implement reliability through use of a range of services and automation.

AWS Infrastructure

AWS Global Cloud Infrastructure is secure, extensive, and reliable, offering over 200 fully featured services from data centers globally which includes seven regions in North America, two of which are GovCloud regions in the United States. GovCloud AWS Gov or Government Cloud is architected and designed to address specific regulatory and compliance requirements of U.S. government agencies at the federal, state, and local level. AWS GovCloud regions are authorized as FedRAMP High and also adhere to U.S. International Traffic in Arms Regulations (ITAR), and Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG) Impact Levels 2, 4, and 5, among other specific regulatory and compliance requirements. All other AWS regions in the U.S. are authorized as FedRamp moderate. Each of these regions are made of multiple availability zones which consist of multiple data centers. The AWS core infrastructure is built to satisfy the requirements of high-sensitivity organizations and each of the regions are built and operate with the same secure hardware and software.

AWS is constantly innovating keeping in mind its customer's security needs. With AWS Nitro, AWS completely re-imagined its virtualization infrastructure. Traditionally, hypervisors protect the physical hardware and bios, virtualize the CPU, storage, networking, and provide a rich set of management capabilities. With the Nitro System, AWS is able to break apart those functions, offload them to dedicated hardware and software, and reduce costs by delivering practically all of the resources of a server to your instances. The Nitro System provides enhanced security that continuously monitors, protects, and verifies the instance hardware and firmware. Virtualization resources are offloaded to dedicated hardware and software minimizing the attack surface. Finally, Nitro System's security model is locked down and prohibits administrative access to instances, eliminating the possibility of human error and tampering.

Entities can configure additional reliability by using various AWS services that are designed to offer high reliability and availability. For example, AWS S3 offers eleven 9s (99.999999999%) of durability by automatically storing data across multiple availability zones within the region an Entity selects. An Entity can configure S3 to encrypt this data using AWS KMS and replicate the data to another North American region for further reliability. AWS Aurora is a MySQL and PostgreSQL compatible database service that replicates data across availability zones and regions based on user configuration. AWS also offers Amazon RDS, a service that offers common relational databases like MS SQL Server and Oracle with the ability to store data across multiple availability zones. Entities can build highly available and reliable systems by utilizing such AWS services that are supported by its geographically distributed infrastructure.

Automation

Automating security best practices is simplified by using cloud services. All AWS capabilities and actions can be accessed via Application Programming Interfaces (APIs), access to which is controlled by the AWS Identity and Access Management

(IAM) service. These APIs enable an Entity to automate the creation, management, control, and monitoring of the cloud networks, security, access management, servers, storage, and backups. Activities performed are logged in the AWS CloudTrail service. Security automation enables Entities to have a proactive incident response capability by automating deny by default functions and other security-based measures, providing the ability to reduce the scope and impact of security events.

Entities can use AWS CloudFormation to model a collection of related AWS resources, provision them quickly and consistently, and manage them throughout their lifecycles, by treating infrastructure as code. CloudFormation templates can be used to describe and launch an entire network, its subnets, route tables, security (NACLs and Security Group rules), and EC2 instances. Further, CloudFormation can be used to install and configure software into the EC2 instances, configure and establish VPN connections, and launch and configure most AWS services using automation.

Once a CloudFormation stack is defined it can be rerun to generate identical environments. This enables the creation of test and development environments in minutes to hours versus weeks to months. It is also designed to enable restoration of an Entity's entire cloud infrastructure on demand with minimal effort, which is valuable for high availability, continuity of operations, and enabling disaster recovery (whether an exercise or a real event).

The automation AWS offers supports Entities' overall security and compliance programs, specifically in the areas of identity and access management (CIP-004), security event monitoring (CIP-007), incident response (CIP-008), recovery (CIP-009), and establishing and maintaining baselines (CIP-010).

Governance at Scale

Entities start building their CIP compliance with CIP-002 asset classification to identify the systems in scope and apply the risk impact level of high, medium, or low depending on which CIP-002 definition fits. AWS recommends that systems with different risk profiles and purpose be separated by using multiple accounts. This approach helps implement and demonstrate segregation of responsibility and limits the risk to any system from another, while also enabling a central source for account management. This collection of accounts to run workloads, and to log, monitor, control access, and implement common security is referred to as an AWS Landing Zone.

Several AWS services enable Entities to manage their Landing Zone:

- AWS Organizations helps you centrally manage and govern your environment as

you grow and scale your AWS resources. Using AWS Organizations, you can programmatically create new AWS accounts and allocate resources, group accounts to organize your workflows, apply policies to accounts or groups for governance, and simplify billing by using a single payment method for all of your accounts. In addition, AWS Organizations is integrated with other AWS services so you can define central configurations, security mechanisms, audit requirements, and resource sharing across accounts in your organization.

- AWS Organizations Service control policies (SCPs) are a type of organization policy that you can use to manage permissions in your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization. SCPs help you to ensure your accounts stay within your organization's access control guidelines.

- AWS Control Tower is a service that enables an Entity to set up and govern a secure, multi-account AWS environment. Control tower simplifies account management by offering blueprints to provide identity management, federate access to accounts, centralize logging, establish cross-account security audits, define workflows for provisioning accounts, and implement account baselines with network configurations. With Control Tower an Entity can implement mandatory and strongly recommended high-level rules, called guardrails that help enforce its policies using service control policies (SCPs), or detect policy violations using AWS Config rules.

In addition to AWS Landing Zone, there are several AWS services that support Entities in achieving security and audit objectives at scale, including:

- AWS Audit Manager helps an Entity continuously audit its AWS usage to simplify how they assess risk and compliance with regulations and industry standards. Audit Manager automates evidence collection to reduce the "all hands-on deck" manual effort that often happens for audits and enables an Entity to scale its audit capability in the cloud as its business grows. With Audit Manager, it is easy to assess if policies, procedures, and activities – also known as controls – are operating effectively. When it is time for an audit, AWS Audit Manager helps an Entity manage stakeholder reviews of their controls and enables it to build audit-ready reports with much less manual effort.

- AWS Firewall Manager is a security management service which enables Entities to centrally configure and manage firewall rules across their accounts and applications in AWS Organizations. As new applications are created, Firewall Manager makes it easy to bring new applications and resources into compliance by enforcing a common set of security rules. With Firewall Manager, Entities have a single service

to build firewall rules, create security policies, and enforce them in a consistent, hierarchical manner across their entire infrastructure, from a central administrator account.

- AWS Systems Manager Inventory enables an Entity to manage and control security of their assets in the cloud by providing visibility into their Amazon Elastic Compute Cloud (Amazon EC2) servers and on-premises computing environment. An Entity can use Systems Manager Inventory to collect metadata from their managed instances, store the metadata in a central Amazon Simple Storage Service (Amazon S3) bucket, and then use built-in tools to query the data and quickly determine which instances are running the software and configurations required by the software policy, and which instances need to be updated. To assist customers in managing their cloud assets in a manner that meets NERC CIP requirements, AWS permits customers to assign metadata to their AWS resources in the form of tags to document the BES cyber categorization of regulated workloads in the cloud.
- Amazon CloudWatch can be configured to automatically create events when certain conditions are met in AWS CloudTrail logs and in logs collected from your servers using the CloudWatch Agent. These events can be used to triggerremedial actions and notifications to you.
- AWS Systems Manager Session Manager provides secure and auditable instance management without the need to open inbound ports, maintain bastionhosts, or manage SSH keys. Session Manager also makes it easy to comply with corporate policies that require controlled access to instances, strict securitypractices, and fully auditable logs with instance access details, while still providing end users with simple one-click access to your Amazon EC2 instances (Virtual Machines).

