NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Security Guideline

Electric Sector: Primer for Cloud and BCSI Protection

May 1, 2025

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

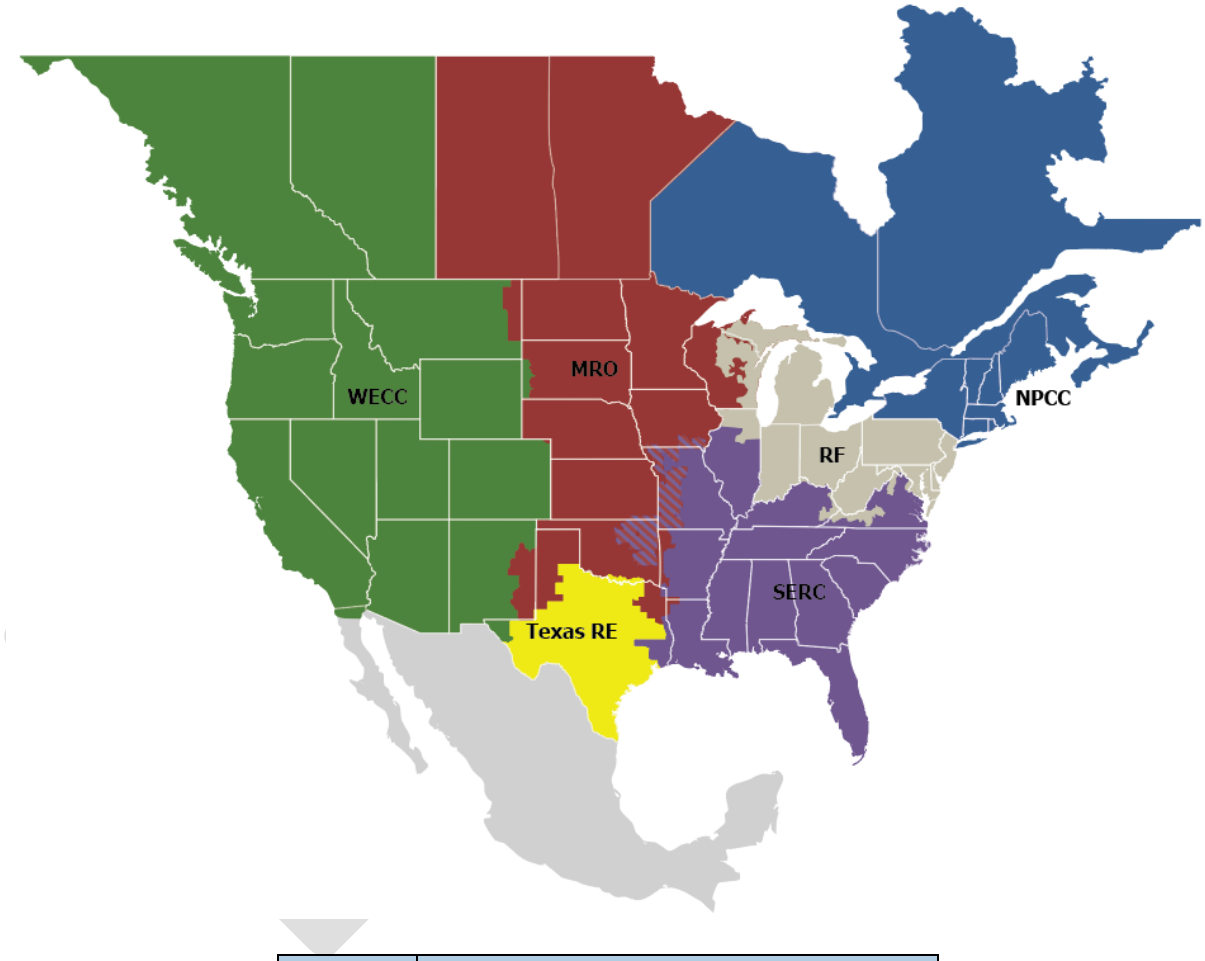
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the NERC and the six Regional Entities, is a highly reliable, resilient, and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six Regional Entities as shown on the map and in the corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Preamble

The NERC Reliability and Security Technical Committee (RSTC), through its subcommittees and working groups, develops and triennially reviews reliability guidelines in accordance with the procedures set forth in the RSTC Charter. Reliability guidelines include the industry's collective experience, expertise, and judgment on matters that impact BPS operations, planning, and security. Reliability guidelines provide key practices, guidance, and information on specific issues critical to promote and maintain a highly reliable and secure BPS.

