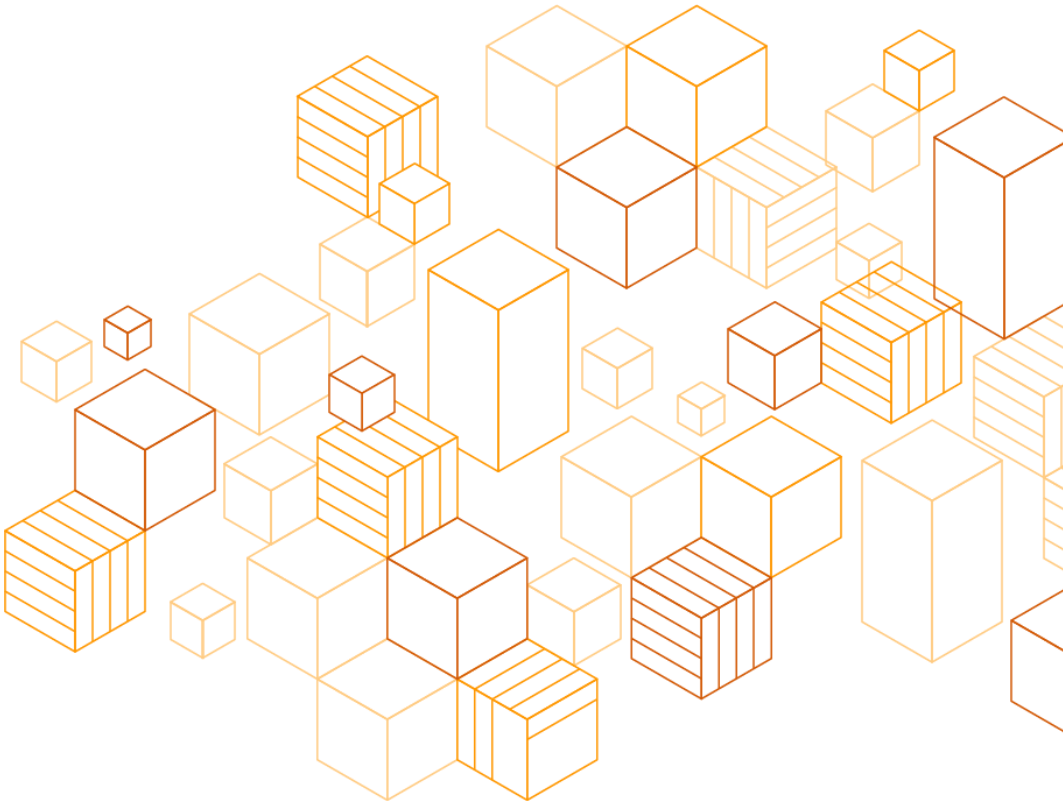
AWS User Guide to Support Compliance with North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards

January 2020



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 customers can use AWS services to realize the benefits of cloud technology and meet 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 meet the security and reliability objectives of the NERC CIP standards. The following sections provide information on AWS services that enable customers to meet and sustain compliance with NERC CIP standards, how these services align with the NERC CIP standards, and considerations for customers as they plan use of AWS Cloud services for data and systems within the regulated scope.

Background

AWS recognizes that our Power and Utility customers are interested in leveraging cloud computing technology to meet their business objectives and the needs of their customers. 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 use of new technology and to enable Responsible Entities to meet their operational, security, and resiliency objectives.

The US electric sector is regulated by the Federal Energy Regulatory Commission (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 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 that meet the defined criteria are mandated to comply with the NERC CIP standards for the data, assets, and systems in-scope of the standards.

To encourage discussion, FERC held panels at Reliability Technical Conferences to discuss how standards can evolve to best leverage the benefits of a cloud environment effectively and securely for utility planning and operations. Existing CIP drafting teams are following the Standards Development Process to assess and propose language revisions, where appropriate.