  The following sections show how customers using AWS Cloud services fulfill the security objectives addressed in the NERC CIP standards.

Identity and Access Management

CIP-004, *Personnel and Training*, includes requirements around access authorization, audit, and revocation. In the cloud, these requirements can be addressed by managing access to perform cloud configuration and management activities (AWS Management Console); remote access to servers in the cloud (SSH and RDP access to EC2 instances); and end user access to applications. AWS offers several services tomanage users in all these categories to granular levels.

Access to perform cloud configuration and management activities is managed by AWS Identity and Access Management (IAM). IAM enables access management, authorization, verification of access privileges, and access revocation to AWS service

APIs, AWS Management Console, and to specific resources. Using IAM, Entities can create users, roles, groups and assign fine grained permissions. Entities can use their existing SAML 2.0 compatible directory services such as Microsoft Active Directory to integrate with IAM by mapping their users or groups to IAM roles. Entities can also choose to only use IAM and AWS Single Sign-On (SSO) service for access management. These services simplify access management by providing a single point to manage users, access, and decommissioning processes. For example, password configuration controls (complexity, length, expiration) can be managed in IAM or in your existing directory service that will integrate with IAM.

AWS IAM offers Access Analyzer to review existing access so that an Entity can identify and remove unintended external or unused permissions. IAM Access Analyzer also uses automated reasoning to generate comprehensive findings for resources that can be accessed from outside an AWS account. For this analysis, IAM Access Analyzer continuously monitors for new or updated resource policies and analyzes permissions granted for Amazon S3 buckets, AWS KMS keys, Amazon SQS queues, IAM roles, AWS Lambda functions, and AWS Secrets Manager secrets.

In the cloud an Entity's team of systems administrators can access EC2 instances over SSH or RDP. Entities can manage this administrative access to theirAmazon EC2 instances using their existing directory service, AWS Directory Service for Microsoft Active Directory (also known as AWS Managed Microsoft AD). In addition, AWS offers Session Manager as a means to connect to or run commands on EC2 instances without the need to open ports for SSH and RDP. Access to Session Manager is granted via AWS IAM. Entities are responsible for configuring user access on their EC2 instances, and providing access to Session Manager via IAM permission policies.

End user access to information on AWS can continue to be controlled by the customer's existing directory service and access controls by integrating with IAM, or applications on AWS, or with Amazon Cognito. Amazon Cognito supports customer end-user sign-up, sign-in, and access control to their web and mobile applications.

Data Protection

Entities can meet their requirements for protecting data throughout the lifecycle, for data at-rest, in-transit and in-use (CIP011-2, *Information Protection*). AWS is committed to offering its customers Data Control, Data Privacy, Data Sovereignty, and Data Security.

Entities have complete control over their data on AWS through the use of AWS services and tools that allow them to determine where their data will be stored, how it is secured, and who has access. Services such as AWS Identity and Access Management (IAM)

allow Entities to securely manage access to AWS services and resources. AWS Key Management Service (KMS) and AWS CloudHSM allow Entities to securely generate and manage encryption keys. AWS personnel are unable to export or use customer keys.

AWS Key Management Service (AWS KMS) is a fully managed, highly available service. Key management and cryptographic functions are integrated with most AWS services. AWS KMS presents a single control point to manage keys and define policies consistently across integrated AWS services and your own applications. Entities can easily create, import, rotate, delete, and manage permissions on keys from the AWS Management Console or by using the AWS SDK or CLI. AWS KMS is integrated with AWS services to simplify using your keys to encrypt data across your AWS workloads. Entities choose the level of access control needed, including the ability to share encrypted resources between accounts and services. KMS logs all use of keys to AWS CloudTrail to give you an independent view of who accessed your encrypted data, including AWS services using them on your behalf.

Customers have the option to use AWS CloudHSM, a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud. With CloudHSM, Entities can manage their own encryption keys using FIPS 140-2 Level 3 validated HSMs. CloudHSM offers you the flexibility to integrate with your applications using industry-standard APIs, such as PKCS#11, Java Cryptography Extensions (JCE), and Microsoft CryptoNG (CNG) libraries. Utilizing HSMs as the root of trust helps you demonstrate compliance with security, privacy and anti-tamper regulations such as HIPAA, FedRAMP and PCI.

Alternatively, customers can maintain local control over their keys by importing keys from an on- premises key management and HSM solution and still take advantage of KMS features. Updates to the AWS KMS HSM firmware are controlled by multi-party access control that is audited and reviewed by an independent group within Amazon as well as a NIST accredited lab in compliance with FIPS 140-2.

For data privacy AWS provides a wide variety of best practice documents and guidance that Entities can leverage to help protect their data. AWS does not use or share customer data without their agreement as described in the AWS Customer Agreement. AWS has achieved certifications and accreditations such as ISO 27017 for cloud security and ISO 27018 for cloud privacy.

For data sovereignty, Entities choose the AWS region in which they wish to store data. Entities can use AWS services with the confidence that their data stays in the AWS Region they select. AWS will not access or use Your Content except as necessary to maintain or provide the Service Offerings, or as necessary to comply with the law or a

binding order of a governmental body. Entities retain ownership and control of their content along with the ability to encrypt it, protect it, move it, and delete it in alignment with their organization's security policies. Encryption is strongly recommended for Entities that store data (data-at-rest) on AWS storage services or transit (data-in-transit) AWS networks.

Security in the cloud is a shared responsibility between AWS and our customer. Entities can improve their ability to meet core security, confidentiality, and compliance requirements with AWS' comprehensive services, whether through Amazon GuardDuty, or the AWS Nitro System, the underlying platform for our EC2 instances. In addition, services such as AWS CloudHSM and AWS Key Management Service allow Entities to securely generate and manage encryption keys, and AWS Config and AWS CloudTrail deliver monitoring and logging capabilities for compliance and audits.

While there are multiple ways for Entities to protect data in-use, one option is using AWS Nitro Enclaves for processing of sensitive workloads. Nitro Enclaves help customers reduce the attack surface area for their most sensitive data processing applications. Enclaves offer an isolated, hardened, and highly constrained environment to host security-critical applications. Nitro Enclaves include cryptographic attestation for software an Entity may choose to run, to confirm that only authorized code is running. As well, Nitro Enclaves integrate with the AWS Key Management Service, so that only the Entity's enclaves can access sensitive material.

AWS follows standards to install, service, and eventually destroy devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored Entity data is not removed from AWS control until it has been securely decommissioned. Entities can further protect their data by using encryption (AWS KMS) for Amazon EBS volumes or use third-party software to wipe storage media before reuse or decommissioning.