Each entity registered in the NERC compliance registry is responsible and accountable for maintaining reliability and compliance with applicable mandatory Reliability Standards. Reliability guidelines are not binding norms or parameters nor are they Reliability Standards; however, NERC encourages entities to review, validate, adjust, and/or develop a program with the practices set forth in this guideline. Entities should review this guideline in detail and in conjunction with evaluations of their internal processes and procedures; these reviews could highlight that appropriate changes are needed, and these changes should be made with consideration of system design, configuration, and business practices.

Executive Summary

This document provides supplemental information for the ERO Enterprise-endorsed *Implementation Guidance: Usage of Cloud Solutions for Bulk Electric System (BES) Cyber System Information (BCSI)*, which provides guidance on using encryption to protect and restrict access to BCSI in a cloud environment. This primer presents basic cloud concepts, including the principles of information protection.

This document is not intended to establish new requirements under NERC's Reliability Standards, modify the requirements in any existing Reliability Standards, or provide an interpretation under Section 7 of the Standard Processes Manual. This guidance does not address the operation of a BES cyber system (BCS), associated physical access control system (PACS), or electronic access control or monitoring system (EACMS) in cloud environments. Other options may exist to fulfill the obligations of the requirements that are not expressed in this document.

The technical information in this document is intended to increase understanding of how encryption can provide additional protection for BCSI when used in conjunction with access controls and other critical infrastructure protection (CIP) requirements.

Chapter 1: Concepts

Data Versus Information

While cloud computing terminology is often focused on data, NERC's definition of BCSI is focused on information. At a high level, data is the raw material, and information is the finished product. Information and data differ in their level of processing and usability. When data is processed and organized in a useful way it is known as 'information.' Definitions are provided as follows:

- **Data:** Raw, unstructured, unorganized facts and figures without context or meaning; the basic input that has not been processed yet
- **Information:** Processed, organized, or structured data that is meaningful and can be used to make decisions or gain insights

"The Cloud"

Cloud computing[1] uses remote servers and appliances hosted in internet-accessible locations to store, manage, and process data (as opposed to local on-premises networks). This equipment is operated and hosted by third-party organizations known as cloud service providers (CSP), including Microsoft Azure, Amazon Web Services, and Google Cloud Platform. These companies provide virtual access to their devices using a "pay-per-usage" model, allowing customers to reduce capital investments and pay only for necessary resources.

Cloud computing has revolutionized data management and processing for organizations representing all industry verticals. Cloud computing's benefits include scalability, flexibility, and cost reduction. Diverse cloud service offerings allow customers (aka tenants) to scale up or down on demand quickly, and users can access data and applications globally using the internet.

The National Institute of Standards and Technology (NIST) Definition of Cloud Computing (NIST-SP 800-145[2]) defines four cloud-deployment models:

- **Private Cloud:** Cloud infrastructure provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). The organization, a third party, or some combination may own, manage, and operate the infrastructure, which may exist on or off premises.
- **Community Cloud:** Cloud infrastructure provisioned for exclusive use by a specific community of consumers from organizations with shared concerns (e.g., mission, security requirements, policy, and compliance considerations). One or more organizations in the community, a third party, or some combination may own, manage, and operate the infrastructure, which may exist on or off premises.
- **Public Cloud:** Cloud infrastructure provisioned for open use by the general public. A business, academic, government organization, or some combination may own, manage, and operate the infrastructure on the cloud provider's premises.
- **Hybrid Cloud:** Cloud infrastructure is made up of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

While organizations and other users share public clouds, private clouds remain dedicated to a single entity. Hybrid clouds combine these types, allowing organizations to leverage private cloud capabilities to provide additional protection for sensitive data/information (like BCSI) while using the public cloud for less-sensitive information.

