NERC CIP Standards for BES Cyber System Information on AWS

Compliance Guide

February 02, 2023

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 agreements between AWS and its customers.

Contents

Abstract

This whitepaper is intended for Entities registered with the North American Electric Reliability Corporation (NERC) as users, owners, and operators of the bulk-power system, also referred to in this whitepaper as “Entities,” that are subject to the Critical Infrastructure Protection (CIP) Standards and responsible for implementing controls to protect Bulk Electric System Cyber System Information (BCSI) on Amazon Web Services (AWS).

This whitepaper identifies the AWS controls that align with CIP-004-7 Cyber Security - Personnel & Training and CIP-011-3 Cyber Security - Information Protection requirements and provides security best practices and architectural recommendations to help you design and deploy NERC CIP-compliant architectures to host and protect BCSI in the AWS Cloud.

Introduction

This whitepaper provides high-level guidance for Entities and partners on how to design and deploy solutions in the AWS Cloud to help protect BCSI. Although Entities can use many design permutations to help meet the applicable requirements in CIP-004-7 and CIP-011-3 on AWS, this document presents sample reference architectures to consider that will address many of the more common use cases.

The paper is designed for information technology (IT) decision makers, operational technology (OT) decision makers, compliance decision makers, and security personnel. It assumes familiarity with basic security concepts in the areas of networking, data encryption, and operational controls.

The purpose of the NERC CIP Standard requirements for Bulk Electric System (BES) Cyber System Information (BCSI) is to protect information that could be used to gain unauthorized access or pose a security risk to a BES Cyber System. BCSI must be identified, protected, and securely handled to mitigate risks of compromising confidentiality through unauthorized access or disclosure. To achieve compliance, Entities must undertake planning to implement the necessary controls, and gather and maintain the evidence necessary to demonstrate compliance with the NERC CIP BCSI requirements identified in CIP-004-7 and CIP-011-3.

In December 2021, the Federal Energy Regulatory Commission (FERC) approved revisions to two NERC CIP standards CIP-004-7 and CIP-011-3. The revised Standards modify the CIP requirements for protecting BCSI to provide a secure, regulator-approved path to modern, third-party data storage and analysis systems including cloud technology. These changes resolve earlier compliance concerns about the use of cloud technology and allow Entities to store, transmit, and use BCSI in the cloud, as long as Entities have the appropriate compliance controls in place and can demonstrate them during a compliance monitoring and enforcement process.

AWS itself is not an owner or operator of the bulk power system and therefore is not subject to the NERC CIP Standards. Although a NERC CIP certification program for cloud services does not exist, AWS has achieved compliance with multiple regulatory and certification frameworks, including FedRAMP and System and Organization Control (SOC), which might be of particular interest to Entities subject to NERC CIP Standards.

Background

AWS recognizes that Entities are interested in increased choice, greater flexibility, higher availability, and reduced-cost options for managing their BCSI in order to enhance BES reliability. Cloud solutions are an important part of the industry's transformative response to maintain reliable operations. As NERC noted in their informational filing to FERC:

> "…as technology has evolved, third-party services, such as cloud services, have become a viable and safe option for storing BCSI. The protections available for Responsible Entities to secure information in the cloud, for example, depend less on the actual storage location of the information and more on file-level rights and permissions."

According to the approved Implementation Plan, the revised Standards will become enforceable on January 1, 2024, but can be adopted ahead of the enforcement date.

In addition to the revised Standards, Entities can reference BCSI and cloud guidance documents developed by the NERC Electric Reliability Organization (ERO) that provide more specific recommendations for BCSI in a cloud environment. For example, Security Guideline for Electricity Sector - Primer for Cloud Solutions and Encrypting BCSI provides guidance on how to use encryption as a means to protect and restrict access to BCSI in a cloud environment. ERO Enterprise CMEP Practice Guide: BES Cyber System Information offers guidance to auditors when assessing an Entity's process to authorize access to BCSI-designated storage locations.

For years, Entities explored moving BCSI to a cloud environment, but struggled to do so in a way that was consistent with the applicable CIP Standards. Regulators were also hesitant to sign off on moving sensitive information to the cloud. The revised Standards and associated NERC guidance help resolve these issues and unlock the ability to use BCSI in a compliant manner consistent with regulatory expectations.

Getting started

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

The AWS Power and Utility Path to Production in the Cloud breaks down the customer journey into manageable parts, and helps Entities envision how to implement cloud solutions considering the people, obligations, and resources required.

To plan for this transition, Entities should consider how to present the change to their regulators in a way that demonstrates the security of BCSI before, during, and after the transition. Collaboration with NERC and the auditor teams that evaluate the Entity's CIP Standards compliance is important to gain auditor confidence in the Entity's compliance program. Considering the regulator perspective and the transparency it necessitates can help an Entity set goals and create workstreams for the transition that allow Entity staff to thrive in the cloud, and help develop and maintain the evidence needed to demonstrate compliance and provide the high level of assurance that auditors will need to find that BCSI is protected in the AWS Cloud.

To get started, you should consider the following technology and compliance questions:

- How can the AWS Cloud advance your NERC CIP compliance program?
- How can you achieve your objectives for security, logging, monitoring, and incident response by using the AWS Cloud?
- Do you have applications and systems that can benefit from greater visibility, reliability, or security?
- What are your compute, storage, and network capacity requirements?
- How can you prepare to scale up (and down) to support your program?

As you consider each question, apply the lenses of flexibility, cost effectiveness, scalability, elasticity, and security with an eye to maintaining the ability to demonstrate compliance. By using AWS services, you can focus on your core competencies and use the resources and experience that AWS provides in a way that aligns with NERC CIP

Standards and helps you to demonstrate compliance in an audit.

Shared responsibilities and governance

Security is a shared responsibility between AWS and Entities, as shown in Figure 1. This shared model helps relieve the Entity's operational burden because AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates.

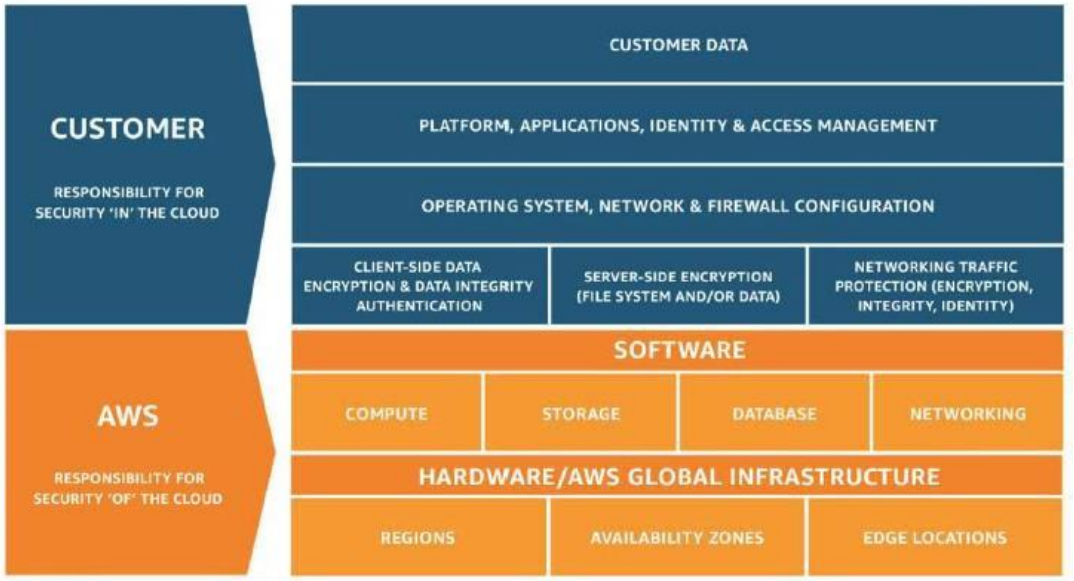

Figure 1: AWS shared responsibility model

The Entity assumes responsibility and management of the guest operating system (including updates and security patches) and other associated application software, as well as the configuration of the AWS-provided security group firewall. Entities should carefully consider the services they choose because their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations. Understanding responsibilities between the Entity and AWS is an important part of the cloud adoption process.

