ERO Enterprise Endorsed
Implementation Guidance

NERC Reliability and Security Technical Committee

Implementation Guidance:

Usage of Cloud Solutions for BES Cyber System Information (BCSI)

CIP-004-7 R6, parts 6.1-6.3
CIP-011-3 R1, parts 1.1 and 1.2

June 21, 2023

Table of Contents

Introduction

NERC "Implementation Guidance provides a means for registered entities to develop examples or approaches to illustrate how registered entities could comply with a standard [or requirement within a Standard] that are vetted by industry and endorsed by the ERO Enterprise. The examples provided in the Implementation Guidance are not exclusive, as there are likely other methods for implementing a standard."[1] This Implementation Guidance document was developed to outline considerations and potential approaches that a registered entity could utilize to comply with CIP-011-3 R1 and CIP-004-7 R6. Both of these standards were modified to clarify and provide a secure path towards utilization of modern third-party off-premises electronic data storage and analysis systems (e.g., cloud services).

Figure 1 illustrates the high-level relationship between CIP-011-3 R1 and CIP-004-7 R6, and explains why you will see guidance on CIP-011-3 R1 before CIP-004-7 R6 within this document:

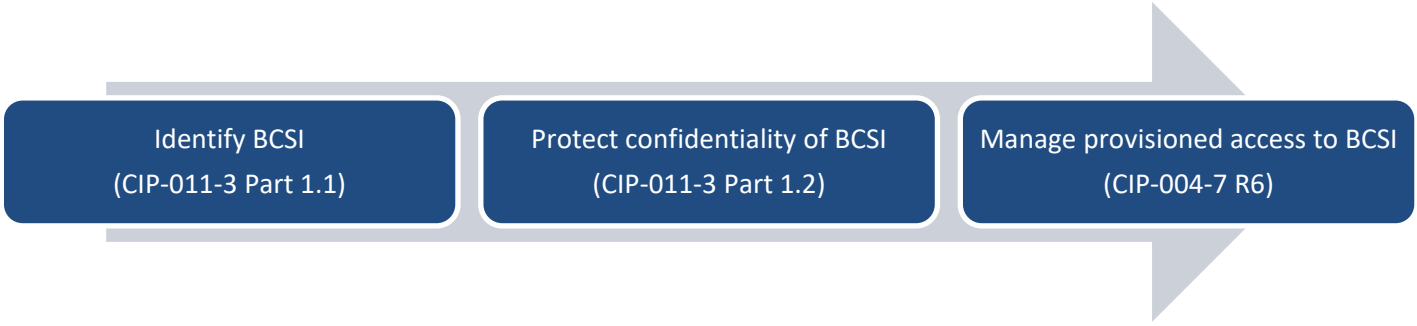


Figure 1 - Relationship between CIP-011-3 R1 & CIP-004-7 R6

Figure 2 is an excerpt from the U.S. General Services Administration (GSA) Cloud Information Center's (CIC) publication on Cloud Security, and is helpful to better understanding the various cloud services. The GSA CIC acts as a centralized location to share guidance and best practices on cloud-related topics with federal agencies, including security, without bias toward particular cloud contract vehicles, vendors or solutions. The publication states:

> "When it comes to cloud, security is always a concern, and should be appropriately addressed by any organization (e.g., consumer) evaluating or using a cloud solution.
>
> The following graphic illustrates the differences in security responsibilities between cloud consumers and Cloud Service Providers (CSPs) for each cloud service model (IaaS, PaaS, SaaS) in comparison to an organization owned and managed data center."