> **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.*

Technical stakeholder working groups are 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. Specifically, guidance is being drafted for protection of BES Cyber System Information (BCSI) in the cloud. 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 Assurance Programs and Inheriting Controls

AWS aligns with other security assurance programs that evaluate, assess and monitor cyber security controls on network infrastructure, applications and services to comport with requirements of existing US government programs. These security assurance programs are consistent with the CIP security objectives. Customers 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.

AWS Artifact

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

AWS maintains certifications and independent, third-party attestations for a variety of industry specific workloads. AWS is routinely audited for its compliance to these assurance programs, which includes continuous monitoring.

Customers can leverage AWS assurance reports in AWS Artifact to help demonstrate compliance for security of the cloud, in addition to their own complementary controls that detail their unique and specific configurations and demonstrate their compliance for security of their resources in the cloud.

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

- **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 help customers and their auditors understand the AWS controls established to support customers' operations and compliance.

  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 reporting and 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 that is 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 that is 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 is the development and implementation of a rigorous security program, which includes 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 aspects of 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 information security 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 applicable to 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.
- **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 continuous monitoring requirements of FedRAMP.
- **NIST Cyber Security Framework** – Whether assessing a cloud service provider like AWS, establishing priorities for traditional technology purchases, or determining 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 to the NIST CSF, thereby streamlining assessments, acquisition, and compliance, and at a lower cost.

AWS is compliant with several security standards including SOC 1, 2, and 3, and FedRAMP moderate and high. The security of AWS data centers is reviewed 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.

Customer compliance teams can build on traditional programs by tying together governance-focused, audit-friendly service features with such certifications, attestations, and audit standards. For more information about the other certifications and attestations from AWS, see the AWS Compliance Center.

Security and Shared Responsibility

Cloud security is a shared responsibility. The Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS in the context of the cloud security principles. AWS manages security of the cloud by ensuring that AWS infrastructure complies with global and regional regulatory requirements and best practices, and security in the cloud is the responsibility of the customer. This means that customers 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.

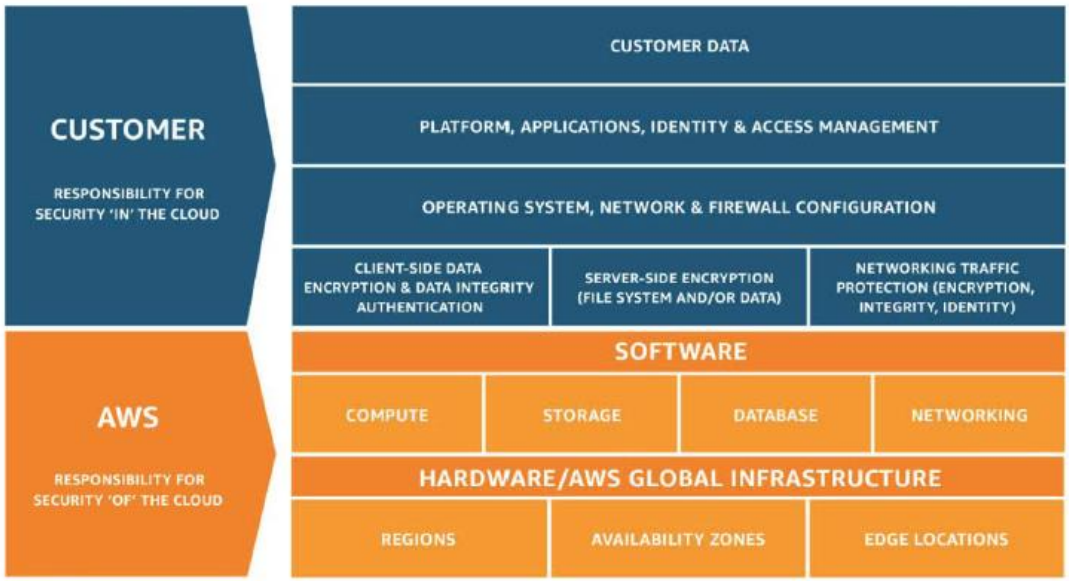


Figure 1: Shared responsibility model

In fulfilling CIP compliance, NERC Responsible Entities are responsible for ensuring compliance with NERC CIP requirements; however, fulfillment of the controls depends on the applicable IT component. Responsible Entities manage controls for NERC CIP classified assets; AWS manages controls for the cloud infrastructure; and both Responsible Entities and AWS perform security control activities for requirements that apply to the cloud infrastructure and NERC CIP classified assets.