The shared responsibility model also extends to compliance controls. Just as the responsibility to operate the environment is shared between AWS and the Entity, so is

the management, operation, maintenance, and verification of shared compliance controls.

Entities using AWS Partner solutions for BCSI should consider how the Shared Responsibility Model applies to their specific use cases because it could differ depending on the selected solutions.

Under applicable NERC guidance, a NERC-registered Entity charged with the performance of a NERC function remains solely responsible for compliance with the Reliability Standards applicable to that function, even if the performance of certain tasks relies on a third party or services provided by a third party. Thus, while the Shared Responsibility model illustrates the division of management, operational, and security controls between AWS and Entities, it does not transfer compliance obligations from the Entity to AWS under the NERC CIP Standards or otherwise require or suggest that AWS will assume the Entity's compliance responsibility or liability.

Inherited, shared, and entity-specific controls

To further clarify shared responsibility, controls are classified into three categories: inherited, shared, and Entity specific.

Inherited controls are controls that an Entity fully inherits from AWS, including physical and environmental controls. AWS is responsible for the security and compliance **of the cloud**: the infrastructure that runs the services offered in the AWS Cloud. The infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. This includes controls that maintain logical separation between Entity resources and data, physical security of AWS data centers, and other administrative, compliance, and security-related controls.

Although physical security controls to protect electronic BCSI are not directly required by the NERC CIP Standards, AWS manages security controls associated with AWS physical infrastructure. Entities can then use the AWS control and compliance documentation available to them in AWS Artifact to perform their control evaluation and verification procedures.

Shared controls apply to both the infrastructure layer and the Entity layer, but in completely separate contexts or perspectives. In a shared control, AWS provides the requirements for the infrastructure, and the Entity provides their own control implementation within their use of AWS services. Shared controls do not imply transfer

of security or compliance obligations. Rather, both parties—AWS and the Entity—must implement independent controls to meet a security objective. Examples include, but are not limited to, the following:

- Patch management – AWS is responsible for patching and maintaining the infrastructure, but Entities are responsible for patching their guest operating systems and applications within their AWS environments.
- Configuration management – AWS maintains the configuration of its infrastructure devices, but an Entity is responsible for configuring their own guest operating systems, databases, and applications within their AWS environments.

Entity-specific controls are solely the responsibility of the Entity based on the application that they deploy on AWS. Entity responsibility is determined by the AWS Cloud services that an Entity selects. This determines the amount of configuration work that the Entity must perform as part of their security responsibilities.

Examples include, but are not limited to, the following:

- Service and communications protection or zone security, which might require an Entity to route or zone data within specific security environments.
- Encryption to protect data.
- Setup and maintenance of identity and access permissions for user accounts and roles.
- Entities that deploy an Amazon Elastic Compute Cloud (Amazon EC2) instance are responsible for management of the guest operating system (including updates and security patches), and software installed on the instances.
- For abstracted services, such as Amazon Simple Storage Service (Amazon S3) and Amazon DynamoDB, Entities are responsible for managing their data (including encryption options), classifying their assets and resources, and using IAM tools to apply appropriate access controls and permissions.

Entities should carefully consider the services that they choose because 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 the AWS Well-Architected Framework).

AWS Support

AWS Support offers a range of plans that provide access to tools and expertise that support the success and operational health of Entities' AWS solutions. Support plans provide 24x7 access to customer service, AWS documentation, technical papers, and support forums. Access to 24x7 on-demand technical support can help Entities gather the information necessary to respond to regulatory inquiries. Note that AWS personnel are not available to act as subject matter expert witnesses during compliance monitoring and enforcement activities.

AWS Support offers five support plans: Basic, Developer, Business, Enterprise On-Ramp, and Enterprise. Entities can compare AWS Support plans against their needs. The Enterprise On-Ramp and Enterprise Support plans offer technical account management that Entities can use to receive proactive guidance and help with optimization, and to coordinate access to programs. For technical support and other resources to plan, deploy, and improve an AWS environment, Entities can choose a support plan that best aligns with their AWS use case.

Scope and BES Cyber System Information (BCSI) environment

The NERC Glossary of Terms defines BCSI as follows:

> "Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System."

BCSI scope determination

Entities are responsible for documenting one or more information protection programs for BCSI that includes methods to identify BCSI. Entities are responsible for determining the data that is classified as BCSI in alignment with their information protection program. The data might include NERC CIP asset databases, operational technology network data, network diagrams, NERC CIP compliance evidence, and other sensitive information.

Off-premises electronic BCSI, including within a cloud environment, should be protected through the implementation of electronic technical methods (for example, encryption, hashing, tokenization, and electronic key management), administrative methods (for example, vendor service risk assessments and business agreements), and identity and access management.

Entities must be able to identify their BCSI scope within the environment, and support auditors' ability to validate the compliance controls that are in place to protect that BCSI.

Guide for NERC CIP BCSI alignment on AWS

This section provides guidance on ways that Entities can use AWS services to help secure their BCSI. The CIP-004-7 and CIP-011-3 requirements applicable to BCSI allow

each Entity to define programs and methods to comply with the language in the requirements. Although this section provides recommendations on program features and controls, each Entity is responsible for evaluating the options against its compliance obligations under the NERC CIP Standards and implementing the controls that it deems appropriate.

For a table that shows shared responsibilities and inherited controls, and how you can use AWS services to support compliance with specific CIP Standards and requirements, see Appendix 1: AWS services and alignment to NERC CIP.

CIP-011-3, Requirement 1 – Information protection program

CIP-011-3 Requirement 1 requires Entities to implement documented information protection programs pertaining to defined Applicable Systems. The information protection program must include methods to identify BCSI (Part 1.1), and methods to protect and securely handle BCSI to mitigate risks of compromising confidentiality (Part 1.2).

CIP-011-3 R1, Part 1.1 – Methods to identify BCSI

In the AWS Cloud, Entities can identify and list the resources associated with storing and processing BCSI. One approach is to assign an AWS tag to each resource associated with BCSI. Another approach is to dedicate specific AWS accounts for BCSI.

AWS tags for BCSI

An Entity can apply tags to AWS resources that contain BCSI. Each tag is a label consisting of a user-defined key and value. Tags can help you manage, identify, organize, search for, and filter resources. You can create tags to categorize resources by purpose, owner, environment, or other criteria.

Tags can identify the following information about an AWS resource:

- Whether the resource stores BCSI
- Security details – for example: encryption type and strength, tokenization, access

controls, and truncation

- Applicable systems to which the BCSI pertains – for example: BES Cyber System, Electronic Access Control or Monitoring System, or Physical Access Control System associated with a BES Cyber System
- Impact rating of the applicable systems to which the BCSI pertains – for example: high impact or medium impact

Figure 2 shows an example of AWS tags for an Amazon Elastic Block Store (Amazon EBS) volume attached to an Amazon EC2 instance that an Entity might use to identify NERC CIP BCSI.

Key	Value
Compliance	BCSI
Encryption Strength	256
Impact Rating	High
Key Management	aws-kms
Name	my-data-server

Figure 2: AWS tags

Entities can use AWS Resource Groups to organize and manage their AWS resources that are in the same AWS Region, including resources associated with BCSI. With Resource Groups, Entities can automate tasks, such as applying security patches and updates, on a group of AWS resources at the same time.