[1] NERC Compliance Guidance Policy, November 5, 2015, available at: https://www.nerc.com/pa/comp/guidance/Documents/Compliance Guidance Policy.pdf

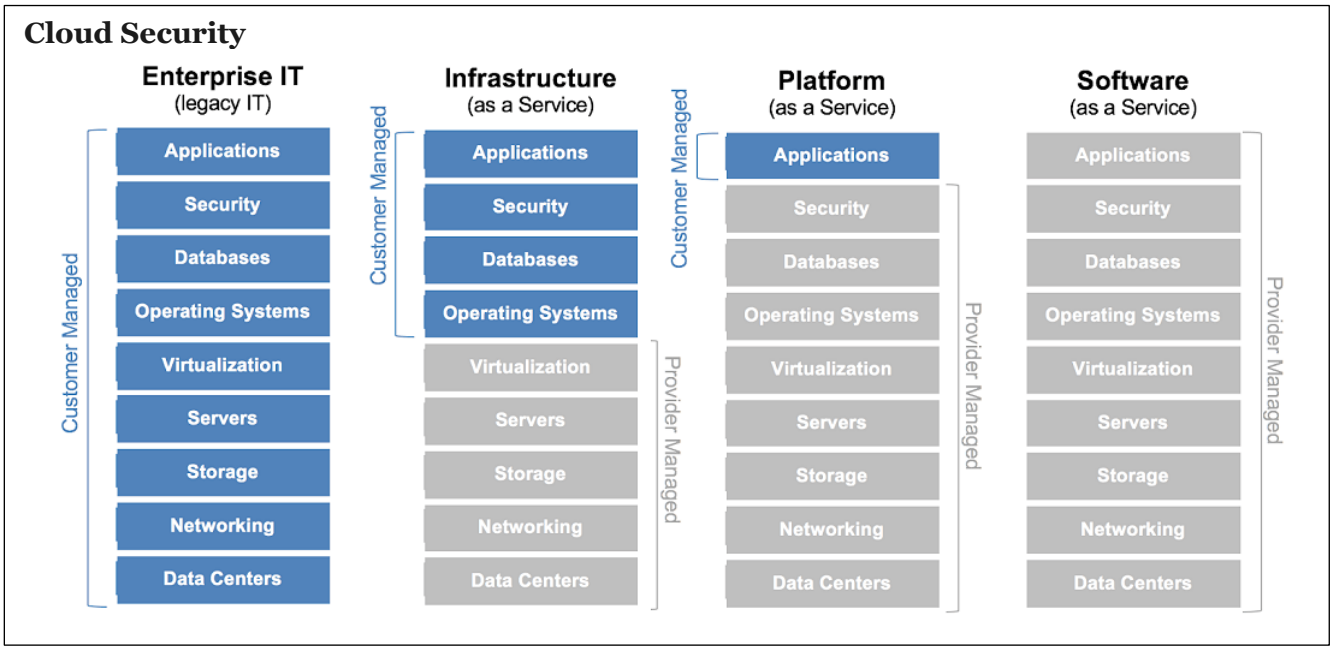


Figure 3 – Security responsibilities by cloud service model

The figure above depicts the typical division of security responsibilities in a cloud environment; however, these roles and responsibilities do not suggest or imply transference of compliance responsibilities from the Responsible Entity to a third-party. Responsible Entities are the data owners. As owners of the data, they must ensure the custody and handling of that data have the required security controls applied to their environment(s) inclusive of third-parties; and Responsible Entities must have the ability to demonstrate compliance with CIP-004-7, and CIP-011-3. Demonstration of compliance is described in further sections but may include a combination of electronic technical controls, and/or implementation of administrative methods to protect BCSI.

Additionally, any mention of specific vendors and their services in this document is not considered an endorsement of any kind. The scenarios referenced under each Requirement are intended to illustrate security concepts and the compliance impacts associated with each.

Goal/Problem Statement

Many vendors are phasing out their on-premises solutions and migrating them to the cloud or building new solutions using only cloud services/environments. Responsible Entities also need increased choice, greater flexibility, higher availability, and reduced-cost options to manage their BCSI, which includes the use of third-party off-premises cloud solutions. Understanding security and compliance in these new and sometimes complex environments has been a common challenge in the industry. In particular, understanding how and whether CSP personnel and/or any third-party service provider have access to BCSI, and the associated compliance impacts, requires a full understanding of the environment and available protections (technical or administrative).

Scope

This Implementation Guidance has been developed to provide examples of the protection and access management of BCSI, in an off-premises cloud environment. In some cases, guidance is provided for the following three NIST-defined cloud service offering models:

- **Software as a Service (SaaS)** – The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
    - In this model, the application provider may contract with a cloud service provider (CSP) to host the application, or the application provider may own, manage and operate their own cloud environment. Either way, all of the underlying infrastructure, middleware, app software and app data are located in the cloud provider's data center and managed by the application provider.