Logical Isolation and Secure Networking

Entities can restrict communications (CIP-005, *Electronic Security Perimeter*) and mitigate threats from malicious communications by using Amazon Virtual Private Cloud (Amazon VPC) to define their cloud network, limit exposure to the internet, inspect, protect, and control all network traffic.

The AWS Web Application Firewall (WAF) helps protect web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. Using AWS WAF, Entities can create custom rules that

block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for your specific application.

Entities can further protect their VPCs on AWS by using AWS Network Firewall a service that provides protection from common network threats. AWS Network Firewall's stateful firewall can incorporate context from traffic flows, like tracking connections and protocol identification, to enforce policies such as preventing your VPCs from accessing domains using an unauthorized protocol.

AWS Network Firewall's intrusion prevention system (IPS) provides active traffic flow inspection so you can identify and block vulnerability exploits using signature-based detection. AWS Network Firewall also offers web filtering that can stop traffic to known bad URLs and monitor fully qualified domain names. Entities can also benefit from the automatic protections of AWS Shield, to defend against the most common, frequently occurring network and transport layer DDoS attacks that target their web site or applications.

Configuration, Vulnerability, and Patch Management

Entities can address their security objectives for configuration change management, vulnerability management (CIP-010, *Configuration Change Management and Vulnerability Assessment*), and patching and malicious code protection (CIP-007, *Systems Security Management*), using AWS services.

On AWS, Entities can use template definition and management tools, such as AWS CloudFormation, to create standard, preconfigured cloud environments. AWS CloudFormation supports the use of automated templates to reduce manual errors when building new devices to accepted baselines. AWS CloudFormation allows an Entity to detect configuration drift when changes are made through the service, which is one way that entities could identify unauthorized baseline changes, or perform baseline reviews.

AWS Config enables customers to assess, audit, and evaluate the configurations of their AWS resources against desired configurations simplifying the baseline review and change management process. AWS Config rules offer dynamic compliance checking by allowing you to detect a change to your cloud configuration, remediate, and notify you of the event in real time. The event notifications are another way that an Entity could identify unauthorized baseline changes.

AWS offers a range of tools to allow Entities to move quickly while still ensuring that cloud resources comply with organizational standards, best practices, and regulatory requirements. Amazon Inspector is a security assessment service that automatically assesses applications for vulnerabilities or deviations from best practices, including

impacted networks, OS, and attached storage. Deployment tools can be used to manage the creation and decommissioning of AWS resources according to organization standards.

Many AWS partners offer third-party host-based detection software for protection against malicious code, or third-party vulnerability assessment tools to scan their servers on AWS that can be used to address the CIP-010 vulnerability assessment requirements.

On AWS, Entities can use third-party software for patch management or they can use AWS Systems Manager Patch Manager to automate the process of patching managed instances with both security related patches and other types of updates.

Security Event Monitoring

CIP-007, *Systems Security Management*, includes requirements for security event monitoring. Security events are generated from API calls, application/server logs, and AWS services. All actions on AWS are a web service call supported by an AWS API. These API calls are logged when AWS CloudTrail is enabled. This approach offers deep visibility into API calls including who, what, when, and from where calls were made. Log aggregation options are available to help streamline investigations and compliance reporting, and alert notifications can be configured through Amazon CloudWatch when specific events occur or thresholds are exceeded. These tools and features provide an Entity the visibility needed to spot issues before they impact the business and allow them to improve security posture, support compliance, and reduce the risk profile of their environment.

In addition, Entities can collect application and server logs from their servers and send them to Amazon CloudWatch where they can create alarms that send notifications. Entities can use AWS Lambda to implement remedial actions when an alarm is triggered. This approach offers Entities with the ability to go beyond monitoring to detect and remediate events in near real time.

Most AWS services also generate logs specific to their function. For example, by enabling VPC flow logs, an Entity can gain visibility on traffic within a VPC. Event monitoring and detection can be performed using Amazon GuardDuty, a threat detection service that continuously monitors for malicious activity and unauthorized behavior. The service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats from events across multiple AWS data sources, such as AWS CloudTrail, Amazon VPC Flow Logs, and DNS logs. By integrating with Amazon CloudWatch Events, GuardDuty alerts are actionable, easy to aggregate across multiple accounts, and straightforward to push into existing event

management and workflow systems. An Entity can use Amazon Detective to further analyze and investigate logs and GuardDuty events to quickly identify the root cause of potential security issues or suspicious activities. Amazon Detective automatically collects log data from your AWS resources and uses machine learning, statistical analysis, and graph theory that enables you to easily conduct faster and more efficient security investigations.

AWS Security Hub offers a comprehensive view of security alerts and security posture across an Entity's AWS accounts. There are a range of powerful security tools at an Entity's disposal, from firewalls and endpoint protection to vulnerability and compliance scanners that can leave teams switching back-and-forth between these tools to deal with hundreds, and sometimes thousands, of security alerts every day. With Security Hub, an Entity has a single place to aggregate, organize, and prioritize security alerts, or findings, from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector, AWS Identity and Access Management (IAM) Access Analyzer, AWS Systems Manager, and AWS Firewall Manager, as well as from AWS Partner Network (APN) solutions.

Application Manager, a capability of AWS Systems Manager, helps system administrators investigate and remediate issues with their AWS resources in the context of their applications. Application Manager aggregates operations information from multiple AWS services and Systems Manager capabilities to a single AWS Management Console. In Application Manager, an application or cyber system is a logical group of AWS resources that an Entity wants to operate as a unit. Application Manager imports metadata about all the AWS resources organized into resource groups. Application Manager also automatically imports metadata about resources that were created by AWS CloudFormation, Amazon Elastic Kubernetes Service (Amazon EKS), and AWS Launch Wizard. Once this metadata is collected, Application Manager provides a single dashboard to display alarms triggered by Amazon CloudWatch, compliance information provided by AWS Config and Systems Manager State Manager, Kubernetes cluster information provided by Amazon EKS, log data provided by AWS CloudTrail and Amazon CloudWatch Logs, information provided by Systems Manager OpsCenter, and resource details provided by the AWS services that host them.

Incident Response

Entities require an organized approach to managing the investigation and response to potential and confirmed incidents. CIP-008, *Incident Reporting and Response Planning*, defines requirements for planning, reporting and managing incident response, recovery and reconstitution. AWS incident response practices, policies and programs that include incident response testing, are evaluated by independent, third-party assessors as part

of assurance programs.

AWS also offers customers various tools and services that enable them to implement their incident response strategy, and monitor and investigate events. The AWS Security Incident Response Guide provides details and strategies that customers can use to meet their security standards.

Resilience and System Recovery

Resilience and availability are paramount to grid reliability, and the AWS Cloud infrastructure provides valuable resources in support. The AWS infrastructure is architected to minimize outages and incidents, and, should a disruption occur, is built to limit impact on customers and maintain continuity of services.

AWS builds its data centers in multiple geographic regions. Each region consists of multiple Availability Zones (AZs). Currently within North America, AWS has 7 Regions, including 2 GovCloud Regions, and 25 AZs. These AZs offer customers the ability to operate production applications and databases at higher availability, fault tolerance, and scalability than would be possible from a single data center as well as offering maximum resiliency against system disruption. For current information on AWS Regions and Availability Zones, see Global Infrastructure.