Security in the Cloud

Customers are responsible for security **in** the cloud. The customer is responsible for managing the guest operating system (including installing updates and security patches) and other associated application software, as well as the configuration of the AWS provided security group firewall. Customers 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.

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

- The AWS services and security features that are used.
- The country where their content is stored.

- The format and structure of their content and whether it is masked, anonymized, or encrypted.
- How their data is encrypted and where the keys are stored.
- Who has access to their content and how those access rights are granted, managed, and revoked.
- Resilience of architecture to ensure availability.

AWS customers in scope for NERC CIP are responsible for managing controls to ensure security **in** the cloud for their regulated assets. The AWS Cloud services used to support regulated assets, along with the specific assets that are managed in the cloud, determine the controls that customers need to manage. For example, to satisfy requirements for account configuration, management and reviews for assets managed in the cloud, customers can use services such as AWS Identity and Access Management (IAM) to configure and manage user access and privileges.

Some NERC CIP requirements are addressed by entity specific policies, plans or processes 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. Whereas cloud services may be used to support performance of these controls, customers will follow their compliance program to meet these requirements and should update governing documents that may be appropriate to accommodate cloud services.

Security of the Cloud

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. Customers 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 to establish 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 leading practices 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 to perform their control evaluation and verification procedures, as required under the applicable compliance standard.
- **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.

Customers inherit the controls that provide security **of** the cloud infrastructure. For a description of general security controls and service-specific security from AWS, see AWS Overview of Security Processes.

Well-Architected Framework

In addition to the division of responsibilities that the Shared Responsibility model provides, AWS also recommends the Well-Architected Framework to assist customers in defining the best approaches to meet the security and reliability objectives of the NERC CIP standards in the planning stages of the cloud adoption journey. AWS developed the Well-Architected Framework to help cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. Based on five pillars—operational excellence, security, reliability, performance efficiency, and cost optimization—the framework provides a consistent approach for customers and partners to evaluate architectures, and implement designs that will scale over time.

For more information on the Well-Architected Framework, see AWS Well-Architected.

Shared Responsibility and Applicable Services by Standard

Appendix: AWS Services and Alignment to NERC CIP includes a table that offers more details on the shared responsibilities and inherited controls, and illustrates how they apply by CIP standard and requirement.

Implementing Controls to Support Security and Compliance Objectives

Inherent features of the cloud enable customers to meet their security objectives.

AWS architecture is designed to provide enhanced reliability and customers can configure additional reliability, if desired. Evidence and reporting is also enhanced by use of automation and the ability to configure responses based on event triggers.

Automating security best practices is simplified by using cloud services. All AWS capabilities and actions are supported by an Application Programming Interface (API). These APIs enable you to automate the creation, management, control, and monitoring of the cloud networks, security, access management, servers, storage, and backups. As a result, all activities generate an evidence log. Security automation enables customers to have a proactive incident response capability, providing the ability to reduce the scope and impact of security events. Using automation also enables restoration of the customer'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).

Customers can simplify compliance auditing, security analysis, change management, and operational troubleshooting by using AWS services such as:

- AWS Systems Manager Inventory enables customers 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-premise computing environment. Customers can use 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, customers can assign metadata to their AWS resources in the form of tags to document the BES cyber categorization of regulated workloads in the cloud.
- AWS Config enables customers to assess, audit, and evaluate the configurations of their AWS resources against desired configurations. 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.
- 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 trigger remedial actions and notifications to you.
- AWS Systems Manager Session Manager provides secure and auditable instance management without the need to open inbound ports, maintain bastion hosts, or manage SSH keys. Session Manager also makes it easy to comply with corporate policies that require controlled access to instances, strict security practices, and fully auditable logs with instance access details, while still providing end users with simple one-click access to your Amazon EC2 instances.