- **Platform as a Service (PaaS)** – The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

- **Infrastructure as a Service (IaaS)** – The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

This document outlines considerations and potential approaches that a Responsible Entity could utilize to comply with CIP-011-3 R1 and CIP-004-7 R6, however, is not intended to be exhaustive considering the numerous services available and implementation choices. For example, the document does not include specific examples for use of data masking, whitelisting/blacklisting of IP ranges, etc., although Responsible Entities may choose to implement those controls in lieu of, or in addition to, those described in this document as part of their Information Protection Program.

Operations of a PACS (Physical Access Control System), EACMS (Electronic Access Control or Monitoring System) or BCS (BES Cyber System)[2] in the cloud is not addressed in this guidance.

This document is not intended to establish new requirements under NERC's Reliability Standards, modify the Requirements in any existing Reliability Standards, nor provide an interpretation under Section 7 of the Standard Processes Manual.

Definitions

- **Cloud:** Off-premises servers that are accessed over the Internet, and the software and databases that run on those servers[3].
- **Cloud Service Provider (CSP):** Third-party or parties involved in hosting the Responsible Entity's BCSI service in an off-premises cloud. This can be the application/software provider, the cloud platform provider, the underlying infrastructure host and/or third-party services. In some cloud implementations, there is more than one CSP involved.
- **Just-In-Time Access:** a security practice/control where the privilege granted to temporarily access applications or systems is limited to predetermined periods of time, on an as-needed basis.
- **Underlay (security of the cloud):** Infrastructure implemented by the CSP that runs all services offered by the CSP. This infrastructure could comprise the hardware, software, networking, and facilities that run cloud services. The security controls associated with this infrastructure are likely verified through certifications or other internal/external activities such as penetration testing.
- **Overlay (security in the cloud):** The portion of the cloud service/product that sits on top of the underlay and is developed by the customer or has been developed for the customer's use. This is how the Responsible Entity generally accesses their BCSI.

[2] See the NERC Glossary of Terms for definitions of PACS, EACMS and BCS: https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf

[3] For more detail, please refer to this Cloudflare, Inc. article: https://www.cloudflare.com/learning/cloud/what-is-the-cloud/

Depending upon a Responsible Entity's implementation and specific services, its BCSI may reside within the Overlay (as is more common with SaaS) or may reside in the Underlay (as is more common in a PaaS or IaaS implementation). Figure 3 is a generalized diagram of a cloud environment depicting the division between the Overlay and Underlay.