Figure 3 shows Resource Groups in the AWS Management Console and how an Entity can view resources tagged as BCSI.

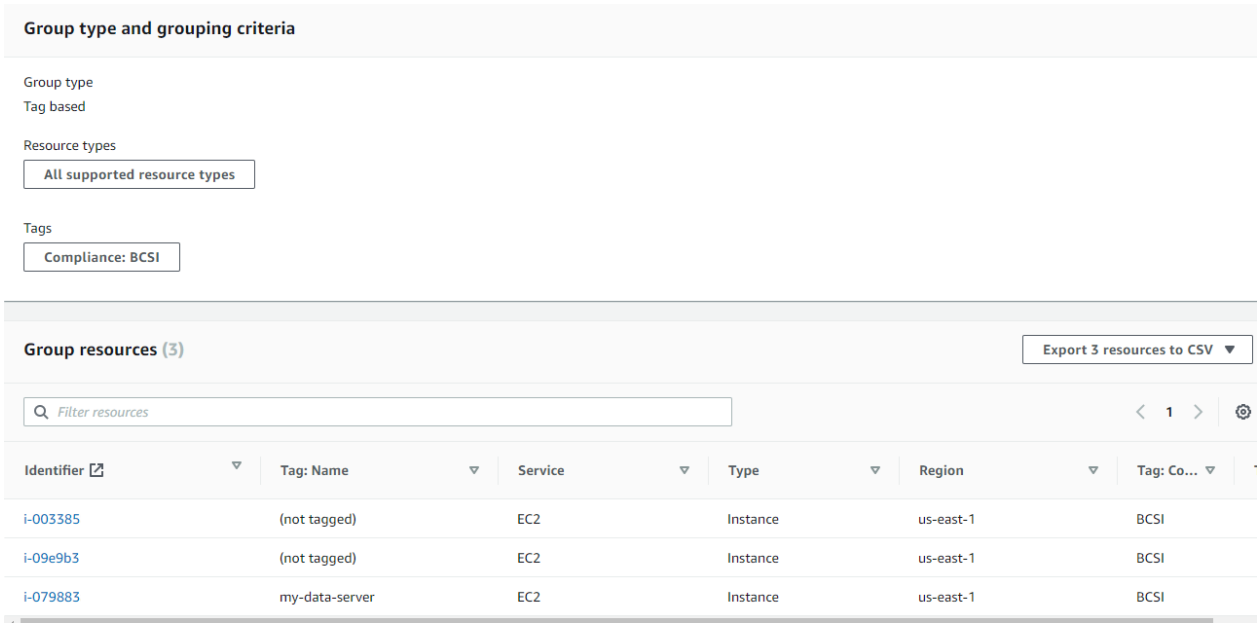

Figure 3: AWS resource groups

Using AWS Config, Entities can query for resources with the relevant tag value. Entities can use this service to assess, audit, and evaluate their configuration of AWS resources. AWS Config continuously monitors and records AWS resource configurations and allows Entities to automate the evaluation of recorded configurations against desired configurations.

With AWS Config, Entities can review changes in configurations and relationships between AWS resources, examine detailed resource configuration histories, and determine their overall compliance against the configurations specified in their internal guidelines. This can help simplify compliance auditing, security analysis, change management, and operational troubleshooting.

Dedicated accounts for BCSI

AWS recommends a multi-account strategy, including a dedicated account or accounts for accessing BCSI, which Entities can govern and manage by using AWS Control Tower. An Entity can classify the resources in these dedicated accounts as BCSI,

reducing the need for manual efforts to identify and tag resources and helping to ensure that security controls are consistently applied to BCSI in the dedicated account.

AWS Control Tower allows Entities to set up and govern a secure, multi-account AWS environment, called a *landing zone*. AWS Control Tower creates the landing zone by using AWS Organizations, which enables programmatic creation of new AWS accounts and allocation of resources, grouping of accounts to organize workflows, application of policies to accounts or groups for governance, and simplification of billing by using a single payment method for your accounts.

AWS Organizations is integrated with other AWS services so that Entities can define central configurations, security mechanisms, audit requirements, and resource sharing across accounts in their organization.

Figure 4 shows an example of how an Entity can implement separation of responsibilities by using AWS Organizations. In this example, enterprise systems are separated under a different organizational unit than operations.

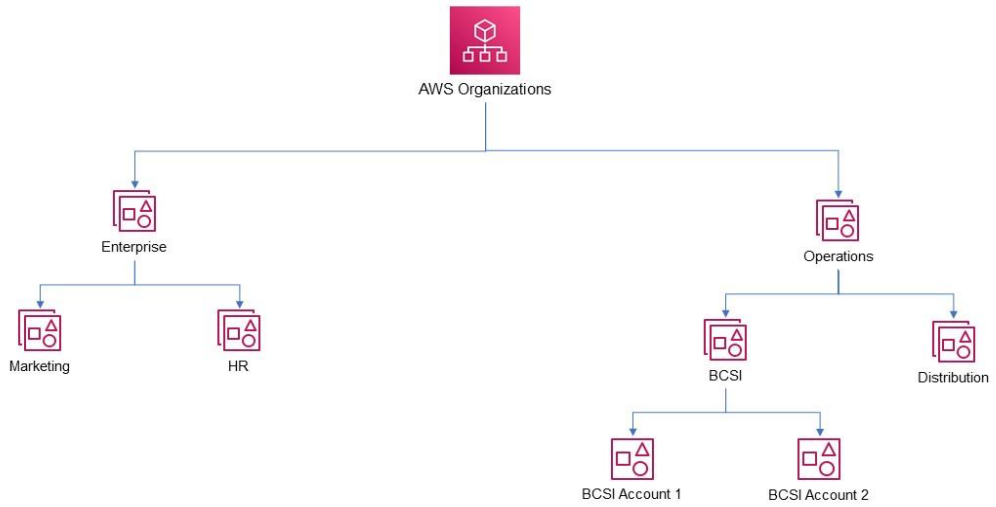

Figure 4: AWS Organizations example

Entities can provision new AWS accounts that conform to company policies, extend governance to new or existing accounts, and gain visibility into their compliance status.

CIP-011-3 R1, Part 1.2 – Electronic technical methods to protect and securely handle electronic BCSI

CIP-011-3 R1, Part 1.2 does not require a particular method or methods to protect and securely handle BCSI. Instead, with off-premises storage in a cloud environment, an Entity can use a variety of electronic methods to protect the BCSI, such as data masking, encryption, hashing, tokenization, ciphers, and electronic key management. AWS provides a number of tools that an Entity can use to accomplish these objectives in an auditable manner, as described in the following sections.

Logical isolation

Logical isolation of data is a foundational component for implementing and demonstrating electronic technical methods to protect electronic BCSI. An Entity might have a well-established AWS environment that uses an AWS Control Tower or landing zone solution, in which case the Entity can create an account dedicated to BCSI; or an Entity might have existing accounts into which some BCSI needs to be moved or used; or an Entity might be building a new AWS environment. In each of these scenarios, the electronic technical methods to protect BCSI include the use of AWS services for logical isolation of data.

With Amazon Virtual Private Cloud (Amazon VPC) , Entities can provision a logically-isolated section of the AWS Cloud where they can launch AWS resources in a virtual network that they define.

By default, a VPC is an isolated network, and resources deployed into subnets within the VPC cannot communicate with those outside of it, such as another AWS account or VPC, the public internet, or the Entity's data center. An Entity must configure a VPN gateway and subnet route tables to allow communications with their on-premises data center. Entities determine the communications links for their environment through the gateways that they select and configure to meet their needs.