Documenting and testing recovery plans is critical to meeting the availability and resilience objectives for any organization. CIP-009, *Recovery Plans for BES Cyber Systems*, defines requirements for recovery planning, backup, and testing. Customers can use AWS services such as AWS Backup and CloudEndure Disaster Recovery to build and deploy highly available and resilient applications. Based on Recovery Time Objectives (RTOs), Entities can choose to deploy their systems in a single AWS Region across multiple Availability Zones or even across Regions with instant or near instant failover. Entities can use the AWS best practice of using automation to deploy their applications enabling fast and low-cost testing of disaster recovery processes.

Remote, Edge, and On-Premises Computing

Entities can have BES cyber assets and systems distributed between data centers, generation facilities, substations, control centers, and along transmission assets. Keeping consistency in technology across all these locations and maintaining secure and zero trust communications between all these assets is critical for BES operations. AWS offers several products and services an Entity can use to securely meet these distributed computing and data acquisition requirements. AWS Outposts is a fully managed service that offers the same AWS infrastructure, AWS services, APIs, and

tools to virtually any datacenter, co-location space, or on-premises facility for a truly consistent hybrid experience. AWS Outposts is ideal for workloads that require low latency access to on-premises systems, local data processing, data residency, and migration of applications with local system interdependencies. AWS compute, storage, database, and other services run locally on Outposts, and an Entity can access the full range of AWS services available in the Region to build, manage, and scale their on-premises applications using familiar AWS services and tools.

AWS Snowball Edge Compute Optimized devices provide 52 virtual central processing units (vCPUs), block and object storage, and an optional graphics processing unit (GPU) for use cases like advanced machine learning and full motion video analysis in disconnected environments. Entities can use these devices for data collection, machine learning and processing, and storage in environments with intermittent connectivity or in extremely remote locations. These devices may also be rack mounted and clustered together to build larger installations. Snowball supports specific Amazon EC2 instance types and AWS Lambda functions, so Entities can develop and test in the AWS Cloud, then deploy applications on devices in remote locations to collect and process data.

AWS IoT offers services for industrial solutions while offering services for all layers of security, including preventive security mechanisms, like encryption and access control to device data, and a service to continuously monitor and audit configurations. Connectivity to devices is secured using x.509 certificates and services like AWS IoT Device Defender help secure a fleet of Industrial IoT devices. AWS IoT Device Defender continuously audits IoT configurations to make sure that they aren't deviating from security best practices and continuously monitors and detects unusual device behaviors that may be indicative of a compromise. AWS IoT Device Management makes it easy to securely register, organize, monitor, and remotely manage IoT devices at scale. With AWS IoT Secure Tunneling, you can securely connect to industrial IoT devices behind restricted firewalls at remote sites for troubleshooting, configuration updates, and other operational tasks. AWS IoT Jobs can be used to define a set of remote operations that are sent to and executed on one or more IIoT devices connected to AWS IoT such as software and firmware updates.

AWS Certificate Manager (ACM) is a managed service on AWS that can generate and sign X.509 certificates in the cloud. The flexibility of ACM allows Entities to bring their own CA and perform certificate signing operations on AWS. AWS protects the physical infrastructure where the CA is held on the ACM service, and the Entity is responsible for enacting appropriate policies for users that have access to the ACM service in their account.

Physical Security

CIP-006, *Physical Security of BES Cyber Systems*, requires each Responsible Entity to implement a documented physical security plan(s) that covers security measures such as physical access controls, and logging and monitoring of access (authorized and unauthorized). Entities inherit the AWS data center controls that physically secure the cloud infrastructure by strictly controlling access at the perimeter, at building ingress points, and to the data center floors. AWS is continuously innovating the design and systems of its data centers to protect them from man-made and natural risks. AWS data centers are made up of layers each implementing access control and security and undergoes third-party audits to confirm security and compliance.

AWS data center physical security begins at the **Perimeter Layer**. This Layer includes a number of security features depending on the location, such as security guards, fencing, security feeds, intrusion detection technology, and other security measures. AWS restricts physical access to people who need to be at a location for a justified business reason. Employees and vendors who have a need to be present at a data center must first apply for access and provide a valid business justification. If access is granted, it is revoked once necessary work is completed. When approved individuals are on site, they are given a badge that requires multi-factor authentication and limits access to pre-approved areas. AWS employees who routinely need access to a data center are given permissions to relevant areas of the facility based on job function. Staff lists are routinely reviewed by an area access manager to ensure each employee's authorization is still necessary.

The **Infrastructure Layer** is the data center building and the equipment and systems that keep it running. Components like back-up power equipment, the HVAC system, and fire suppression equipment are all part of the Infrastructure Layer. These devices and systems help protect servers and, ultimately, customer data. AWS implements strict access controls for each layer of its infrastructure. Access to the Infrastructure Layer is restricted based on business need. By implementing a layer-by-layer access review, the right to enter every layer is not granted by default. Access to any particular layer is only granted if there is a specific need to access that specific layer. Water, power, telecommunications, and internet connectivity are designed with redundancy, so AWS can maintain continuous operations in an emergency. Electrical power systems are designed to be fully redundant so that in the event of a disruption, uninterruptible power supply units can be engaged for certain functions, while generators can provide backup power for the entire facility. People and systems monitor and control the temperature and humidity to prevent overheating, further reducing possible service outages.

The **Data Layer** is the most critical point of protection because it is the only area in an

AWS data center that holds customer data. Protection begins by restricting access and maintaining a separation of privilege for each layer. In addition, AWS deploys threat detection devices, video surveillance and system protocols, further safeguarding this layer. There are mandatory procedures to obtain authorization to enter the Data Layer. This includes review and approval of a person's access application by authorized individuals. Meanwhile, threat and electronic intrusion detection systems monitor and automatically trigger alerts of identified threats or suspicious activity.

Access points to server rooms are fortified with electronic control devices that require multi-factor authorization. To prevent technological intrusion, AWS servers can warn employees of any attempts to remove data. In the unlikely event of a breach, the server is automatically disabled. Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life-cycle. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from AWS control until it has been securely decommissioned.

The **Environmental Layer** is dedicated to environmental considerations from site selection and construction to operations and sustainability. AWS carefully chooses data center locations to mitigate environmental risk, such as flooding, extreme weather, and seismic activity.

Planning Considerations for Use of Cloud Services

Each organization's cloud adoption journey is unique. To successfully migrate to the cloud, it is valuable to understand your organization's current state, the desired objectives, and the transition required to achieve those objectives. When setting goals, Entities should take a risk-based approach to implementing their internal security requirements on AWS.

In the development process, collaboration with NERC or Regional Entities' auditors can be important to gaining confidence with compliance. Opening dialogue, being transparent, and understanding auditor perspectives and expectations can help you set goals and create work streams that not only enable staff to thrive in the cloud, but also help define evidence needs to support compliance demonstration.

Entities are encouraged to use the resources available to implement cloud services like those described in the Resources for Entities section, and provided in the Additional

Resources Section. AWS would like to support Entities in their cloud adoption journey through personnel resources, immersion days, and game days. Entities are encouraged to contact their AWS Account Manager, or AWS Sales.