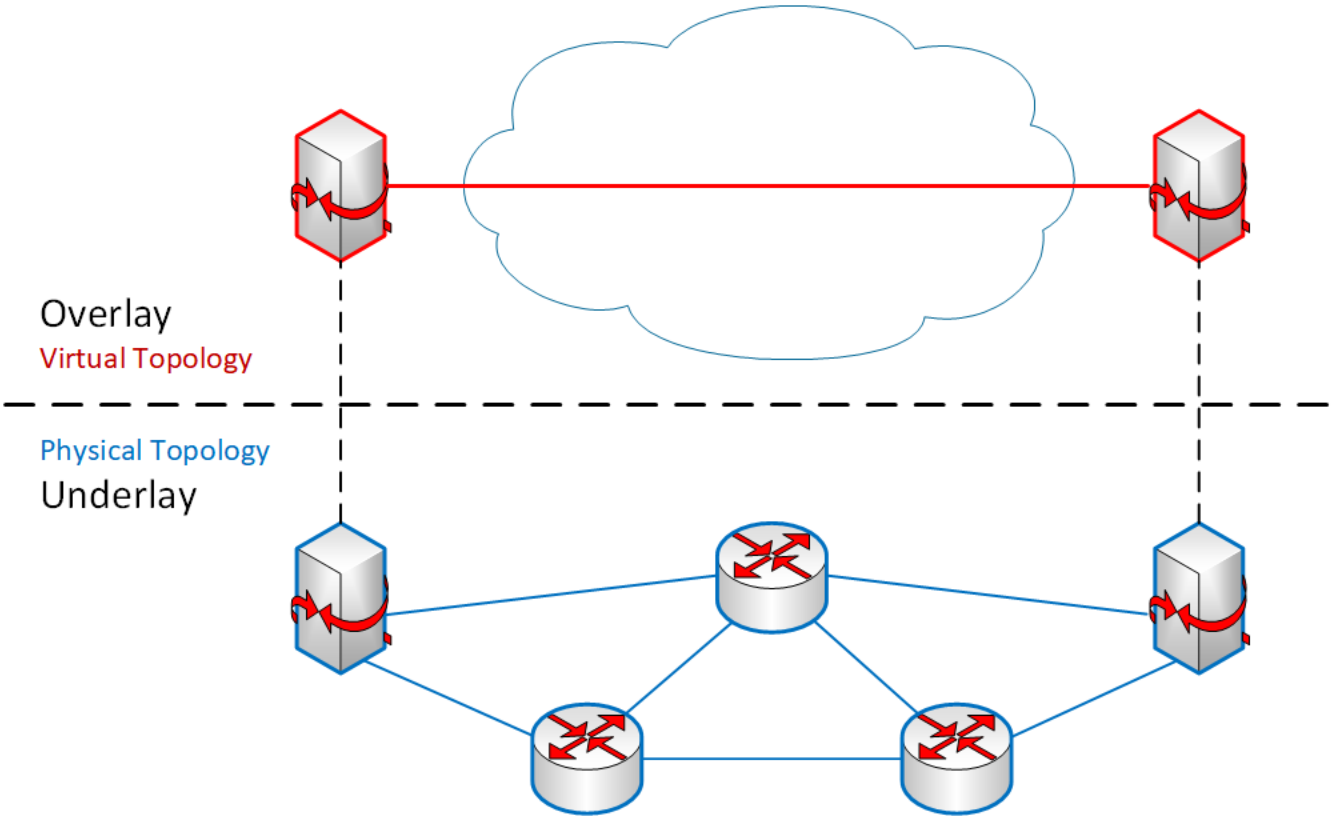


Figure 3 – Example diagram of a cloud environment to depict the division between the Overlay and Underlay

CIP-011-3 – Cyber Security – Information Protection

Requirement R1

R1. Each Responsible Entity shall implement one or more documented information protection program(s) for BES Cyber System Information (BCSI) pertaining to "Applicable Systems" identified in CIP-011-3 Table R1 – Information Protection Program that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection Program.

Requirement R1, Part 1.1

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify BCSI.	Examples of acceptable evidence may include, but are not limited to, the following: • Documented method(s) to identify BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify BCSI; or • Storage locations identified for housing BCSI in the entity's information protection program.

As indicated in the last bullet of the Measures, a Responsible Entity may still utilize "designated storage locations" as a method to identify BCSI, as contemplated in CIP-004-6. As it relates to a cloud environment, an example of this could be a specific site or folder within an application that has been designated as a BCSI repository.

However, a Responsible Entity may utilize other options within a cloud environment to identify BCSI. Some examples include, but are not limited to:

- File-level tagging via metadata or labels,
- Application-level whereby the entire application has been designated as a BCSI storage location,
- A designated container/space within a CSP-provided environment.

Requirement R1, Part 1.2

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Examples of evidence for on-premise BCSI may include, but are not limited to, the following: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BCSI; or • Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premise BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or • Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

Following are conditions that Responsible Entities should consider when implementing Part 1.2:

- If BCSI is not encrypted, only password protection of the storage hardware alone may not be sufficient protection. In this situation, a Responsible Entity should address physical and administrative protection of electronic BCSI.
- If CSP personnel has access to BCSI in the Overlay and/or the Underlay, then this should be accounted for and addressed by the Responsible Entity's Information Protection Program.
- Responsible Entities need to understand and identify how personnel (CSP or their own) can obtain access to BCSI in the Overlay and/or the Underlay. For example:
    - eDiscovery tools typically utilized by legal staff,

- Administrator roles within the cloud environment that provide access to BCSI,
- Emergency/ Break-Glass accounts that provide access to BCSI.