[1] See the **References** section for the NIST definition of cloud computing and other details.
[2] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

Cloud Services

CSPs offer a variety of cloud services. The three primary NIST-defined cloud service types are as follows:

- **Software as a Service (SaaS)**
  In this model, the CSP provides entities with access to applications running on a cloud infrastructure. Application vendors may own, manage, operate, and maintain their own cloud environment or contract directly with CSPs to host their software for tenant access. These applications are accessible from various client devices using "thin client" architecture[3] or program interfaces (e.g., web-based email, trouble ticketing services, collaborative document editing, and online meeting platforms). Such applications usually maintain constant real-time communication and coordination to ensure synchronization between end users' interfaces and cloud services.

  Entities do not manage or control the underlying cloud infrastructure except for essential user permission and application settings. The application provider manages the underlying infrastructure, middleware, application software, and application data in the CSP data center, while the CSP manages the networks, servers, appliances, operating systems, storage, or individual application capabilities. A typical example of SaaS would be simultaneously editing or reviewing documents using online office productivity applications, accessing cloud backup and storage, and leveraging persistent near real-time communication between the CSP infrastructure and end-user devices.

- **Platform as a Service (PaaS)**
  This model allows entities to deploy applications onto the cloud infrastructure using programming languages, libraries, services, and tools the provider supports onto the cloud infrastructure. The CSP manages the underlying cloud infrastructure, including network, servers, operating systems, or storage. Customers have control over the deployed applications and possibly the configuration settings for the application-hosting environment. Organizations may leverage PaaS to host web-based services or applications during their development, testing, and production.

- **Infrastructure as a Service (IaaS)**
  This model, sometimes called "path, ping, operating system, and infrastructure," refers to the outsourced delivery of computer infrastructure to support the customer's operations. The customer has the capability to provision processing, storage, networks, and other fundamental computing resources needed to deploy and run software. When the CSP manages the hardware, storage, network components, and/or data center space, the product is considered IaaS. A common example would be the CSP managing the underlying infrastructure while the customer controls operating systems, storage systems, deployed applications, and optional networking components (e.g., host-based firewalls). A common use case for IaaS would be for backing up business records off-premises backup and storage, and would encrypt sensitive data/information (e.g., BCSI) both when it is stored ("at rest") and during transmission between the CSP and the customer.

Shared Responsibility Model

Figure 1.1 is taken from the National Security Agency's March 2024 cyber security information sheet (*Uphold the Cloud Shared Responsibility Model*)[4] to illustrate the typical division of security responsibilities between the CSP and the customer for each cloud service model.

[3] Thin clients are designed to be simple, often lacking local storage and processing power, relying instead on a central server for most of their computing needs.

[4] NSA CSI: Uphold the Cloud Shared Responsibility Model, dated March 2024: https://media.defense.gov/2024/Mar/07/2003407863/-1/-1/0/CSI-CloudTop10-Shared-Responsibility-Model.PDF