Security groups act as stateful firewalls for resources within an Amazon VPC,

controlling both inbound and outbound traffic. Entities can use security groups to restrict traffic by IP address, port, and protocol, and to support elements of CIP-011-3 Requirement 1, Part 1.2.

Network access control lists (network ACLs) are an optional layer of security for VPCs that act as a stateless router for controlling traffic in and out of one or more subnets. Entities that use network ACLs can evaluate and deny traffic based on the connection source (whether in standard CIDR IPv4 or IPv6 format) or specific AWS resources and provide traffic filtering above layer 4 of the Open Systems Interconnection (OSI) model.

VPC endpoints are a feature of Amazon VPC that allows Entities to connect to supported AWS services by using private IP addresses in their own VPC. VPC endpoint services are powered by AWS PrivateLink. This traffic does not leave the AWS network and does not require internet access or public IP addresses to communicate with resources exposed with VPC endpoints.

Entities can use third-party firewall software made available by AWS Partners through AWS Marketplace to help deploy a comprehensive security architecture and seamless experience across AWS and Entities' on-premises environments.

For an illustrative example of an AWS NERC CIP BCSI reference architecture, see Appendix 2: AWS NERC CIP BCSI reference architecture.

Encryption in transit

AWS offers Entities secure ways to connect to an Amazon VPC. Virtual private network (VPN) solutions help establish secure connections between an Entity's on-premises network, remote offices, client devices, and the AWS global network. AWS VPN comprises two services: AWS Site-to-Site VPN and AWS Client VPN. Each service provides a highly-available, encrypted, managed, and elastic cloud VPN solution to help protect your network traffic.

To help ensure bandwidth and high performance, Entities can work with AWS Direct Connect Delivery Partners to implement AWS Direct Connect, a dedicated fiber connection to AWS that supports MAC Security (MACsec) (IEEE 802.1AE). AWS Direct Connect delivers native, near line-rate, and point-to-point encryption for 10 gigabits per

second (Gbps) and 100 Gbps links.

To help secure communications between servers owned by an Entity, or an Entity and a third party, the Entity should use SSL/TLS. With AWS Certificate Manager (ACM), the Entity can provision, manage, and deploy public and private SSL/TLS certificates for use with AWS services and internal connected resources.

SSL/TLS certificates can help secure network communications and establish the identity of websites over the internet, as well as resources on private networks. ACM helps alleviate the time-consuming manual process of purchasing, uploading, and renewing SSL/TLS certificates.

Entities can use FIPS 140-2 validated cryptographic modules when accessing US East/West or AWS Canada (Central) Regions through use of the command line interface (CLI) or programmatically by using AWS provided FIPS endpoints to help support their security or compliance needs.

Encryption at rest

AWS Key Management Service (AWS KMS) integrates with other AWS services to encrypt data at rest, or to facilitate signing and verification by using an AWS KMS key. To protect data at rest, integrated AWS services use envelope encryption, where a data key is used to encrypt data, and the data key itself is encrypted under a KMS key stored in AWS KMS. For signing and verification, integrated AWS services use a key pair from an asymmetric KMS key in AWS KMS. To learn more about how integrated services use AWS KMS, see the documentation for your AWS service.

It is the Entity's responsibility to configure encryption and maintain strong data retention policies and procedures. Entities can use AWS KMS, AWS CloudHSM, or both to help create and manage the key material involved in Requirement 1, Part 1.2. They can use IAM to enforce granular access restrictions.

Key management

Entities can use AWS KMS, AWS CloudHSM, or both to help reduce the compliance burden for many key management requirements. For customers wanting to transition to a cloud-native approach, optimize encryption for cloud workloads, and reduce

administrative burden compared to self-managed HSMs, Entities should choose AWS KMS. With AWS KMS, Entities can create, store, and manage KMS keys securely. An Entity's KMS keys never leave AWS KMS unencrypted. Entities can also create and manage key policies in AWS KMS so that only trusted users have access to KMS keys. KMS keys are backed by FIPS-validated *hardware security modules* (HSMs) that AWS KMS manages. An HSM is a specialized security device that generates and stores cryptographic keys.

Security and quality controls in AWS KMS have been validated and certified by the following compliance regimes: AWS System and Organization Controls (SOC 1, SOC 2, and SOC 3), FIPS 140-2 Level 3, and FedRAMP.

Entities are responsible for controlling access to AWS KMS key management functionality through key policies and IAM policies. With AWS KMS, Entities have full control over KMS keys, including establishing and maintaining key policies, IAM policies, and grants, enabling and disabling the KMS keys, rotating their cryptographic material, adding tags, creating aliases that refer to the KMS keys, and scheduling the KMS keys for deletion. AWS KMS natively integrates with other AWS services.

AWS KMS supports three types of keys: customer managed, AWS managed, and customer imported keys. Customer managed keys are generated, owned, and managed by the customer using AWS KMS. AWS managed keys take advantage of automation and integration with AWS services, enabling an Entity to tell the service to encrypt and then AWS generates and encrypts a key. The Entity from this point on uses the keys and experiences the benefits of AWS KMS.

The third option is where a customer imports keys generated by another HSM. The Entity has full responsibility for customer imported keys, which includes generating the key material by using a source of randomness that meets the Entity's security requirements and that must be a 256-bit symmetric encryption key; responsibility for the key material's overall availability and durability; and retaining a copy of the key material in a system that the Entity controls for restoration purposes. Imported keys are designed to help Entities meet compliance requirements, which might include the ability to generate or maintain a secure copy of the key in the Entity's infrastructure, and the ability to immediately delete the imported copy of the key from AWS infrastructure.

For Entities needing to meet corporate, contractual, and regulatory compliance requirements that require a single-tenant FIPS 140-2 Level 3 validated HSM under your

control, CloudHSM can be used. CloudHSM offers single-tenant access to tamper-resistant HSMs that comply with the U.S. Government's FIPS 140-2 Level 3 standard for cryptographic modules. The CIP-011-3 requirements do not explicitly dictate the use of a single-tenant FIPS 140-2 Level 3 validated HSM, but Entities may choose this approach based on their own internal security and/or compliance program(s).

CloudHSM allows the Entity to move existing encrypted data directly into the cloud. However, the availability and latency of such a solution over time may be suboptimal. The critical risk is that if the HSM becomes unavailable, the hardware fails, or the encryption keys are lost, the Entity could face business outages or lose access to data. CloudHSM complements existing data protection solutions and allows Entities to protect their encryption keys within HSMs that are designed and validated to government standards for secure key management.

CIP-011-3 R1, Part 1.2 – Administrative methods to protect electronic BCSI

In addition to the electronic technical controls outlined in the previous section, the Standard also allows the use of "administrative methods" to protect BES stored off-premises, such as in the cloud. AWS offers a number of certifications, security assessment approaches, and similar methods to help verify the security of data on AWS.

AWS Artifact is a no cost, self-service portal for on-demand access to AWS compliance reports, such as AWS SOC reports, FedRAMP certification packages, and other certifications or reports from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls. When new reports are released, you can access them in AWS Artifact.

AWS Artifact Agreements enable Entities to review, accept, and manage agreements with AWS for an individual account, and for accounts that are part of your organization in AWS Organizations. Agreements available in AWS Artifact include the Business Associate Addendum (BAA) and the nondisclosure agreement (NDA).

The Getting Started with AWS Artifact guide helps Entities understand how to set up access to AWS Artifact, and how to review, accept, and manage agreements with AWS. For more information, see AWS Artifact FAQs.

The AWS Legal page provides resources to help you document administrative methods to protect off-premises BCSI, including the AWS Customer Agreement, AWS Service Level Agreements, AWS Acceptable Use Policy, and Privacy Notice.