Contributors

Contributors to this document include:

- Ranjan Banerji, Principal Partner Solutions Architect, Power & Utilities, AWS
- Maggy Powell, Principal Industry Specialist, Power & Utilities, AWS Security
- Kristine Martz, Industry Specialist, Power & Utilities, AWS Security

Additional Resources

For additional information, see:

- NIST Cybersecurity Framework
- IDC Technology Spotlight – Cloud Adoption Unleashes Greater Value for Power and Utility Companies
- AWS Cloud Adoption Framework
- AWS Cloud Adoption Framework Security Perspective
- AWS Well Architected Framework
- AWS Well Architected Framework Security Pillar
- AWS Well Architected Framework IoT Lens
- Data Center Controls
- AWS Security Best Practices
- Ten Security Golden Rules for Industrial IoT Solutions
- AWS Incident Response
- AWS Answers to Key Compliance Questions
- AWS Logical Separation on AWS Whitepaper
- AWS Foundational Security Best Practice Controls
- Control Tower Best Practices
- Networking Multiple VPCs

- Power & Utility Path to Production Info Guide
- Executive's Guide to AWS Cloud Security
- Executive's Guide to AWS Security Control Domains

Document Revisions

Date	Description
January 2020	First publication
November 2021	Updated with additional content on AWS security and compliance services, aligned content with revisions to NERC CIP Standards

Appendix: AWS Services and Alignment to NERC CIP

The following table illustrates how AWS services and inherited controls can be used to help demonstrate compliance with NERC CIP and provides an overview of customer considerations for security **in** the cloud. For CIP Standards and Requirements that are an AWS Responsibility, further details about the controls that have been implemented can be found in the security assurance reports described previously.

CIP Standard Requirement Objectives	CIP Standard Description	AWS Services	Customer Considerations	AWS Responsibility
CIP-002-5.1a, R1	Identify and categorize cyber assets	AWS Tags AWS Organizations AWS Systems Manager Inventory	Entities can continue to follow their existing compliance program to identify and categorize cyber assets. Once assets are categorized, entities can assign metadata to their AWS resources in the form of tags to document the BES cyber categorization of regulated workloads in the cloud. Use of tags can enhance the categorization process and support automation of the recurring asset categorization reviews. Each tag is a simple label consisting of a customer-defined key and an optional value that can make it easier to manage, search for, and filter resources. Tags enable customers to categorize resources by purpose, owner, environment, or other criteria such as BES cyber system categorization. AWS Systems Manager Inventory	
CIP-002-5.1a, R2	Review and approve, every 15 months	AWS Tags AWS Organizations AWS Systems Manager Inventory		

			provides visibility into Amazon EC2 and on-premises computing environment. You can use Inventory to collect metadata from your managed instances. This metadata can be stored in a central Amazon S3 bucket, and queried using built-in tools to quickly determine which instances are running the software and configurations required by your software policy, and which instances need to be updated. You can configure Inventory on all of your managed instances by using a one-click procedure.	
CIP-003-8, R1	Cyber policies		Entities can continue to follow their existing compliance program for security management controls. Customer cyber policies and security plans should be reviewed to identify updates needed to address the use of cloud services.	AWS is responsible for the security of infrastructure of the cloud and has a shared responsibility to maintain security policies to address security of the cloud infrastructure. AWS security policies address controls such as security awareness training for AWS employees, physical and logical access control procedures, and incident response procedures. Customers can reference our assurance reports demonstrating our controls in the artifact section of the AWS Management Console.
CIP-003-8, R2	Security plans for low impact systems			
CIP-003-8, R3	Document CIP Senior Manager			
CIP-003-8, R4	CIP Senior Manager delegation			
CIP-003-8 Attachment 1, Section 1	Low impact BCS - Cybersecurity awareness		Entities can continue to follow their existing compliance program on security awareness and training, personnel security and access management	AWS is responsible for the security of the cloud infrastructure and has demonstrated compliance with multiple control frameworks, addressing controls

			controls requirements.	for security training and awareness, personnel security, and access management and authorization. AWS customers inherit these controls and can reference our assurance reports demonstrating the validity of our controls in the artifact section of the AWS Management Console.
CIP-003-8 Attachment 1, Section 2	Low impact BCS - Physical security controls			AWS is responsible for the security of the cloud infrastructure and has demonstrated compliance with multiple control frameworks, addressing controls for physical security. AWS customers inherit these controls and can reference our assurance reports demonstrating the validity of our controls in the artifact section of the AWS Management Console. Physical access to all AWS data centers housing IT infrastructure components is restricted to authorized data center employees, vendors, and contractors who require access in order to execute their jobs. Access to facilities is only permitted at controlled access points that require multi-factor authentication designed to prevent tailgating and to ensure that only authorized individuals enter an AWS data center. On a quarterly basis, access lists and authorization credentials of personnel

				with access to AWS data centers are reviewed by the respective data center Area Access Managers (AAM).
CIP-003-8 Attachment 1, Section 3	Low impact BCS - Electronic access controls	AWS Identity & Access Management (IAM) IAM Access Analyzer AWS Managed Directory Service Amazon Cognito AWS VPN AWS Direct Connect	Entities can manage user access, authorization, and revocation for administrative access to the AWS Management console using AWS IAM. AWS IAM offers the ability to implement fine grained permissions to users and roles. AWS IAM integrates with the customer's current SAML 2.0 compatible directory service. To manage access to servers (SSH and RDP) and end user access to services customers can use their existing directory service, AWS Directory Service, AWS IAM, and AWS Cognito. Entities can audit users, grant and revoke access to users using a combination of these tools. IAM Access Analyzer can be used to get a deeper insight into who or what system has access to AWS assets. Access Analyzer runs continuously and will	Remote access to AWS production environments is limited to defined security groups. The addition of members into a group must be reviewed and approved by authorized individuals who confirm the user's need for access to the environment. Remote access requires multi-factor authentication over an approved cryptographic channel for authentication. AWS employs automated mechanisms to facilitate the monitoring and control of remote access methods. Auditing occurs on the systems and devices, which are then aggregated and stored in a proprietary tool for review and incident investigation. The AWS operational environment, to include network and security configuration, is considered confidential information and is required

			inform the Responsible Entity of any external access to its systems immediately. To support secure remote access management, entities can configure AWS VPN for encrypted remote access to servers on AWS. For better performance and reliability, the VPN connection can be established over AWS Direct Connect. Multi-factor authentication can be configured to protect your AWS environment by using AWS MFA. MFA for remote access to assets on AWS can be implemented over VPN to the AWS VPC using your existing identity provider's capabilities. Customers can also use AWS Managed Microsoft AD to implement user management and MFA.	to be protected by employees per Amazon data classification policies. All remote administrative access attempts are logged and limited to a specific number of attempts. Auditing logs are reviewed by the AWS Security team for unauthorized attempts or suspicious activity. In the event that suspicious activity is detected, the incident response procedures are initiated.
CIP-003-8 Attachment 1, Section 4	Low impact BCS - Cyber security incident response	AWS CloudFormationAmazon S3AWS CloudTrailAmazon CloudWatchAmazon ElasticSearch	To support incident response planning and testing, customers should automate deployment of their systems using AWS CloudFormation to create a duplicate environment for a quick and low-cost way to test incident response procedures, at lower risk to operations and more frequently. As an investigative tool, customers can create a data lake on S3 to store logs from CloudTrail, other AWS services, CloudWatch, and	AWS is responsible for the security of the cloud infrastructure and has demonstrated compliance with multiple control frameworks, addressing controls for incident response for the cloud infrastructure. AWS customers inherit these controls and can reference our assurance reports demonstrating the validity of our controls in the artifact section of the AWS Management Console.AWS has implemented a