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 to manage users in all these categories.

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. Customers 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. Customers 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.

In the cloud, remote access to assets is considered as administrative control of Amazon EC2 instances over SSH or RDP. Customers can manage administrative access to their Amazon EC2 instances using their existing directory service, AWS Directory Service for Microsoft Active Directory (also known as AWS Managed Microsoft AD).

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

Customers can meet their requirements for protecting data throughout the lifecycle, for data at-rest, in-transit and in-use (CIP011-2, *Information Protection*). Customers 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 customers that store data (data-at-rest) on AWS storage services or transit (data-in-transit) AWS networks. Encryption and data access control features are built into foundational service offerings such as Amazon Simple Storage Service (Amazon S3), a highly scalable object storage service, Amazon Elastic Block Store (Amazon EBS), which provides network-attached storage to EC2 instances, and Amazon Relational Database Service (Amazon RDS), which provides managed database engines. These features provide documentation to help customers understand how to protect their data and the configuration options they can control to customize who can access the systems and the keys required to decrypt data residing on them.

AWS Key Management Service (AWS KMS) is a fully managed, highly available regionally isolated service. Key management and cryptographic functions are integrated with other AWS services. The service is scalable and validated for security assurance by third parties through the security assurance programs. Customers have the option to use AWS CloudHSM, a cloud-based hardware security module (HSM). Alternatively, customers can maintain local control over their keys by importing keys from an on-premise key management and HSM solution and still take advantage of the other KMS features. Use of AWS KMS does not enable any AWS personnel to have access to key material or to data content.

For data in-use, customers leverage security controls other than encryption, whether procedural or technical, to protect their data, such as IAM, two-factor authentication, and others.

AWS follows standards to install, service, and eventually destroy the 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 customer data is not removed from AWS control until it has been securely decommissioned. Customers can further protect their data by using encryption (AWS KMS); for Amazon EBS volumes, customers can use third-party software to wipe storage media before reuse or decommissioning.

Patching and Vulnerability Management

Customers can address their security objectives for patching and malicious code protection (CIP-007, *Systems Security Management*), and configuration and vulnerability management (CIP-010, *Configuration Change Management and Vulnerability Assessment*) using AWS services. On AWS, customers 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 and other types of updates.

Customers can restrict communications (CIP005, *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. Customers can also use AWS Web Application Firewall (WAF) to help protect web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. Using AWS WAF, customers 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. AWS customers 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.

AWS offers a range of tools to allow customers to move quickly while still ensuring that cloud resources comply with organizational standards and best practices. 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. Inventory and configuration management tools, such as AWS Config, allow customers to identify AWS resources and then track and manage changes to those resources over time. Customers can also use template definition and management tools, such as AWS CloudFormation, to create standard, preconfigured cloud environments. For protection against malicious code, customers can install third-party host-based detection software from one of many AWS partners. Customers can also use third-party vulnerability assessment tools to scan their servers on AWS.

Security Event Monitoring

CIP007, *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 customers 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, customers can collect application and server logs from their servers and send them to Amazon CloudWatch where customers can create alarms that send notifications. Customers can use AWS Lambda to implement remedial actions when an alarm is triggered. This approach offers customers 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, customers 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. Customers 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.

Incident Response

Customers 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 practices incident response policies and programs that that include incident response testing. and, as part of the assurance programs, is evaluated by independent, third-party assessors.

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).. 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) customers 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. Customers can use the AWS best practice of using automation to deploy their applications enabling fast and low cost testing of disaster recovery processes.

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). Customers 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 allows physical data center access only to approved employees and authorized visitors. Access is logged and audited routinely. Physical access to data centers in AWS GovCloud (US) is restricted to people who have been validated as being US citizens.