CIP-004-7, Requirement 6

CIP-004-7, Requirement 6 requires Entities to implement documented access management programs to authorize, verify, and revoke provisioned access to BCSI. Specifically, Entities must authorize electronic access to BCSI based on need before they provision access (Part 6.1); verify at least once every 15 calendar months that individuals with provisioned access to BCSI have an authorization record and still need the provisioned access to perform their current work functions (Part 6.2); and remove an individual's ability to access electronic BCSI by the end of the next calendar day following the effective date of a termination action (Part 6.3).

According to CIP-004-7 R6, to be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered "the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys)." This is a significant step forward from older versions of the Standard that focused on access to storage locations, rather than access to data in a usable format, and it facilitates the use of cloud storage to help meet compliance requirements.

AWS provides Entities with complete control over provisioned access to BCSI. AWS does not have visibility into, or knowledge of, the content inside a customer account, including whether or not that content includes personal information. For more information, see Mitigating Unauthorized Access to Data. AWS customers are also empowered to use various techniques illustrated in the Security Pillar of the AWS Well-Architected Framework, such as encryption, and tokenization, to render content unintelligible to AWS or other parties, helping to ensure that only those individuals authorized by the Entity have the ability to obtain and use BCSI.

CIP-004-7 R6, Part 6.1.1 – Authorize provisioned electronic access to electronic BCSI

Much of CIP-004-7 Requirement 6, Part 6.1, is addressed by the Entity's access management policies and practices. With AWS Identity and Access Management (AWS IAM), Entities can manage access to perform cloud configuration and management activities. IAM enables access management, authorization, verification of access privileges, and access revocation to AWS service APIs, the AWS Management Console, and specific resources. Using IAM, Entities can create users, roles, and groups and assign fine-grained permissions.

With IAM, Entities can define a SAML 2.0 or OIDC identity provider (IdP), such as Microsoft Active Directory, for each AWS account. Entities can pass federated user attributes, such as the cost center or job role, from their IdPs to AWS, and use them for access control by implementing access permissions based on these attributes. IAM helps Entities define permissions once, and then grant, revoke, or modify AWS access by changing the attributes in the IdP.

Entities can also choose to use only IAM and AWS IAM Identity Center (successor to AWS Single Sign-on) for access management. These services provide a single point to manage users, access, and decommissioning processes. For example, you can manage password configuration controls, such as complexity, length, and expiration, in IAM or in your existing directory service that integrates with IAM.

In the cloud, an Entity's team of systems administrators can access Amazon EC2 instances over Secure Shell (SSH) or Remote Desktop Protocol (RDP). Entities can manage this administrative access to their EC2 instances by using their existing directory service or 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 through IAM.

The Entity's existing on-premises directory service and access controls can be used to control end-user access to information on AWS by integrating with AWS IAM Identity Center, AWS Partner solutions, or Amazon Cognito. Amazon Cognito supports Entity end-user sign-up, sign-in, and access control to their web and mobile applications.

CIP-004-7 R6, Part 6.2 – Verify provisioned access

An Entity can use AWS IAM Access Analyzer to review existing access so that the Entity can identify and remove unintended external or unused permissions. IAM includes a default "deny-all" setting that reduces the risk of unauthorized access. You can activate IAM Access Analyzer for your entire organization or specific accounts.

IAM Access Analyzer 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 AWS services.

Entities can review access permissions on a schedule of their choosing, including every 15 months as required by CIP-004-7 Requirement 6, Part 6.2.

CIP-004-7 R6, Part 6.3 – BCSI access removal

Entities also need a procedure or automated mechanism in place to remove an individual's ability to use provisioned access to BCSI by the end of the next calendar day following termination. Entities have several options to implement this requirement. AWS recommends using IAM Identity Center or IAM integration with a SAML 2.0 or OIDC identity provider. By doing so, an Entity can terminate access at a single centralized location for AWS accounts and services.

Entities can use CloudTrail reports and API calls to generate reports of user access, including information on users who were added or removed within a timeframe selected by the Entity. Entities can compare the reports against termination records to validate that the ability to access the BCSI was removed by the end of the next calendar day after the termination action.

Governance at scale

Entities at all stages of the cloud journey can govern their AWS environment at scale—whether they are just starting their cloud journey with AWS, pursuing a new cloud initiative, or managing an existing multi-account AWS environment but preferring a solution with built-in blueprints and guardrails.

To create or manage a multi-account AWS environment that follows best practices, Entities can use AWS Control Tower. AWS Control Tower offers prescriptive guidance to help you govern your AWS environment at scale. It also offers *guardrails* for ongoing governance of your AWS environment. Guardrails provide governance controls by preventing deployment of resources that don't conform to selected policies or by detecting non-conformance of provisioned resources.

AWS Control Tower automatically implements guardrails by using multiple building blocks, such as AWS CloudFormation to establish a baseline, AWS Organizations service control policies (SCPs) to prevent configuration changes, and AWS Config rules to continuously detect non-conformance.

AWS Control Tower also provides a dashboard for continuous oversight of your multi-account environment. The dashboard produces reports on detective and preventive guardrails that are enabled on your accounts, and provides the status of resources that don't comply with policies enabled through guardrails.

Entities can take advantage of the visibility and control offered by AWS Control Tower for their BCSI environments.

Implement and review audit trails

AWS provides many service-specific security and audit logs to help Entities meet their compliance documentation and validation needs on demand. CloudTrail provides an event history of account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. These logs include details to help support validation that controls are in place to securely handle BCSI. CloudTrail can also deliver logs to Amazon S3 for secure storage and analysis.

Entities that store BCSI in Amazon S3 should enable and configure S3 server access logging to capture object-level activity and authentication failures, and CloudTrail to capture bucket-level activity and API calls.

Entities can use CloudWatch to log requests that are handled by AWS Lambda functions. Entities are responsible for inserting logging statements as applicable into their code to record BCSI access and administrative activities within their applications. For additional system-level metrics, Entities can install a CloudWatch agent on EC2 instances.

Entities that are already using a security information and event management (SIEM)

solution can use their existing tool to review audit trails, including SIEM solutions that are available from AWS Partners through the AWS Partner Network.

In addition, an Entity can customize the analysis of their log data by using AWS services and features, including Amazon Athena to query audit trail logs saved to Amazon S3 from VPC Flow Logs, CloudTrail, and CloudWatch. Entities can use Amazon GuardDuty and AWS Security Hub together to provide automated event analysis, and pair these services with Amazon CloudWatch Events and Lambda to provide automated remediation.

Audit trail protection and retention

Entities should restrict Amazon S3 and CloudTrail by using fine-grained IAM policies to allow only specific information security personnel to have access to audit trails. Both services support the use of versioning, lifecycle policies, and deny-delete capabilities to help protect log data. CloudTrail also offers a log file integrity validation feature that can help support CIP-011-3 R1 Entities.

Entities can help protect their logs in Amazon S3 by applying an object lock in compliance mode. In compliance mode, a protected object version cannot be overwritten or deleted by users, including the AWS account root user. When an object is locked in compliance mode, its retention mode cannot be changed, and its retention period cannot be shortened. Compliance mode helps ensure that an object version cannot be overwritten or deleted for the duration of the retention period.

Entities can use a dedicated AWS account and Amazon S3 bucket to retain audit trails, and can configure lifecycle policies to migrate data older than three months to Amazon S3 Glacier for additional cost savings. The Amazon S3 Glacier storage classes provide retrieval options from milliseconds to hours to fit your performance needs. Entities can export CloudWatch logs to Amazon S3 to help protect log data with encryption and prevent or detect changes.