- Responsible Entities would need to understand and address how BCSI is being protected if in a multi-tenant environment (e.g. encryption, authentication to AD, etc.)

Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS)

The Measures for part 1.2 provide examples of the evidence that could be utilized to demonstrate compliance. More specific compliance evidence examples could include but are not limited to:

1. Implementation of electronic technical method(s) to protect BCSI:
   a. This could include evidence of encryption keys utilized at a container or application/software-specific level. Entities should also ensure the level of encryption used by default or that can be configured follows encryption best practices[4]. Additional technical methods may be needed depending on how the encryption keys are managed:
      i. Vendor-owned and managed keys: Detection/notification controls could be implemented to ensure that the keys are not utilized when not authorized by the Responsible Entity.
      ii. Customer-owned keys – managed within the cloud vault: Detection/notification controls could be implemented to ensure that the key vault is not accessed without authorization by the Responsible Entity.
      iii. Customer-owned keys – managed on-premises or in a separate cloud: Service contract and diagram showing how the keys to fully unencrypt BCSI is not stored in the cloud with the BCSI.
      iv. Customer-owned keys – cloud-based Hardware Security Module (HSM) with Federal Information Processing Standards (FIPS) level 4 protection (tamper-resistant controls): Service contract and CSP procedure to explain how the keys are managed.
   b. Access control Lists
   c. Data masking/ anonymization
   d. Multi-factor authentication
   e. Technical tools that prevent BCSI from being transmitted in clear text outside of an encrypted container (e.g. inability to attach documents to email, automated scan of documents attached to emails prior to sending, etc.)
   f. Utilizing a distributed model for data storage, where the Responsible Entity's data is split up across multiple locations (e.g. Blockchain)
2. Implementation of administrative methods to protect BCSI:
   a. Vendor service agreements and/or vendor service risk assessments that specifically address the confidentiality of the Responsible Entity's information or specifically address the CSP's access management controls/obligations.

[4] One source for cyber industry encryption best-practice information is Federal Information Processing Standards (FIPS) 140-2.

b. Vendor's certification, including security controls that reduces the risks of compromising the confidentiality of Responsible Entity's BCSI; and third-party audit reports providing reasonable assurance/confirms that those security controls are effective and being followed, such as FedRAMP Audit reports, SOC 2 Type 2 reports or similar.
c. Electronic banners to remind personnel of certain handling actions to either take or not take in order to ensure the confidentiality of BCSI.

CIP-004-7 – Cyber Security – Personnel & Training

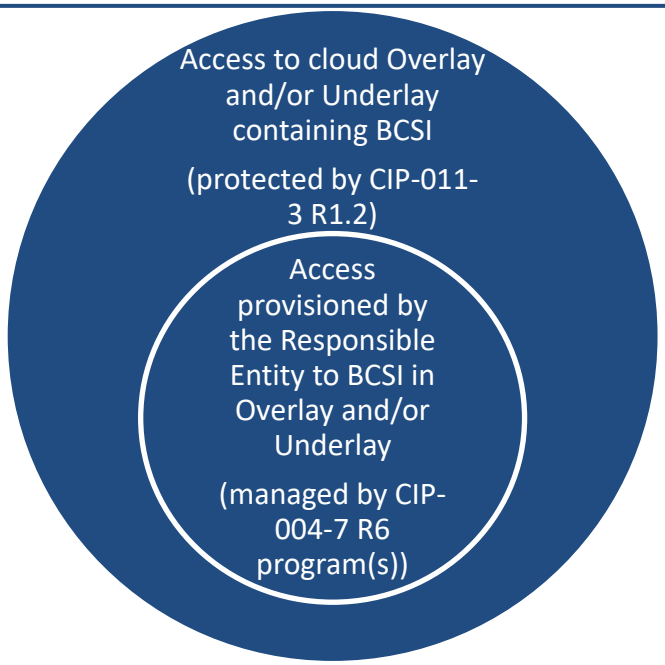
Requirement R6

> R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable Systems" identified in CIP-004-7 Table R6 – Access Management for BES Cyber System Information that collectively include each of the applicable requirement parts in CIP-004-7 Table R6 – Access Management for BES Cyber System Information. 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).