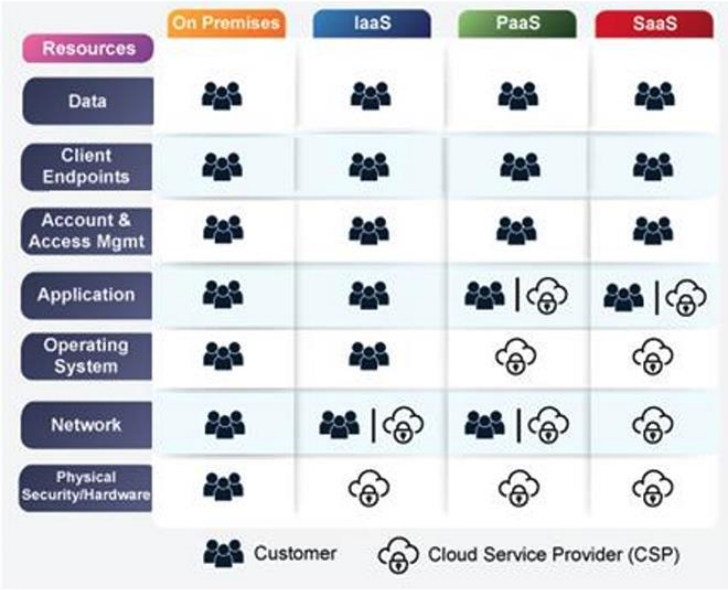


Figure 1.1: Cloud Service Model Security—Division of Responsibilities

The publication states that both the customer and the CSP are accountable for securing cloud environments and that understanding and upholding these partnership responsibilities is necessary for good cloud security results. A registered entity must understand what security measures it can implement to help minimize risks and ensure the confidentiality of its BCSI. (Note: This security guideline is focused on cloud security responsibilities, not NERC CIP compliance responsibilities.)

U.S. government entities, including the Department of Defense, have a longstanding history of applying this shared responsibility model. More detail is provided in **Chapter 2: References**.

Encryption

Encryption is the transformation of information into a form unreadable by anyone without the decryption key, thereby preserving privacy for the intended audience. For example, if one encrypts a folder through an encryption program, only those with access to the key can reverse the process and read the original contents. Before encrypted information can be used again, the information must be decrypted and returned to its original, readable state through the use of a key and the appropriate encryption algorithm. In another example, third-party encryption software can be used to encrypt BCSI documents, which are stored in an off-premises environment that does not provide a native method of encryption. File-level encryption, which protects the file while in transit and at rest, gives the entity full control over who has access to the BCSI and control over the encryption keys.

The strength of a given encryption process is determined by the complexity of the mathematical algorithm behind it. Like many technologies, encryption is constantly changing. To maintain a sufficient degree of information security, utilities should periodically review and keep pace with cyber industry encryption best practices by using sources such as the Federal Information Processing Standards (FIPS) 140-2.

Encryption Key Management

Two basic encryption key management models aid in understanding the security of encrypted information. In the first model, when a registered entity has control of the encryption keys, the registered entity entirely controls the CSP's access to BCSI. In the second model, the registered entity and the CSP may mutually manage the encryption process and/or key management.

In the first model, which this paper refers to as entity-managed encryption keys, the registered entity manages the encryption keys in a hardware security module (HSM), on its own premises, via a third-party separate from the CSP, or in a service within the cloud solution. An HSM is a special network computer/cluster that performs cryptographic operations, such as key management and encryption. An HSM cluster, designed to scale and offer high-speed encryption of information, resides on the registered entity's network (on prem, with a third party, or in the cloud) and is designed to scale and offer high-speed encryption of information. Entity-managed encryption is one way of preventing a CSP from accessing the keys and being able to decrypt or read the information. However, there are a variety of different entity-managed key models, and not every model will offer the entity the same level of control.

From a compliance perspective, entity-managed encryption keys have an advantage in simplicity and security. The registered entity controls the encryption keys and encrypted information, and the CSP cannot decrypt or read the information. Consequently, demonstrating access controls around BCSI protected with entity-managed encryption keys is not as complex as those required for a mutually managed encryption key management approach.

However, entity-managed encryption keys have some disadvantages. The CSP may be unable to support a registered entity if encryption keys are lost. The CSP does not have access to decrypt information for the purposes of supporting storage or applications. Key material being transferred from the responsible entity or third party to the cloud could be at risk of corruption while in transit. Additionally, the registered entity faces significant additional overhead burden in maintaining the keys or contracting with a third party to do so.

In the second model, which this paper refers to as mutually managed encryption keys,[5] the registered entity may choose an implementation design in which the CSP controls some or all of the encryption process. In this model, the CSP and the registered entity share access and mutually manage the encryption keys and processes. As such, the CSP may have access to some or all of the registered entity's information because the CSP has access to the keys.

Mutually managed encryption keys generally offer more flexibility and support operationally. When a CSP manages part or all of the encryption, the registered entity faces less overhead. CSPs can manage security and support applications and infrastructure. Under this model, the CSP can also reset passwords, decrypt files, manage applications, and provide other general support tasks because it manages all or part of the encryption process.