			system and application logs. Customers can then use AWS Elasticsearch to analyze event logs to support incident investigation activities.	formal, documented incident response policy and program. The policy addresses purpose, scope, roles, responsibilities, and management commitment. AWS utilizes a three-phased approach to manage incidents:1. Activation and Notification Phase2. Recovery Phase3. Reconstitution PhaseTo ensure the effectiveness of the AWS Incident Management plan, AWS conducts incident response testing. This testing provides excellent coverage for the discovery of previously unknown defects and failure modes. In addition, it allows the Amazon Security and Service teams to test the systems for potential customer impact and further prepare staff to handle incidents such as detection and analysis, containment, eradication, and recovery, and post-incident activities. The Incident Response Test Plan is executed annually, in conjunction with the Incident Response plan. AWS Incident Management planning, testing and test results are reviewed by third party auditors.
CIP-003-8 Attachment 1, Section 5	Low impact BCS - Transient cyber asset and removable		Entities can continue to follow their compliance program on the use of TCAs.	AWS is responsible for the security of the cloud and meets several regulatory compliance requirements including FedRAMP. AWS implements security

	media malicious code risk mitigation			controls including FedRAMP/NIST AC-17 to 20 to protect its infrastructure.
CIP-004-6, R1	Security Awareness program		Entities can continue to follow their existing compliance program on security awareness and training, personnel security and access management controls requirements.	AWS is responsible for the security of the cloud infrastructure and has demonstrated compliance with multiple control frameworks, addressing controls for security training and awareness, personnel security, and access management and authorization. AWS customers inherit these controls and can reference our assurance reports demonstrating the validity of our controls in the artifact section of the AWS Management Console.
CIP-004-6, R2	Security training prior to access and every 15 months			
CIP-004-6, R3	Personnel Risk Assessment and background checks			
CIP-004-6, R4	Access Management, authorization, verify access privileges	AWS Identity & Access Management (IAM) IAM Access Analyzer AWS Managed Directory Service Amazon Cognito	Customers can manage user access, authorization, and revocation for administrative access to the AWS Management console using AWS IAM. AWS IAM offers the ability to implement fine grained permissions to users and roles. AWS IAM integrates with the customer's current SAML 2.0 compatible directory service. To manage access to servers (SSH and RDP) and end user access to services customers can use their existing directory service, AWS Directory Service, AWS IAM, and AWS Cognito. Customers can audit users, grant and revoke access to users using a	
CIP-004-6, R5	Access Revocation			

			combination of these tools. IAM Access Analyzer can be used to get a deeper insight into who or what system has access to AWS assets. Access Analyzer runs continuously and will inform the Responsible Entity of any external access to its systems immediately.	
CIP-005-6, R1	Defined Electronic Security Perimeter, traffic managed through External Access Point, detect malicious communications	Amazon CloudFront AWS Shield Amazon Route 53 Amazon Guard Duty AWS IoT Device Defender	Entities can continue to follow their existing compliance program on Electronic Security Perimeter controls. Entities maintain ownership and control over their content and are responsible for managing security requirements, including controls over electronic security perimeter. To help meet electronic security perimeter controls requirements in the cloud, entities can use AWS Virtual Private Cloud (VPC) to define their cloud network, limit exposure to the internet, automate configuration, inspect, protect, and control all traffic (inbound, outbound, and within network). Entities should use AWS Shield with Amazon CloudFront and Amazon Route 53, to receive comprehensive availability protection against known infrastructure (Layer 3 and 4) attacks. To support detection of malicious communications entities can use Amazon GuardDuty, a	AWS is responsible for the security of the cloud infrastructure and has demonstrated compliance with multiple control frameworks, addressing controls for network security and remote access management. AWS customers inherit these controls and can reference our assurance reports demonstrating the validity of our controls in the artifact section of the AWS Management Console. Network devices, including firewall and other boundary devices, are in place to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services. ACLs, or traffic flow policies, are established on

			threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect their AWS accounts and workloads. To help protect remote and edge devices and gateways running AWS IOT Core or AWS GreenGrass an entity should use AWS IoT Device Defender which detects unusual device behavior that may be indicative of a compromise by continuously monitoring high-value security metrics from the devices.	each managed interface, which manage and enforce the flow of traffic. ACL policies are approved by Amazon Information Security. These policies are automatically pushed using AWS's ACLManage tool, to help ensure these managed interfaces enforce the most up-to-date ACLs.
CIP-005-6, R2	Remote access management via intermediate system, utilize encryption and multifactor authentication	AWS VPNAWS Direct ConnectAWS Managed Microsoft ADAWS IoT Secure Tunneling	To support secure remote access management, entities can configure AWS VPN for encrypted remote access to servers on AWS. For better performance and reliability, the VPN connection can be established over AWS Direct Connect. With AWS IoT secure tunneling, entities can establish a bidirectional communication to their AWS IoT or GreenGrass devices behind restricted firewalls at remote sites.Multi-factor authentication can be configured to help protect your AWS environment by using AWS MFA. MFA for remote access to assets on AWS can be implemented over VPN to the AWS VPC using your existing identity provider's capabilities. Customers can also use AWS Managed Microsoft AD to implement user	Remote access to AWS production environments is limited to defined security groups. The addition of members into a group must be reviewed and approved by authorized individuals who confirm the user's need for access to the environment. Remote access requires multi-factor authentication over an approved cryptographic channel for authentication.AWS employs automated mechanisms to facilitate the monitoring and control of remote access methods. Auditing occurs on the systems and devices, which are then aggregated and stored in a proprietary tool for review and incident investigation. The AWS operational environment, to include network and security configuration, is considered confidential information and

			management and MFA.	is required to be protected by employees per Amazon data classification policies. All remote administrative access attempts are logged and limited to a specific number of attempts. Auditing logs are reviewed by the AWS Security team for unauthorized attempts or suspicious activity. In the event that suspicious activity is detected, the incident response procedures are initiated.
CIP-006-6, R1	Physical security plan and access management		Entities can continue to follow their existing compliance program on physical security of BES cyber systems. Customer cyber policies and security plans should be reviewed to identify updates needed to address the use of cloud services.	AWS is responsible for the security of the cloud infrastructure and has demonstrated compliance with multiple control frameworks, addressing controls for physical security. AWS customers inherit these controls and can reference our assurance reports demonstrating the validity of our controls in the artifact section of the AWS Management Console. Physical access to all AWS data centers housing IT infrastructure components is restricted to authorized data center employees, vendors, and contractors who require access in order to execute their jobs. Access to facilities is only permitted at controlled access points that require multi-factor authentication designed to prevent tailgating and to
CIP-006-6, R2	Visitor control program			
CIP-006-6, R3	Physical access control system maintenance and testing			