Depending upon a Responsible Entity's implementation and specific services, its BCSI may reside within the Overlay (as is more common with SaaS) or may reside within the Underlay (as is more common with PaaS and IaaS). As it pertains to an off-premises cloud environment, the Responsible Entity may document within its access management program(s) that provisioned access pertains to access to BCSI in the Overlay and/or Underlay that is authorized by the Responsible Entity. They may also further clarify that this does not include:

- access to information within the Overlay and/or Underlay, which includes BCSI, that is authorized by the CSP for their personnel (such as may be needed for workflow management, etc.) This should be addressed by the Responsible Entity's CIP-011-3 Information Protection Program.
- Access to the Underlay that may be needed by CSP personnel for maintenance (patching, updates, etc.) of the Underlay infrastructure. This should be addressed by the Responsible Entity's CIP-011-3 Information Protection Program.

This diagram depicts at a high-level how access to a Responsible Entity's Overlay and/or Underlay (containing BCSI) could be protected between CIP-004-7 R6 and CIP-011-3 R1:



Requirement R6, Part 6.1

CIP-004-7 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI.	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

Following are conditions that Responsible Entities should consider when implementing Part 6.1:

- A Responsible Entity should assess and account for all entities (i.e. CSP, Responsible Entity) for which it is authorizing BCSI access in the Overlay and/or Underlay, including external parties, in order to ensure all "provisioned access" is identified and authorized; in some implementations this could be multiple parties (for example but not exhaustive: for IaaS, CSP only; for SaaS, software/application provider and CSP if the software/application provider is using a CSP other than itself; for PaaS, platform provider, application provider(s), and CSP)

- Evaluate and identify any shared accounts that are provisioned access to BCSI and ensure individuals are authorized to those accounts. An example of shared accounts in a cloud environment could include emergency or break-glass accounts.

Example compliance approaches have been detailed below, organized by service type and specific example scenarios.

Software as a Service (SaaS) – BCSI is in the Overlay, not Underlay

1. Scenario 1: CSP personnel do not have persistent access to BCSI. CSP personnel may have persistent access to the Responsible Entity's environment/container, but not to the BCSI due to implemented controls. CSP access to BCSI is permitted and controlled by the Responsible Entity with a "Just-In-Time" process. Compliance evidence examples could include but are not limited to:
    a. Documentation of the "Just-In-Time" process and that it has been activated/enabled.
    b. Documentation of each "Just-In-Time" session including the business need, start and end date, and the Responsible Entity's approval. Examples of evidence sources include but are not limited to: 1) the customer/Responsible Entity's ticketing system, 2) "Just-In-Time" usage logs, and 3) customer/Responsible Entity Overlay security and/or audit logs.
2. Scenario 2: The Responsible Entity authorizes CSP personnel to have persistent access to BCSI. This could consist of access to BCSI in clear text or where the individual has access to the encrypted BCSI and the key(s) to unencrypt it. Compliance evidence examples could include but are not limited to:
    a. Documented process for how CSP personnel provisioned access is authorized based on need, whether authorized directly by the Responsible Entity or indirectly by a contractual agreement with the CSP, and one of the following
        i. List of CSP personnel with provisioned access. This would include 1) access to BCSI in clear text, and 2) access to both encrypted BCSI and the encryption keys.
        ii. Authorization records for CSP personnel access. This could include procedural authorization (such as in an access management program/procedure for specific groups of personnel), or individual records of authorization (such as in-service tickets, Just-In-Time access requests, etc.)
        iii. If i. and ii. are not available to the Responsible Entity, then third-party audit reports providing reasonable assurance/confirms that the documented authorization process is being followed could be utilized. This could include FedRAMP audit reports, SOC 2 Type 2 reports or similar.
3. Scenario 3: CSP personnel cannot access BCSI. In this scenario, CSP personnel would not have the possibility of obtaining provisioned access, however compliance auditors may want to verify for reasonable assurance. Compliance evidence examples could include but are not limited to:
    a. Diagram(s), processes and/or narrative depicting how CSP personnel are prevented from accessing BCSI. Diagram(s) may include Entity-specific cloud architecture diagrams

for the environment hosting BCSI, and/or diagrams provided by the CSP describing their security controls.

b. Evidence of implementation of technical controls preventing CSP personnel from accessing Entity BCSI including: Application programming interface (API) calls identifying who has access to resources owned by the Entity in the cloud environment and associated API logs, evidence of encryption controls implemented by the Entity including access to/management of encryption keys, identity and access management policies implemented by the Entity controlling access to Entity BCSI and list of users.
c. Business Agreements and/or Contracts that include clauses related to customer data privacy and protections as described in the diagram processes, and/or narrative.