However, in the mutually managed approach, key management may not be entirely controlled by the responsible entity and therefore could enable the CSP to decrypt files (including BCSI) and view them in the original, unencrypted form, inherently increasing the risk of unauthorized disclosure or access. A registered entity should incorporate controls around mutually managed key management and CSP access into its information protection program and/or access management program.

Information Lifecycle

All of the information's states of being need to be addressed to ensure protection and secure handling at all times. Each cloud implementation must be assessed to determine which states are applicable, but the common states to consider are listed below:

- Transit
- Storage/At Rest
- Use
- End of Life/Destruction

[5] Note that key encryption services are complex and vary across CSPs. Customers should understand those complexities to determine if the CSP has access to the encryption keys.

In some cases, information may simultaneously exist in multiple states:

- Email is a good example of information at rest and in transit. For example, BCSI attached to or embodied in an email sent outside of a corporate network (or even within a corporate network that relies upon a cloud-based email service) is simultaneously in transit (from one user to another) and in storage (in email servers and in backups for those servers).
- Another SaaS example would be a document open for editing or review using an online office productivity application. The document is simultaneously in transit from the CSP to the end user's desktop, in storage and backup in the cloud, and in use by the authorized end user during editing.

Encryption is commonly used to secure information from unauthorized users. The methods for using encryption or other controls to secure BCSI in these different states are detailed below.

Information in Transit

As the name implies, information in transit refers to information being moved from one system to another. The encryption of information in transit does not receive much attention in local networks because the information never leaves the private company network. However, encryption of information is a primary concern in a cloud environment because the information will traverse network elements that are not controlled by the registered entity as the information travels between the end user and CSP.

Email services and online office productivity applications are good examples of information traversing networks not owned by the registered entity. Email and files destined for the cloud move over the public internet as they move from the registered entity to the CSP. Unencrypted information moving over the public internet is at higher risk of unauthorized exposure or access. On its journey to a CSP, the information must pass through intermediate service provider networks, none of which will be party to the registered entity's agreement with the CSP. These intermediate service providers have little or no obligation to a registered entity or the CSP to protect the transit of the information.

BCSI traveling across the public internet must be encrypted in transit to prevent unauthorized individuals from accessing it. Most CSPs, email services, and online office applications use encryption to protect information in transit. Transport Layer Security (TLS) is most commonly used to secure communication between customers and services like email, online shopping and banking, and other communications over the internet. Any time the "*https://*" prefix precedes a web address, TLS encryption is being used. Even though TLS encryption is commonly used to secure information in transit, not all versions of TLS are equally secure. The TLS version should be reviewed to ensure that a version with known vulnerabilities is not being utilized.

Information at Rest (Storage)

Information at rest is not being actively processed or used and exists in storage. Encryption protects information (including BCSI) at rest whether in the cloud or another environment. Information is at rest in SaaS, IaaS, and on-premises environments and when on portable devices (e.g., laptops, thumb drives). It is extremely difficult or impossible to access encrypted information at rest without the encryption keys, such as in cases of encrypted information being stolen or inadvertently released.

Information in Use

Information in use refers to information that is being used or modified by an end user. BCSI in the cloud environment may not have a "use" state. Where a "use" state may exist in a cloud environment, encryption of BCSI while being used may not be practical or even an option. Instead, access controls (such as username and password, role-based access, or two-factor authentication) may be used as a security measure to prevent any BCSI in a "use" state from being accessed by unauthorized personnel.

End of Life/Destruction

Entities are responsible for ensuring that their BCSI is removed or destroyed/deleted from a cloud environment. Simply encrypting the BCSI and destroying the keys is not best practice. Prior to removal or destruction, entities should consider any retention requirements (such as those found in the evidence retention section of each NERC standard or their internal record retention policy and schedule) to prevent prematurely erasing BCSI. Finally, entities should ensure that retention settings in their cloud environment are set to retain information as expected or develop other methods to retain that information as required.