Compliance at scale

AWS Config includes an Operational Best Practices for NERC CIP BCSI conformance pack to help Entities manage configuration compliance of their AWS resources at

scale—from policy definition to auditing and aggregated reporting—by using a common framework and packaging model. The NERC CIP BCSI conformance pack can help Entities monitor and assess security and governance controls associated with CIP-004-7 Requirement 6 – Access Management for BCSI and CIP-011-3 Requirement 1 – Information Protection Program for NERC CIP BCSI.

The conformance pack includes more than 60 AWS Config rules that can help you implement access control best practices and data protection controls, including encryption of data at rest and in transit, and protection against exposure of data. Entities can run the conformance pack as compiled or modify it to include or remove AWS Config rules as needed to align with their information protection program.

For example, to support data protection, the conformance pack identifies unencrypted storage volumes or publicly exposed S3 buckets. Entities can create CloudWatch and Amazon Simple Notification Service (Amazon SNS) notifications to receive a text or email notification about changes in their environment that do not align with the controls in the conformance pack so that they can assess them and determine if remediation is necessary.

You can create conformance packs by authoring a YAML template that contains the list of AWS Config managed or custom rules and remediation actions. Within each conformance pack template, you can use one or more AWS Config rules and remediation actions. The AWS Config rules listed within the conformance pack can be AWS Config managed rules, AWS Config custom rules, or both. You can download the conformance pack templates from GitHub.

By using AWS Audit Manager, Entities can continually audit their AWS usage to help with risk and compliance assessments. Entities using the Operational Best Practices for NERC CIP BCSI conformance pack can transform it into an AWS Audit Manager Assessment.

An Audit Manager assessment is based on a *framework*, which is a grouping of controls. Using the Operational Best Practices for NERC CIP BCSI conformance pack, Entities can create an assessment that collects evidence for the controls in that framework. In the assessment, Entities can define the scope of the audit, which includes specifying the AWS accounts and services that you want to collect evidence for.

When you create an assessment, Audit Manager starts the ongoing collection of evidence. When it's time for an audit, or as determined necessary for internal reviews, the Entity can review the evidence and then add it to an assessment report for sharing with external auditors.

Conclusion

Each organization's cloud adoption journey is unique. To successfully migrate to the cloud, you need 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.

During the development process, collaboration with NERC or regional Entities' auditors can help you gain confidence with compliance. Opening dialogue, being transparent, and understanding auditor perspectives and expectations can help you set goals and create workstreams that not only enable staff to thrive in a cloud environment, 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 this paper, and in the Further reading section that follows. AWS supports 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, Amazon Web Services
- Kristine Martz, Industry Specialist – Energy & Utilities, Amazon Web Service
- Sean Murray, Sr Partner Solutions Architect, Amazon Web Services
- Maggy Powell, Industry Specialist – Energy & Utilities, Amazon Web Services

Further reading

For additional information, see the following resources:

- AWS Glossary of Terms
- AWS Security Reference Architecture (AWS SRA)
- AWS Well Architected Framework Security Pillar

- AWS User Guide Supporting NERC CIP Compliance
- AWS Best Practices for Security, Identity, and Compliance
- Compliance FAQs
- AWS Foundational Security Best Practice controls
- Power and Utility Path to Production in the Cloud
- The Utility Executive's Guide to AWS Cloud Security
- Utility Executive's Guide to AWS Security Control Domains
- AWS Shared Responsibility Model
- Logical Separation on AWS
- AWS NERC CIP BCSI Conformance Pack
- AWS NERC CIP BCSI Reference Architecture
- AWS Config NERC CIP BCSI Audit Manager Assessment

Document revisions

Date	Description
February 2023	First publication

Appendix 1: AWS services and alignment to NERC CIP

The following table illustrates AWS services that Entities can use to help implement and/or demonstrate compliance with NERC CIP BCSI requirements. Entities can choose the combination of AWS services and tools that meet the needs of their information protection program. This is not an exhaustive list and is meant to illustrate the services and concepts described in previous sections of this document.

NERC CIP standard or AWS feature and description	AWS services, features, and resources	Customer considerations	AWS responsibility
CIP-004-7 R6 Access management for BCSI, authorization, verify access privileges to BCSI	Amazon Cognito AWS CloudTrail AWS Directory Service AWS Directory Service for Microsoft AD AWS Identity and Access Management (IAM) AWS IAM Access Analyzer AWS IAM Identity Center	Entities can manage user access, authorization, and revocation for administrative access to the AWS Management Console by using IAM. IAM offers the ability to implement fine-grained permissions for users and roles, and it can integrate with the Entity's current SAML 2.0 compatible directory service. To manage access to servers (SSH and RDP) and end-user access to services, Entities can use their existing directory service, AWS Directory Service, IAM, and Amazon Cognito. By using a combination of these tools, Entities can audit users and grant and revoke access to users. Entities can enable	AWS personnel by default do not have the ability to obtain and use Entity content electronically or physically, including BCSI. AWS classifies customer information into two categories: customer content and account information. AWS defines customer content as software (including machine images), data, text, audio, video, or images that a customer or end user transfers to AWS for processing, storage, or hosting by AWS services in connection with that customer's account, and computational results that a customer or end user derives from the foregoing through their use of AWS

	AWS Management Console	IAM Identity Center to manage access centrally across their organization. AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD, allows your directory-aware workloads and AWS resources to use managed Active Directory on AWS. AWS Managed Microsoft AD is built on Microsoft AD and does not require you to synchronize or replicate data from your existing Active Directory to the cloud. You can use the standard Active Directory administration tools and built-in Active Directory features, such as Group Policy and single sign-on. With IAM Access Analyzer, you can gain insight into who or what system has access to AWS assets. IAM Access Analyzer runs continuously and informs the Entity of external access to its systems immediately. With AWS CloudTrail, you can enable governance, compliance, operational, and risk auditing of your account. Actions taken by a user, role, or AWS service are recorded as events in CloudTrail.	services. For example, customer content includes content that a customer or end user stores in Amazon S3. Customer content does not include account information. Customer content also does not include information included in resource identifiers, metadata tags, usage policies, permissions, and similar items related to the management of AWS resources. The terms of the AWS Customer Agreement and the AWS Service Terms apply to customer content.

NERC CIP standard or AWS feature and description	AWS services, features, and resources	Customer considerations	AWS responsibility
CIP-011-3, R1 Identify, protect, and securely handle BCSI to mitigate risks of compromising confidentiality	AWS Artifact Amazon Athena AWS Certificate Manager AWS Client VPN AWS CloudHSM AWS CloudTrail Amazon CloudWatch AWS Config AWS Control Tower AWS Direct Connect Amazon DynamoDB Amazon EBS Amazon EC2 AWS KMS	Entities can continue to follow their existing compliance program for information protection requirements. Entities can deploy tags to AWS assets that contain BCSI. With AWS Config, Entities can query for assets with the relevant tag value. Entities can encrypt data in transit and at rest. AWS storage services, such as Amazon Elastic Block Store, Amazon Relational Database Service, Amazon DynamoDb, and Amazon S3 offer the ability to encrypt data at rest. Entities can control user access to data by using IAM policies, and they can encrypt data at rest by using AWS Key Management Service (AWS KMS), Cloud HSM, or both.	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 that demonstrate the validity of our controls. You can find these reports in AWS Artifact.

	AWS Lambda AWS landing zone AWS Organizations AWS PrivateLink Amazon RDS AWS Resource Groups Amazon S3 AWS SDKs AWS Security Hub AWS Site-to-Site VPN AWS tags Amazon VPC	Entities can implement and audit trails through services such as CloudTrail, CloudWatch, and Amazon Athena. These logs provide detail to help show that controls are in place to securely handle BCSI.	