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, customers should take a risk-based approach to their implementation of their internal security requirements on AWS. This includes validating that your customer service agreement aligns with your internal security and resilience requirements; building detective controls, if needed, to ensure that processes are functioning as intended; and, updating processes to incorporate AWS services.

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.

Customers are encouraged to use the resources available to implement cloud services like the AWS Well-Architected Framework. As previously noted, AWS recommends that customers use the AWS Well-Architected Framework as a foundational tool in the planning stages of the cloud adoption journey.

Customers can also use the AWS Cloud Adoption Framework (AWS CAF) which offers structure to help organizations develop an efficient and effective plan for their cloud adoption journey. Guidance and best-practices prescribed within the framework can help you build a comprehensive approach to cloud computing across your organization, throughout your IT lifecycle. The AWS CAF breaks down the complicated process of planning into manageable areas of focus.

Beyond the AWS Well-Architected Framework and AWS CAF, there are many other free resources available for customers to leverage during their cloud adoption journey, including whitepapers listed in the Additional Resources section of this paper and computer-based trainings. Customers seeking a closer partnership with AWS can also reach out to their Account Managers.

Contributors

Contributors to this document include:

- Ranjan Banerji, Sr. Partner Solutions Architect, Power & Utilities, AWS
- Samara Moore, Sr. Manager, 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
- AWS Incident Response
- AWS Security Whitepaper
- AWS Answers to Key Compliance Questions
- AWS Securing Data at Rest with Encryption
- AWS Security at Scale Logging in AWS Whitepaper
- Secure Content Delivery with CloudFront Whitepaper

Document Revisions

Date	Description
January 2020	First publication

Appendix: AWS Services and Alignment to NERC CIP

The following table illustrates how AWS services and inherited controls can be used to 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 assurance reports described previously.

CIP Standard Requirement Objectives	CIP Standard Description	AWS Services	Customer Considerations	AWS Responsibility
CIP002-5.1a-R1	Identify and categorize cyber assets	AWS Tags	Customers can continue to follow their compliance program processes to meet identify and categorize cyber assets, and to review asset categorization. (CIP002-5.1a, R1-R2) Once assets are categorized, customers 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.	
CIP002-5.1a-R2	Review and approve, every 15 months	AWS Tags		

CIP Standard Requirement Objectives	CIP Standard Description	AWS Services	Customer Considerations	AWS Responsibility
CIP003-6-R1	Cyber policies		Customers can continue to follow their compliance program processes to meet security management controls requirements. Customer cyber policies and security plans should be reviewed to identify updates needed to address the use of cloud services. (CIP003-6, R1-R4)	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. (CIP003-6, R1)
CIP003-6-R2	Security plans for low impact systems			
CIP003-6-R3	Document CIP Senior Manager			
CIP003-6-R4	CIP Senior Manager delegation			
CIP004-6-R1	Security Awareness program			

CIP Standard Requirement Objectives	CIP Standard Description	AWS Services	Customer Considerations	AWS Responsibility
CIP004-6-R2	Security training prior to access and every 15 months		Customers can continue to follow their compliance program processes to meet security awareness and training, personnel security and access management controls requirements. (CIP004-6, R1-R5)	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. (CIP004-6 R1, CIP004-6 R2, R1-R5)
CIP004-6-R3	Personnel Risk Assessment and background checks			
CIP004-6-R4	Access Management, authorization, verify access privileges			

CIP Standard Requirement Objectives	CIP Standard Description	AWS Services	Customer Considerations	AWS Responsibility
CIP004-6-R5	Access Revocation	AWS Identity & Access Management (IAM) 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 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. (CIP004-6, R4-R5)	