Platform as a Service (PaaS) – BCSI can be in the Overlay and Underlay, depending upon the implementation of cloud services

Evidence examples provided under SaaS apply here as well. However, entities need to understand and account for platform providers if the Responsible Entity provisions their access to the Overlay, which may be different than the application/software provider.

Infrastructure as a Service (IaaS) – BCSI can be in the Overlay and Underlay, depending upon the implementation of cloud services

Evidence examples provided under SaaS apply here as well. However, entities need to understand and account for infrastructure providers if the Responsible Entity provisions their access to the Overlay, which may be different than the application/software provider.

Requirement R6, Part 6.2

Part	Applicable Systems	Requirements	Measures
6.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • List of authorized individuals; • List of individuals who have been provisioned access; • Verification that provisioned access is appropriate based on need; and • Documented reconciliation actions, if any.

Following are conditions that Responsible Entities should consider when implementing Part 6.2:

- Where shared cloud accounts permit access to BCSI, such as those utilized for break glass or emergencies, the Responsible Entity should ensure that the individuals provisioned access to these

accounts are evaluated as part of this review. This implies that the Responsible Entity has a process for authorization to the shared cloud accounts.

- Exception reporting is commonly found in a cloud environment and could be utilized as evidence for part 6.2.1, however the Responsible Entity should be prepared to demonstrate/show the logic behind the report to ensure all provisioned access is being included and compared to authorization records. In this case, a separate process would be needed to verify the continued need for access for compliance with part 6.2.2.

Software as a Service (Saas), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS)

The Measures for part 6.2 provide examples of the evidence that may be utilized to demonstrate compliance. Below are specific examples that may be available/utilized, as it relates to a cloud service and how access is managed:

1. Scenario 1: Responsible Entity performs all access provisioning to BCSI in the Overlay.
    a. List of authorized individuals:
        i. Output from the Responsible Entity's identity and access management system or other similar access management processes.[5]
    b. List of authorized individuals who have been provisioned access:
        i. Report or screenshot of accounts and/or roles within the cloud service that have provisioned access to BCSI
        ii. If all accounts authenticate to the Entity's on-premises active directory, then a report or screenshot of all active directory accounts that have provisioned access to BCSI within the cloud service
    c. Verification that provisioned access is appropriate based on need:
        i. Output from the Responsible Entity's access management system/process showing verification that the access is still appropriate based on need.
        ii. Evidence of an access review by each individual's manager attesting that access is still appropriate based on need.
        iii. Evidence of an access review of each role and the associated individuals with provisioned access. This review should include an evaluation that the role's access is still appropriate based on need and that the individuals assigned to the role are still appropriate for their current work function(s).
    d. Documented reconciliation actions, if any:
        i. Dated documentation comparing the list of who has been provisioned access in the source system against the list of who has been authorized, the identification of any deltas between the two lists, and the corrective actions taken.
        ii. Exception reports showing only deltas (or null results) between provisioned access and authorization; in addition, evidence of the logic/configuration behind the exception report.

[5] Where a Just-In-Time process is utilized for CSP personnel access, this would include any such active access session at the time of the review.

iii. Additional evidence demonstrating corrective actions were taken could include, but are not limited to:
    1. Completed tickets from the Responsible Entity's tracking system showing that corrective action was taken.
    2. Email instruction from the reviewer to the asset owner to take corrective action.