NERC CIP standard or AWS feature and description	AWS services, features, and resources	Customer considerations	AWS responsibility
Governance at Scale and Compliance at Scale AWS services that help support the management and implementation of CIP controls	AWS Audit Manager AWS CloudTrail AWS CloudWatch AWS Config AWS Control Tower Amazon GuardDuty AWS Management Console AWS Organizations AWS Security Hub Amazon SNS Operational Best Practices for NERC CIP BCSI Conformance Pack	Entities can use several AWS services that help with managing cloud assets at scale, referred to as "*Governance at Scale*." With AWS Control Tower, you can automate the setup of a multi-account AWS environment with just a few clicks. The setup uses blueprints that 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 you centrally manage and govern environments. Using AWS Organizations, an Entity can programmatically create new AWS	N/A

		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 your accounts. Entities can use AWS Security Hub to get a comprehensive view of their security alerts and posture across their accounts and organizations. With Security Hub, an Entity can aggregate, organize, and prioritize security alerts from multiple AWS services, and from AWS Partner Network (APN) solutions, in a single place. Entities can use AWS Audit Manager to continuously audit their AWS usage to help assess their risk and compliance with regulations and industry standards. Audit Manager automates evidence collection, helps manage stakeholder reviews of controls, and enables building audit-ready reports with less manual effort. Entities can use the AWS Config Operational Best Practices for NERC CIP BCSI conformance pack to perform continuous governance checks of their	

		environment, validating the security controls implemented.	

Appendix 2: AWS NERC CIP BCSI reference architecture

AWS developed a high-level NERC CIP BCSI reference architecture to visually represent the AWS services that can help support an Entity subject to NERC CIP Standards in developing and implementing a secure and compliant environment for BCSI. This document includes detailed explanations for the services described in the previous sections.

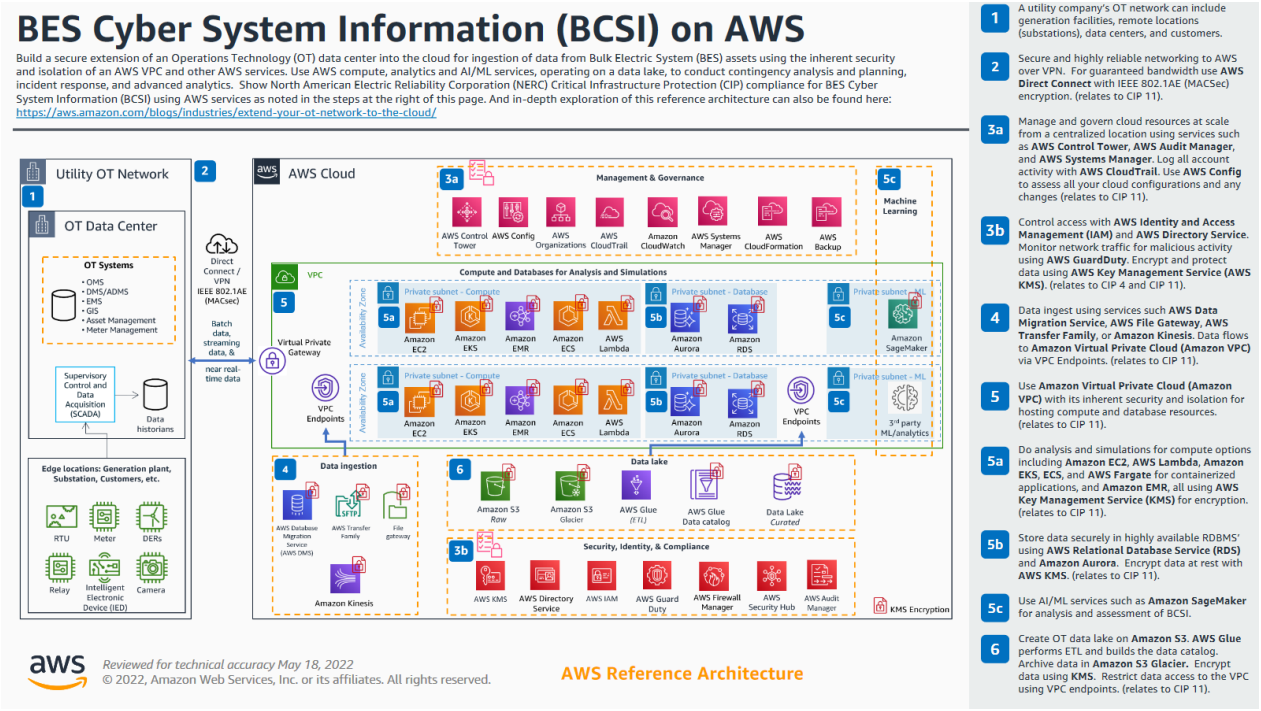

Figure 5: AWS NERC CIP BCSI reference architecture

There are two example architectures below that follow the reference architecture, including one server-based and one serverless example.

Appendix 3: Example use cases

Example 1: Server-based applications on AWS

Entities run many applications that host or use BCSI on a Windows or Linux server, with application servers for processing data, and database servers for storing data. Such server-based systems, often referred to as *n-tier applications*, can be used for many electric transmission, generation, and other utility-related use cases, such as asset management, GIS, predictive maintenance, and planning and contingency analysis systems. Entities can migrate these systems to AWS while demonstrating adherence with NERC CIP requirements for BCSI.

Why

N-tier applications on AWS can take advantage of high resilience, availability, scalability, and lower operational effort by using AWS features, such as Availability Zones, auto scaling, and automation scripts. In addition, Entities can extend the value of their data by creating data lakes and conducting analytics. They can use the latest in machine learning technologies to gain deeper insights and value from their data.

Architecture

Entities should design and architect their applications to be secure and highly available to minimize downtime in the event of a disaster. On AWS, you can help achieve these objectives by providing encryption at rest using AWS KMS and encryption in transit using TLS, and by deploying applications across multiple Availability Zones. Entities can access their servers in the AWS Cloud by establishing a secure VPN connection over AWS Direct Connect, which offers Entities a dedicated, high-bandwidth fiber connection to the AWS Cloud.

The following architecture shows how an Entity can deploy a server-based application hosting BCSI following AWS best practices and AWS Well Architected principles that focus on increasing performance, reliability, security, and operational excellence while controlling costs.

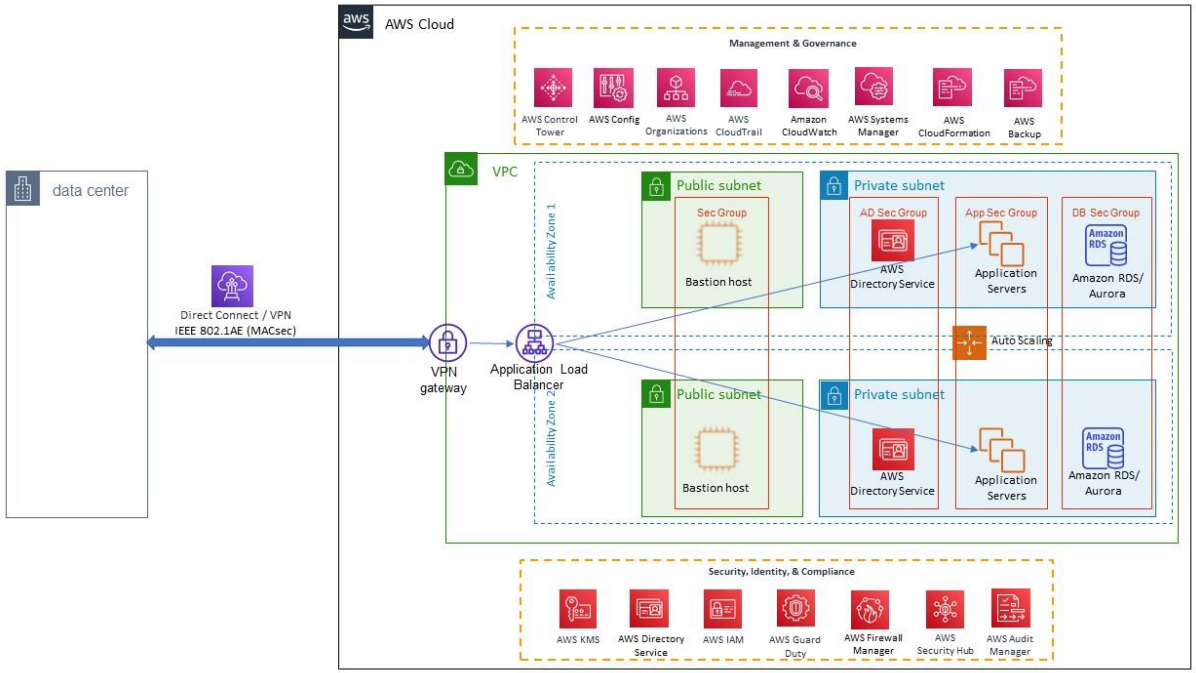

Figure 6: Example of server-based applications on AWS architecture

Some of the salient features of this architecture include the following:

1. Applications are placed across Availability Zones (AZs) and behind application load balancers. This configuration offers high availability and failover in the event of an infrastructure failure.

2. This configuration uses AWS Auto Scaling so that Entities can configure both the minimum servers required and a maximum, helping to ensure availability while providing the ability to scale up to handle larger workloads.
3. The database servers use AWS RDS or AWS Aurora in a multi-AZ configuration, providing high availability and resilience.
4. Storage media is encrypted by using AWS KMS, including data in the AWS RDS databases.
5. Communications between servers occurs over TLS using certificates issued from AWS Certificate Manager.
6. AWS offers many services that these servers can access. AWS PrivateLink helps to make communication between servers and AWS services private and encrypted—data never leaves AWS.
7. The AWS VPC used to host the servers is connected to the Entity's data center over DirectConnect using IEEE 802.1AE MACsec encryption or VPN using FIPS compliant algorithms through a virtual private gateway. In this architecture, the VPC has no access to the public internet. This VPC is now an extension of your on-premises data center.
8. The NERC CIP BCSI conformance pack template has been applied to AWS Config. AWS Config will notify you if a deviation from data protection occurs, such as storage media that has not been encrypted.
9. To continuously monitor its AWS environments, an Entity should configure Amazon GuardDuty to detect network anomalies. Entities should also consider using AWS Security Hub to help ensure that they are using security best practices.
10. Traffic between servers is restricted to specific ports using Security Groups.
11. Traffic to and from the on-premises data center is configured to specific CIDR by using the VPC's route tables.

High availability, disaster recovery, and continuity of operations

The preceding architecture offers high availability even if an Availability Zone becomes unavailable. This architecture has the following benefits:

1. An always on, active-active capability for disaster recovery and continuity of operations.
2. No failover or manual effort required if a disaster occurs. The system continues to operate.
3. No need for disaster recovery drills or exercises because the system is always on and in use.
4. No need to incur the cost of infrastructure that would be rarely used.

For protection against catastrophic regional events, an Entity can consider deploying the BCSI workloads to more than one AWS Region. This decision depends on the criticality of the application and the risk tolerance of the Entity. For more information, see the blog post How energy and utility companies can recover from ransomware and other disasters using infrastructure as code on AWS.

Example 2: Serverless applications on AWS

Transmission and generation operators might have BCSI information that can be ingested, stored, and processed on AWS using serverless services. Organizations use these services on AWS while meeting NERC CIP requirements for BCSI. Serverless applications on AWS can take advantage of scalability, higher resilience and availability, and lower operational effort while remaining secure.

Architecture

Entities can use Amazon Kinesis data streams to collect data in real-time from an operational technology system as a data source. The data is then processed using AWS Lambda and stored in Amazon S3. Entities can then use Amazon Athena to query the data stored in Amazon S3 and from there use Amazon Quicksight to visualize the data. Throughout this application, Entities can meet BCSI objectives by using AWS KMS for encryption at rest, and AWS Certificate Manager for encryption in transit. Entities can access their information in the AWS Cloud by establishing a secure VPN connection over AWS Direct Connect, which offers a dedicated, high bandwidth fiber connection to the AWS Cloud.

The following architecture demonstrates how Entities can deploy a serverless application that hosts BCSI information to help satisfy NERC CIP compliance requirements.

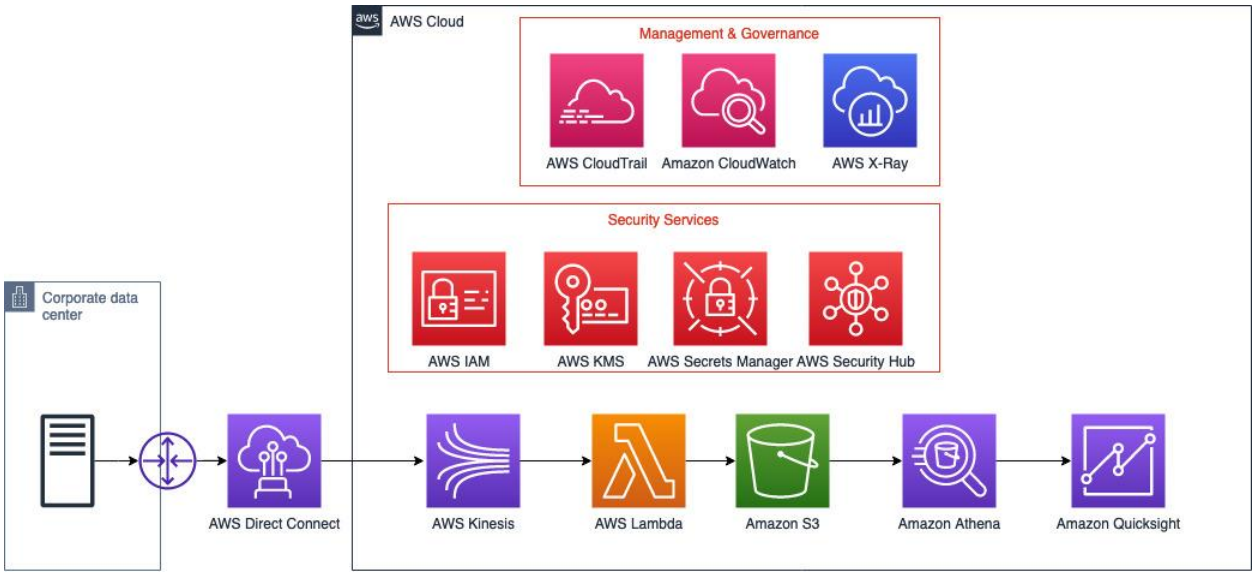

Figure 7: Example of serverless applications on AWS architecture

Some of the salient features of this architecture include the following:

1. IAM is used to manage access to AWS services.
2. Security Groups and route tables are configured to allow traffic between services.

3. Using Direct Connect with IEEE 802.1AE MACsec encryption or a VPN connection through a virtual private gateway helps to ensure there is no public internet connectivity between the operational technology network and AWS services.
4. AWS KMS is used to encrypt data at rest while the data is stored in Amazon S3.
5. Data ingestion occurs through Amazon Kinesis Firehose.
6. Lambda functions support TLS 1.2. Requests are signed with an access key ID and secret access key associated with an IAM principal.
7. Data stored in Amazon S3 is encrypted with an AWS KMS key.
8. Communications between AWS services are private and encrypted, and data never leaves AWS.
9. The NERC CIP BCSI conformance pack template is applied by using AWS Config. AWS Config notifies you if a deviation from data protection occurs, such as storage media that has not been encrypted.