CIP Standard Requirement Objectives	CIP Standard Description	AWS Services	Customer Considerations	AWS Responsibility
CIP005-5-R1	Defined Electronic Security Perimeter, traffic managed through External Access Point, detect malicious communications	Amazon CloudFront AWS Shield Amazon Route 53 Amazon Guard Duty	Customers can continue to follow their compliance program processes to meet electronic security perimeter controls requirements. Customers maintain ownership and control over their content and are responsible for managing security requirements, including controls over electronic security perimeter. To meet electronic security perimeter controls requirements in the cloud, customers can use AWS Virtual Private Cloud (VPC) to define your cloud network, limit exposure to the internet, automate configuration, inspect, protect, and control all traffic (inbound, outbound, and within network). (CIP005-5, R1) Customers 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 customers can use Amazon GuardDuty, a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect their AWS accounts and workloads.(CIP005-5, R1)	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 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. (CIP005-5, R1)

CIP Standard Requirement Objectives	CIP Standard Description	AWS Services	Customer Considerations	AWS Responsibility
CIP005-5-R2	Remote access management via intermediate system, utilize encryption and multifactor authentication	AWS VPN AWS Direct Connect AWS Managed Microsoft AD	To support secure remote access management, customers 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.	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 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. (CIP005-5, R2)

CIP Standard Requirement Objectives	CIP Standard Description	AWS Services	Customer Considerations	AWS Responsibility
CIP006-6-R1	Physical security plan and access management		Customers can continue to follow their compliance program processes to meet physical security of BES cyber systems controls requirements. Customer cyber policies and security plans should be reviewed to identify updates needed to address the use of cloud services. (CIP006-6, R1-R3)	AWS is responsible for the security of the physical 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). (CIP006-6, R1-R3)
CIP006-6-R2	Visitor control program			
CIP006-6-R3	Physical access control system maintenance and testing			

CIP Standard Requirement Objectives	CIP Standard Description	AWS Services	Customer Considerations	AWS Responsibility
CIP007-6-R1	Ports and services access restriction	AWS VPC	Customers can continue to follow their compliance program processes to meet systems security management controls requirements. Customers 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, customers 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 customer's VPC. (CIP007-6, R1)	AWS is responsible for the security of the physical 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. (CIP007-6, R1-R5)

CIP Standard Requirement Objectives	CIP Standard Description	AWS Services	Customer Considerations	AWS Responsibility
CIP007-6-R2	Patch management	AWS Systems Manager	To support patch management, customers should use AWS Systems Manager to help maintain security and compliance by scanning your instances against your patch, configuration, and custom policies. You can define patch baselines, maintain up-to-date anti-virus definitions, and enforce firewall policies. You can also remotely manage your servers at scale without manually logging in to each server. (CIP007-6, R2)	

CIP Standard Requirement Objectives	CIP Standard Description	AWS Services	Customer Considerations	AWS Responsibility
CIP007-6-R3	Malicious code prevention	Amazon GuardDuty AWS WAF	To support prevention of malicious code customers can use Amazon GuardDuty, a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads. Customers 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 you control over which traffic to allow or block to your web applications by defining customizable web security rules. Customers 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 your specific application. In addition, various third-party IDS/IPS are available from AWS Partners. (CIP007-6, R3)	

CIP Standard Requirement Objectives	CIP Standard Description	AWS Services	Customer Considerations	AWS Responsibility
CIP007-6-R4	Security Event Monitoring	AWS CloudTrail AWS CloudWatch AWS CloudWatch Agent Amazon Detective Amazon S3 Amazon Elasticsearch Service	To support security event monitoring customers can use AWS CloudTrail to generate logs for all AWS API actions. In addition, customers 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 CloudWatch. Customers can create events based on these logs and receive alerts in near real-time. Customers can also create a data lake on S3 to store these logs and use AWS Elasticsearch for log analytics and monitoring. Customers can also 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. (CIP007-6, R4)	
CIP007-6-R5	System Access Control	Amazon Cognito AWS Directory Service AWS Managed Microsoft AD	Customers can continue to follow their compliance program processes to meet system access control requirements. Customers can use their existing directory service, AWS Directory Service or AWS Cognito to support interactive user authentication and account management. (CIP007-6, R5)	

CIP Standard Requirement Objectives	CIP Standard Description	AWS Services	Customer Considerations	AWS Responsibility
CIP008-5-R1	Incident Response Plans		Customers can continue to follow their compliance program processes to meet incident reporting and response planning requirements. Response plans should be reviewed and updated to incorporate use of AWS services that support incident detection and response. (CIP008-5, R1-R3)	
CIP008-5-R2	Incident Response plan implementation and testing	AWS CloudFormation	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.	