2. Scenario 2: CSP performs all access provisioning to BCSI in the Overlay, after authorization has been provided by the Responsible Entity.
    a. A documented process on how the CSP reviews provisioned access at least once every 15 months, and
    b. Records of the review process, or third-party audit reports providing reasonable assurance/confirms that the review process is being followed (such as FedRAMP Audit reports, SOC 2 Type 2 reports or similar).
3. Scenario 3: Hybrid Responsible Entity performs all access provisioning for their personnel, and the CSP performs all access provisioning for the CSP personnel.
    a. Please refer to the examples provided for scenarios 1 & 2 above

Requirement R6, Part 6.3

6.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

Following are conditions Responsible Entities should consider when implementing Part 6.3:

- Responsible Entities should have a clear understanding as to how provisioned access to BCSI is revoked in the cloud. For example, if access is revoked via a connection from the Responsible Entity's active directory to the cloud active directory, then the Responsible Entity should review the synchronization cycles to ensure they occur frequent enough to meet the end of the next calendar day in all scenarios.
- If emergency/break-glass accounts are used, particularly if they do not authenticate back to the Responsible Entity's active directory, then the Responsible Entity should consider and address how to ensure a terminated individual's ability to use provisioned access to BCSI via those account credentials is revoked. For example, if the credentials are believed to be known to the individual, the Responsible Entity could change the password to those accounts as a means to remove their ability to access BCSI.

Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS)

The Measures for part 6.3 provide an example of the evidence that may be utilized to demonstrate compliance. Below are some more specific evidence examples that may be available/utilized, as it relates to a cloud service and how access is managed:

1. Scenario 1: Responsible Entity performs revocation of all provisioned access to BCSI in the Overlay. Examples of evidence may include but are not limited to:
    a. Evidence demonstrating the termination effective date for the individual.
    b. Access revocation record from the cloud audit log showing date and time when access for the terminated individual was revoked.
    c. Completed and dated ticket showing action taken to revoke a terminated individual's access.
    d. If the terminated individual's account(s) authenticates to the Responsible Entity's on-premises active directory, then a report or record showing when the individual's active directory account was disabled; in addition, evidence of the active directory synchronization setting/configuration.
2. Scenario 2: CSP performs revocation of all provisioned access to BCSI in the Overlay. Examples of evidence may include but are not limited to:
    a. Evidence demonstrating the termination effective date for the individual.
    b. A documented process on how the CSP terminates provisioned access before the end of the next calendar day, and either 1) dated records of the provisioned access revocation or, 2) audit reports validating that the provisioned access revocation process is being followed, such as FedRAMP Audit reports, SOC 2 Type 2 reports or similar.
    c. Access revocation record from the customer/Responsible Entity's Overlay security and/or audit logs showing date and time when access for the terminated individual was revoked.
    d. Completed and dated ticket showing action taken to revoke a terminated individual's access.
    e. If the terminated individual's account(s) authenticates to the CSP-managed cloud application active directory, then a report or record showing when the individual's active directory account was disabled.
3. Scenario 3: Hybrid performance of revocation: Responsible Entity revoked all provisioned access to BCSI in the Overlay for their personnel, and the CSP revokes all provisioned access to BCSI in the Overlay for the CSP personnel.
    a. Refer to the examples provided for scenarios 1 & 2 above.

Periodic Review

This document will be reviewed and updated upon initiation of a standards development project to modify the CIP-004-7 and/or the CIP-011-3 Standard, or as the need to modify has been determined by the NERC Security Working Group or Reliability and Security Technical Committee.

Appendix A –Examples of Cloud Services

To aid readers in better understanding the three models of cloud service, below are some examples of current services in the market. (Note: The services in this list will likely change over time.) Please note that this list should not be considered as an endorsement of any kind.

Software as a Service (SaaS)

- Web-based email services such as Outlook and Gmail
- Microsoft 365 (includes apps such as SharePoint Online, Exchange Online, Teams, etc.)
- ServiceNow Enterprise CX (IT asset inventory and ticketing system)

Platform as a Service (PaaS)

- Microsoft Azure
- ServiceNow Now Platform
- SAP Cloud
- AWS Elastic Beanstalk
- Google App Engine

Infrastructure as a Service (IaaS)

- Amazon Web Services (AWS)
- IBM Cloud
- Microsoft Azure
- Commvault Backup & Recovery
- Faction