Cloud Geography

To ensure reliability and resilience, data in the cloud may be distributed and stored over a wide geographical area. It is not uncommon for cloud data to traverse regional locations or international borders, although agreements limiting storage to certain geographical regions or nations are commonplace. Geographical location in the cloud can be complicated because data may be redistributed or moved to a new location as a cost-saving or reliability measure. In effect, the controlling location of cloud data can change if allowed by the agreements between the CSP and registered entity.

The flow of data through a foreign country in this geographically distributed storage model can prove disadvantageous, however, during a breach because while the data is in a foreign country the registered entity may not have the same legal recourse to enforce the terms of the agreement as it would have in the United States.

Using a distributed model for data storage (in which the customer's data is split up across multiple locations) can be an effective security control, especially if encryption is also applied. This would prevent a physical attacker from obtaining access to all of the data, and, if the data is also encrypted, prevent them from reading and using the data. A common example of this methodology is Blockchain. As a physical security feature, cloud storage does not require physical labeling of registered entity data on a specific server location in a data center, which prevents data center personnel from recognizing data owners.

The shared nature of cloud storage means that the CSP may be responsible for managing some or all of the system. Consequently, the CSP may have access to BCSI stored within the system and in transit during communication with the registered entity. If the information is not encrypted during transit and while at rest, security management of a cloud service can require more complex access controls, contract language, and non-disclosure agreements.

Certifications and Attestations

CSPs may obtain a variety of certifications and attestations to demonstrate to their customers that they have internal controls and systems in place for data/information security, confidentiality, and more. Some of these certifications and attestations require controls similar to those required by the NERC CIP standards, such as conducting a background check prior to provisioning access and revocation of access within 24 hours of a termination. These certifications and attestations require regular audits and continuous monitoring, including testing of the security controls, by an authorized third party to maintain and keep the certification/attestation active. Therefore, the audit results of such third-party testing can be used by the registered entity to confirm that the protections being applied to their BCSI are being maintained. The most common certifications relevant to NERC CIP are as follows:

- **Service Organization Control (SOC) 2 Type 2:** This is a set of standards designed by the American Institute of Certified Public Accountants focused on five areas: security, availability, processing integrity, confidentiality, and privacy. Assessors issue attestations after an independent assessment of the CSP's systems and internal controls are deemed sufficient and effective after several months of testing (typically six months) and the attestations are valid for 12 months. A full-scope audit is required annually by an accredited firm, which in turn produces a report on the company's security posture.

- **ISO/IEC 27001:** This is the international standard, similar to SOC 2 Type 2, established by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). However, unlike the SOC 2 Type 2, certifications (not attestations) are issued once an organization has demonstrated that its risk management framework (including internal controls) is sufficient and effective for maintaining information security. Maintaining this certification requires annual audits by an approved auditor of an accredited certifying body and a full recertification every three years.
- **Federal Risk and Authorization Management Program (FedRAMP) Moderate or High:** This is a set of standards based on NIST- and Federal Information Security Management Act-defined standards that apply to the U.S. federal government's use of cloud products and services, with an emphasis on security and protection of federal information. A CSP is issued a FedRAMP Authorization at a low, moderate, or high impact level for each cloud service offering, based off the security categorization of the data/information that will be processed, stored, and/or transmitted within the system. FedRAMP moderate and high are the levels most similar to the NERC CIP medium- and high-impact requirements. While this program was designed for U.S. federal government agencies, many CSPs have made their FedRAMP-authorized environments available to non-government entities. Maintaining a FedRAMP authorization requires annual audits by an accredited third-party assessment organization.

Cloud Security Assessment Aid

Entities should conduct a risk assessment prior to implementing/utilizing a cloud service and again after implementation to confirm that the intended security controls were not adversely impacted. The Cloud Security Alliance (CSA) has developed the Cloud Controls Matrix (CCM), a set of security controls and guidelines to help customers assess the security of cloud computing providers. The CSA's CCM currently includes a set of 197 security controls mapped to various security frameworks, such as ISO/IEC 27001, NIST SP 800-53, NIST CSF 2.0, and the European Union's General Data Protection Regulation (GDPR).