				ensure that only authorized individuals enter an AWS data center. On a quarterly basis, access lists and authorization credentials of personnel with access to AWS data centers are reviewed by the respective data center Area Access Managers (AAM).
CIP-007-6, R1	Ports and services access restriction	AWS VPC AWS Network Firewall AWS Firewall Manager	Entities can continue to follow their existing compliance program on systems security management controls. Entities maintain ownership and control over their content and systems in the cloud, and are responsible for managing security requirements, including restricting ports and services, patch management, malicious code prevention, security event monitoring, and system access control. To manage ports and services access, entities can configure their AWS VPC(s) to restrict traffic to specific ports and source/destination CIDRs by using security groups and network ACLs. Amazon S3 Access Points can be used to limit access to S3 data and data lakes to specific VPCs. Different sets of permission can be granted to fine tune access. With Amazon S3 Access Points S3 data never leaves the entity's VPC. AWS Network Firewall is a managed	AWS is responsible for the security of the cloud infrastructure and has demonstrated compliance with multiple control frameworks, addressing controls for systems and network security for the cloud infrastructure. AWS customers inherit these controls and can reference our assurance reports demonstrating the validity of our controls in the artifact section of the AWS Management Console.

			service that makes it easy to deploy network protections for all of your Amazon Virtual Private Clouds (VPCs). AWS Network Firewall offers a flexible rules engine to define firewall rules that give you fine-grained control over network traffic, such as blocking outbound Server Message Block (SMB) requests to prevent the spread of malicious activity. AWS Firewall offers a single service to build firewall rules, create security policies, and enforce them in a consistent, hierarchical manner across your entire infrastructure, from a central administrator account.	
CIP-007-6, R2	Patch management	AWS Systems Manager AWS IoT jobs	To support patch management, entities should use AWS Systems Manager to help maintain security and compliance by scanning their instances against their patch, configuration, and custom policies. Entities can define patch baselines, maintain up-to-date anti-virus definitions, and enforce firewall policies. Entities can also remotely manage their servers at scale without manually logging in to each server. For their AWS IoT or GreenGrass devices entities can use AWS IoT jobs to push software and firmware to devices in the field to patch security vulnerabilities and improve device functionality.	

CIP-007-6, R3	Malicious code prevention	Amazon GuardDuty AWS WAF	To support prevention of malicious code entities can use Amazon GuardDuty, a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads. Entities should also use AWS WAF, a web application firewall that helps protect applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF gives entities control over which traffic to allow or block to their web applications by defining customizable web security rules. Entities can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for their specific application. In addition, various third-party IDS/IPS are available from AWS Partners.	
CIP-007-6, R4	Security Event Monitoring	AWS CloudTrailAWS CloudWatchAWS CloudWatch AgentAmazon DetectiveAmazon S3Amazon Elasticsearch ServiceAWS Security HubAWS IoT Device	To support security event monitoring entities can use AWS CloudTrail to generate logs for all AWS API actions. In addition, entities can install the AWS CloudWatch Agent on their EC2 instances to collect application and server logs. Logs generated from CloudTrail and the CloudWatch Agent can be monitored using AWS	

		Defender	CloudWatch. Entities can create events based on these logs and receive alerts in near real-time. They can also create a data lake on S3 to store these logs and use AWS Elasticsearch for log analytics and monitoring. Entities can use a third-party product on their EC2 instances to collect and monitor logs. Amazon Detective can be used to collect logs from AWS Services and conduct a security event triage and investigation as events are occurring. AWS Security Hub gives entities a comprehensive view of their security alerts and security posture across their AWS accounts. Security Hub, offers a single place that aggregates, organizes, and prioritizes security alerts, or findings, from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector, AWS Identity and Access Management (IAM) Access Analyzer, AWS Systems Manager, and AWS Firewall Manager, as well as from AWS Partner Network (APN) solutions.AWS IoT Device Defender lets entities continuously monitor security metrics from devices running AWS IoT or AWS GreenGrass for deviations from the expected behaviors for each device.	

CIP-007-6, R5	System Access Control	Amazon Cognito AWS Directory Service AWS Managed Microsoft AD	Entities can continue to follow their existing compliance program on system access control. Entities can use their existing directory service, AWS Directory Service or AWS Cognito to support interactive user authentication and account management.	
CIP-008-6, R1	Incident Response Plans		Entities can continue to follow their existing compliance program on incident response plans. Response plans should be reviewed and updated to incorporate use of AWS services that support incident detection and response.	AWS is responsible for the security of the cloud infrastructure and has demonstrated compliance with multiple control frameworks, addressing controls for incident response for the cloud infrastructure. AWS customers inherit these controls and can reference our assurance reports demonstrating the validity of our controls in the artifact section of the AWS Management Console. AWS has implemented a formal, documented incident response policy and program. The policy addresses purpose, scope, roles, responsibilities, and management commitment. AWS utilizes a three-phased approach to manage incidents: 1. Activation and Notification Phase 2. Recovery Phase 3. Reconstitution Phase To ensure the effectiveness of the AWS
CIP-008-6, R2	Incident Response plan implementation and testing	Amazon S3 AWS CloudTrail AWS CloudFormation Amazon CloudWatch Amazon ElasticSearch AWS IoT Device Defender	To support response efforts, entities can create a data lake on S3 to store logs from CloudTrail, other AWS services, CloudWatch, and system and application logs. Entities can then use AWS Elasticsearch to analyze event logs to support incident investigation activities. AWS IoT Device Defender can be used to conduct security investigations on devices running AWS IoT or AWS GreenGrass. AWS Simple Notification Service can be integrated with Device Defender to receive immediate notifications on events. To support incident response planning and testing, entities should automate	

			deployment of their systems using AWS CloudFormation to create a duplicate environment for a quick and low-cost way to test incident response procedures, at lower risk to operations and more frequently.	Incident Management plan, AWS conducts incident response testing. This testing provides excellent coverage for the discovery of previously unknown defects and failure modes. In addition, it allows the Amazon Security and Service teams to test the systems for potential customer impact and further prepare staff to handle incidents such as detection and analysis, containment, eradication, and recovery, and post-incident activities. The Incident Response Test Plan is executed annually, in conjunction with the Incident Response plan. AWS Incident Management planning, testing and test results are reviewed by third party auditors.
CIP-008-6, R3	Incident Response plan review, update and communication		Entities can continue to follow their existing compliance program on incident response review, update and communication. Response plans should be reviewed and updated to incorporate use of AWS services that support incident detection and response.	
CIP-008-6, R4	Incident Response plan review, update and communication		Entities can continue to follow their existing compliance program processes on incident notification and reporting. Response plans should be reviewed and updated to incorporate use of AWS services that support incident detection and response.	