CIP008-5-R3	Incident Response plan review, update and communication	Amazon S3 AWS CloudTrail Amazon CloudWatch Amazon ElasticSearch	As an investigative tool customers can create a data lake on S3 to store logs from CloudTrail, other AWS services, CloudWatch, and system and application logs. Customers can then use AWS Elasticsearch to analyze event logs to support incident investigation activities.	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 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

CIP Standard Requirement Objectives	CIP Standard Description	AWS Services	Customer Considerations	AWS Responsibility
				Incident Response plan. AWS Incident Management planning, testing and test results are reviewed by third party auditors.

CIP Standard Requirement Objectives	CIP Standard Description	AWS Services	Customer Considerations	AWS Responsibility
CIP009-6-R1	Recovery plans, Backup and Recovery Process, Data Preservation	AWS Backup AWS Disaster Recovery AWS CloudFormation	Customers can continue to follow their compliance program processes to meet recovery planning, backup and testing requirements. Customers 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. (CIP009-6, R1)	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. (CIP009-6, R1-R3)

CIP Standard Requirement Objectives	CIP Standard Description	AWS Services	Customer Considerations	AWS Responsibility
CIP009-6-R2	Recovery plan implementation and testing	AWS Backup AWS Disaster Recovery AWS 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. (CIP009-6, R2) Using CloudFormation customers 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. (CIP009-6, R2)	
CIP009-6-R3	Recovery plan review, update and communication		Customers can follow their compliance program processes to meet recovery planning requirements for documenting lessons learned, update recovery plans, and notify identified persons or groups of the updates.	

CIP Standard Requirement Objectives	CIP Standard Description	AWS Services	Customer Considerations	AWS Responsibility
CIP010-2-R1	Baseline Configuration and Change Management	AWS Config AWS Systems Manager Amazon Inspector AWS Lambda Amazon SNS AWS CloudFormation	Customers can continue to follow their compliance program processes to meet configuration change management and vulnerability assessment requirements. 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. (CIP010-2, R1-R2)	AWS is responsible for the security of the cloud infrastructure and has 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. (CIP010-2, R1-R2)
CIP010-2-R2	Configuration Monitoring			

CIP Standard Requirement Objectives	CIP Standard Description	AWS Services	Customer Considerations	AWS Responsibility
CIP010-2-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. (CIP10-2, R3)	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. (CIP010-2, R3)
CIP010-2-R4	Transient Cyber Assets and Removable Media Management	AWS KMS		

CIP Standard Requirement Objectives	CIP Standard Description	AWS Services	Customer Considerations	AWS Responsibility
CIP011-2-R1	Identify and protect BCSI	Amazon Macie	Customers can continue to follow their compliance program processes to meet information protection requirements. To help identify BCSI, customers can use Amazon Macie, a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Macie recognizes sensitive data such as personally identifiable information (PII) or intellectual property. It provides you with dashboards and alerts that give visibility into how this data is being accessed or moved. In addition, 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. (CIP011-2, R1)	

CIP Standard Requirement Objectives	CIP Standard Description	AWS Services	Customer Considerations	AWS Responsibility
CIP011-2-R2	Sanitization of BCSCI prior to cyber asset reuse or disposal	AWS IAM AWS KMS AWS CloudTrail	Customers 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. AWS also offers you with the ability to sanitize your EBS volumes, if needed. Customers can control user access to data using IAM policies and encrypt data at rest using the AWS Key Management Service (KMS). (CIP011-2, R2)	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 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. (CIP011-2, R2) 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.