The CCM framework covers 17 security domains, including the following:

- Audit and Assurance
- Application and Interface Security
- Change Control and Configuration Management
- Identity and Access Management
- Datacenter Security
- Data Security and Privacy
- Human Resources Security
- Security Incident Management, E-Discovery, and Cloud Forensics
- Business Continuity Management and Operations Resilience
- Cryptography, Encryption, and Key Management
- Infrastructure and Virtualization Security
- Logging and Monitoring
- Supply Chain Management, Transparency, and Accountability
- Interoperability and Portability
- Threat and Vulnerability Management

- Universal Endpoint Management
- Governance, Risk Management, and Compliance

By using the CCM, organizations can assess the security postures of cloud providers, develop security policies and procedures, and identify areas where additional security controls may be needed.

For specific cloud service and key management examples, see the ERO Enterprise-endorsed *Implementation Guidance: Usage of Cloud Solutions for BCSI*.[6]

[6] https://www.nerc.com/pa/comp/guidance/EROEndorsedImplementationGuidance/CIP-004-7%20R6%20and%20CIP-011-3%20R1%20-%20Cloud%20Solutions%20for%20BCSI%20(RSTC).pdf

Chapter 2: References

Cloud Computing

Cloud services are powered by cloud computing, which is further explained in NIST Special Publication (S.P.) 800-145, *Definition of Cloud Computing*.[7]

Mitigating Cloud Vulnerabilities

Managing risk in the cloud requires customers to fully consider exposure to threats and vulnerabilities, not only during procurement but also as an ongoing process. The U.S. National Security Agency published the *Mitigating Cloud Vulnerabilities*[8] document on January 22, 2020, to assist customers in both awareness and assessment of these key known areas of vulnerability:

- Misconfiguration
- Poor Access Control
- Shared Tenancy
- Supply Chain

Shared Responsibility Model as Part of DoD Risk Management Framework

The U.S. Department of Defense (DoD) Risk Management Framework (RMF) outlines a *shared responsibility* model[9] for managing risk and securing systems in the DoD.

This model identifies a shared responsibility between the DoD and the system owners for managing and securing DoD information systems as detailed below:

- The DoD is responsible for the infrastructure and environment security of the systems' environment. This responsibility includes ensuring the security of the systems' information processed, stored, and transmitted. The DoD is also responsible for providing security services such as vulnerability management, incident response, and threat intelligence.
- System owners are responsible for implementing and maintaining security controls to protect their information systems. Control implementation includes identifying and categorizing the information processed, stored, and transmitted by the system, selecting and implementing security controls, assessing control effectiveness, and monitoring and reporting security events and incidents.

The shared responsibility model recognizes that the security of information systems is a mutual responsibility between the DoD and the system owners. Both parties must work together to manage risk and secure the systems.

In summary, the "shared responsibility" model, as defined by the DoD RMF, recognizes the mutual responsibility between the DoD and the system owners for managing and securing DoD information systems. The DoD is responsible for the security of the infrastructure and environment, while system owners are responsible for implementing and maintaining security controls to protect the information systems that they operate.

[7] https://csrc.nist.gov/pubs/sp/800/145/final
[8] https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF
[9] Version issued July 19, 2022: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf?ver=2019-02-26-101520-300

DoD Cloud Computing Security Requirements Guide

Registered entities could leverage the DoD Cloud Computing Security Requirements Guide (SRG)[10] as an input into their security controls within a cloud environment.

The DoD Cloud Computing SRG defines cloud information security objectives and impact levels based on a combination of the following:

- Sensitivity or confidentiality level of information (e.g., public, private, classified) to be stored and processed in the CSP environment
- Potential impact of an event resulting in the loss of confidentiality, integrity, or availability of that information

DoD impact levels (I.L.s) are used to determine what level of security is required to operate in a cloud environment and are based on moderate confidentiality and moderate integrity (while ignoring availability). The DoD Cloud Computing SRG uses the FedRAMP moderate baseline at all information I.L.s, considering the high baseline for some. However, the DoD security control baseline does not support a high baseline for systems and information categorized as high confidentiality or integrity.