CIP-009-6, R1	Recovery plans, Backup and Recovery Process, Data Preservation	AWS Backup AWS Disaster Recovery AWS CloudFormation	Entities can continue to follow their existing compliance program processes on recovery planning, backup and testing. Entities are responsible for properly implementing contingency planning, training, and testing for their systems hosted on AWS. Recovery plans should be reviewed and updated to incorporate use of AWS services that support backup and recovery processes. AWS provides customers with the capability to implement a robust continuity plan, including the utilization of frequent server instance back-ups, data redundancy replication, and the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. AWS Backup is a fully managed backup service that makes it easy to centralize and automate the back up of data across AWS services in the cloud as well as on premises using the AWS Storage Gateway.	AWS is responsible for the security of the cloud infrastructure and has demonstrated compliance with multiple control frameworks, addressing controls for recovery planning for the cloud infrastructure. AWS customers inherit these controls and can reference our assurance reports demonstrating the validity of our controls in the artifact section of the AWS Management Console. The AWS Business Continuity plan details the process that AWS follows in the case of an outage, from detection to deactivation. AWS maintains a ubiquitous security control environment across all regions. Each data center is built to physical, environmental, and security standards in an active-active configuration, employing redundancy to ensure system availability in the event of component failure.

CIP-009-6, R2	Recovery plan implementation and testing	AWS BackupAWS Disaster RecoveryAWS CloudFormation	CloudEndure Disaster Recovery is an AWS service that makes it quick and easy to shift your disaster recovery strategy to the AWS cloud from existing physical or virtual data centers, private clouds, or other public clouds. If you have already migrated to AWS, you can further protect your mission-critical workloads with cross-region disaster recovery. Using CloudFormation entities can automate deployment of their systems. A strategy of auto scaling, data backups, and automated deployment offers the ability to recreate systems to support recovery efforts in significantly less time than rebuilding manually. The AWS Cloud supports multiple disaster recovery (DR) architectures that can be configured to meet customer requirements, these include simple backup and recovery, pilot light, warm standby, and multi region always on.	
CIP-009-6, R3	Recovery plan review, update and communication		Entities can follow their existing compliance program processes on recovery planning requirements for documenting lessons learned, update recovery plans, and notify identified persons or groups of the updates.	
CIP-010-3, R1	Baseline Configuration	AWS Config AWS Systems	Entities can continue to follow their existing compliance program on	AWS is responsible for the security of the cloud infrastructure and has

	and Change Management	Manager Amazon Inspector AWS Lambda Amazon SNS AWS CloudFormation	configuration change management and vulnerability assessments. You can continuously monitor, assess, and manage changes to your AWS environment using AWS Config. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting. Using AWS CloudFormation, you can also develop and utilize templates for the development of secure network, storage, and compute assets. Customers can also monitor baseline standards configured for assets deployed within your AWS environment using AWS Inspector and AWS Systems Manager.	demonstrated compliance with multiple control frameworks, addressing controls for configuration and vulnerability management for the cloud infrastructure. AWS customers inherit these controls and can reference our assurance reports demonstrating the validity of our controls in the artifact section of the AWS Management Console. AWS applies a systematic approach to managing change to ensure that all changes are reviewed, tested, and approved.
CIP-010-3, R2	Configuration Monitoring			
CIP-010-3, R3	Vulnerability Assessments and Remediation		Customers can use third party vulnerability assessment tools to scan their servers on AWS. Many of these tools can be directly obtained and deployed from the AWS Marketplace.	AWS Security notifies and coordinates with the appropriate service teams when conducting security-related activities within the system boundary. Activities include vulnerability scanning, contingency testing, and incident

				response exercises. AWS performs external vulnerability assessments at least quarterly, and identified issues are investigated and tracked to resolution. Additionally, AWS performs unannounced penetration tests by engaging independent third parties to probe the defenses and device configuration settings within the system.
CIP-010-3, R4	Transient Cyber Assets and Removable Media Management		Entities can continue to follow their existing compliance program on the use of TCAs.	AWS is responsible for the security of the cloud and meets several regulatory compliance requirements including FedRAMP. AWS implements security controls including FedRAMP/NIST AC-17 to 20 to protect its infrastructure.
CIP-011-2, R1	Identify and protect BCSI	AWS KMS	Entities can continue to follow their existing compliance program on information protection requirements. Features like Access Analyzer for S3 will immediately alert the responsible entity if any S3 content is accessible from outside of the AWS Account and will help evaluate bucket access policies as they are being written.	AWS is responsible for the security of the cloud infrastructure and has demonstrated compliance with multiple control frameworks, addressing controls for information protection for the cloud infrastructure. AWS customers inherit these controls and can reference our assurance reports demonstrating the validity of our controls in the artifact section of the AWS Management

CIP-011-2, R2	Sanitization of BCSCI prior to cyber asset reuse or disposal	AWS IAM AWS KMS AWS CloudTrail	Entities can encrypt data in transit and at rest. AWS storage services including EBS, RDS, DynamoDb, and S3 offer the ability to encrypt data at rest. Entities can control user access to data using IAM policies and encrypt data at rest using the AWS Key Management Service (KMS).	Console. When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in NIST 800-88 (“Guidelines for Media Sanitization”) as part of the decommissioning process. Content on drives is treated at the highest level of classification per AWS policy. Content is destroyed on storage devices as part of the decommissioning process in accordance with AWS security standards. AWS hosts are securely wiped or overwritten prior to provisioning for reuse. AWS media is securely wiped or degaussed and physically destroyed prior to leaving AWS secure zones.

Governance at Scale	AWS services that will aid in managing and implementing CIP controls	AWS Audit Manager Control Tower Security Hub AWS Organizations	Entities can use several AWS services that help with managing cloud assets at scale, referred to as "Governance at Scale." AWS Control Tower is a service that automates the setup of a multi-account AWS environment with a few clicks. The setup employs blueprints, which capture AWS best practices for configuring AWS security and management services to govern your environment. Blueprints are available to provide identity management, federate access to accounts, centralize logging, establish cross-account security audits, define workflows for provisioning accounts, and implement account baselines with network configurations. AWS Organizations helps centrally manage and govern environments. Using AWS Organizations, an entity can programmatically create new AWS accounts and allocate resources, group accounts to organize workflows, apply policies to accounts or groups for governance, and simplify billing by using a single payment method for all of its accounts. For example, an entity can create a group of accounts for in scope workloads and set common policies.	

			Entities can use AWS Security Hub to get a comprehensive view of their security alerts and posture across their AWS accounts/organization. With Security Hub, an entity will have a single place that aggregates, organizes, and prioritizes their security alerts, or findings, from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector, AWS Identity and Access Management (IAM) Access Analyzer, AWS Systems Manager, and AWS Firewall Manager, and from AWS Partner Network (APN) solutions. Entities can use AWS Audit Manager to continuously audit their AWS usage to simplify how they assess risk and compliance with regulations and standards. Audit Manager automates evidence collection to reduce the “all hands-on deck” manual effort that often happens for audits and enables scaling an entity’s audit capability in the cloud. With Audit Manager, it is easy to assess if policies, procedures, and activities – also known as controls are operating effectively. At audit, AWS Audit Manager helps manage stakeholder reviews of controls and enables building audit-ready reports with much less manual effort.	