DoD Risk Management Processes

Traditionally, DoD risk management processes addressed physical on-premises systems and applications, necessitating adjustments to accommodate the cloud and commercial cloud service offerings (CSO) while ensuring the security of the DoD's core missions and networks. The risks and legal considerations in using virtualization technologies further restrict the types of tenants obtaining cloud services from a virtualized environment on the same physical infrastructure, along with restricting the cloud deployment models for processing and storing various kinds of DoD information.

FedRAMP and the DoD require ongoing assessments and authorization for CSOs providing services to the DoD. These assessments leverage the DoD RMF and the FedRAMP continuous monitoring strategy. Mission owners inherit compliance from the CSO for the security controls (or portions thereof) that the CSP maintains. A mission owner's system or application built on an IaaS or PaaS offering must meet many of the same security controls within the system/application. Mission owners contracting for SaaS offerings inherit the bulk of security control compliance from the CSO—however, inheritance differs between CSPs operating within a given service model, requiring separate evaluations. Additionally, the number of controls increases with higher I.L.s.

[10] https://public.cyber.mil/stigs/downloads

Contributors

NERC gratefully acknowledges the contributions and assistance of the following industry experts in the preparation of this guideline (ordered alphabetically by last name).

Name	Entity
Dr. Tom Duffey	Knight Consulting Services
Alice Ireland (lead)	Proven Compliance Solutions, a Radian Generation Company
James Tosh Keele	Entergy
Guillermo Macias	Origis Energy
Sergio Martinez	Origis Energy
Kristine Martz	Edison Electric Institute
James McNierney	NYISO
Jared Williams	Entergy

Guideline Information and Revision History

Guideline Information	
Category/Topic: Cyber	**Reliability Guideline/Security Guideline/Hybrid:** Security Guideline
Identification Number: SG-CYB-MMYY-2	**Subgroup:** Security Working Group

Revision History		
Version	**Comments**	**Approval Date**
1	Initial Version	6/10/2020
2	Refresh. Substantial changes include addition of a table of contents, new sections for shared responsibility model, destruction of BCSI, certifications/attestations, security assessment aid, and Appendix C with references. Other substantial edits were made within the existing sections.	TBD

Metrics

Pursuant to the Federal Energy Regulatory Commission's (FERC) order on January 19, 2021, North American Electric Reliability Corporation, 174 FERC ¶ 61,030 (2021), reliability guidelines shall now include metrics to support evaluation during triennial review consistent with the RSTC Charter.

Baseline Metrics

All NERC reliability guidelines include the following baseline metrics:

- BPS performance prior to and after a reliability guideline as reflected in NERC's *State of Reliability* report and long-term reliability assessments (e.g., *Long-Term Reliability Assessment* and seasonal assessments)
- Use and effectiveness of reliability guidelines as reported by industry via survey
- Industry assessment of the extent to which a reliability guideline is addressing risk as reported via survey

Specific Metrics

The RSTC or any of its subcommittees can modify and propose metrics specific to the guideline to measure and evaluate its effectiveness, listed as follows:

- The Security Working Group (SWG) will use survey responses to evaluate the extent to which industry is using the recommendations from this security guide to implement best practices.
- The SWG may poll its membership to evaluate the extent to which industry is using the recommendations from this security guide to implement security best practices.

Effectiveness Survey

On January 19, 2021, FERC accepted the NERC proposed approach for evaluating reliability guidelines. This evaluation process takes place under the leadership of the RSTC and includes the following:

- Industry survey on the effectiveness of reliability guidelines;
- Triennial review with a recommendation to NERC on the effectiveness of a reliability guideline and/or whether risks warrant additional measures; and
- NERC's determination whether additional action might be appropriate to address potential risks to reliability in light of the RSTC's recommendation and all other data within NERC's possession pertaining to the relevant issue.

NERC asks entities that use reliability and security guidelines to respond to the short survey provided in the link below.

Guideline Effectiveness Survey