MIDWEST RELIABILITY ORGANIZATION

MRO SAC and CMEPAC Hosted Webinar on

BES Cyber System Information (BCSI) in the Cloud

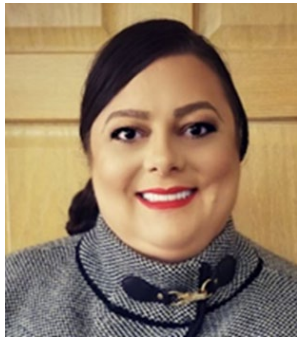
Sharon Koller, Reliability Standards Compliance Strategist & Assurance Manager, American Transmission Company and MRO CMEPAC Member

Clayton Whitacre, Senior Systems Analyst, Great River Energy and MRO SAC Member

Alice Ireland, Sr. Manager, Reliability Compliance, Tri-State Generation and Transmission Assoc., Inc.

Trevor Stiles, Manager, Reliability Standards Compliance and Associate General Counsel, American Transmission Company

August 18, 2021



Sharon Koller, Reliability Standards Compliance Strategist & Assurance Manager, American Transmission Company and MRO CMEPAC Member

Email: skoller@atcllc.com

Clayton Whitacre, Senior Systems Analyst, Great River Energy and MRO SAC Member

Email: CWhitacre@GREnergy.com

Alice Ireland, Sr. Manager, Reliability Compliance, Tri-State Generation and Transmission Assoc., Inc.

Email: aireland@tristategt.org

Trevor Stiles, Manager, Reliability Standards Compliance and Associate General Counsel, American Transmission Company

Email: tstiles@atcllc.com

Disclaimer

Midwest Reliability Organization (MRO) is committed to providing outreach, training, and non-binding guidance to industry stakeholders on important industry topics. Subject Matter Experts (SMEs) from MRO's organizational groups and the industry may develop materials, including presentations, provided as a part of the event. The views expressed in the event materials are those of the SMEs and do not necessarily express the opinions and views of MRO.

MRO CMEPAC and SAC/SACTF Tentative 2021 Meetings and Events

- **CMEPAC:**
  - Quarter 3 Joint Meeting with the OGOC on **September 29, 2021**
  - Quarter 4 Meeting on **November 10, 2021**
  - Ask CMEPAC Call at 3:00 p.m. the 2nd Tuesday each month
- **SAC**
  - Security Technical Training on **October 4-5, 2021**
  - Security Conference on **October 6, 2021**
  - Regional Security Risk Assessment on **October 7, 2021**
  - Quarter 4 Meeting on **November 3, 2021** (Registration is Open)
- **SACTF:**
  - Threat Call at 8:15 a.m. on Wednesday Mornings

BCSI in the Cloud

- **Agenda:**
  - Overview of Initiatives Related to BCSI in “the Cloud”
  - CIP Compliance Requirements
  - Securing BCSI in the Cloud
  - Additional Resources
  - Q&A

BES Cyber System Information (BCSI) in the Cloud

Initiatives Overview

Alice Ireland, Sr. Manager, Reliability Compliance, Tri-State Generation and Transmission Assoc., Inc.

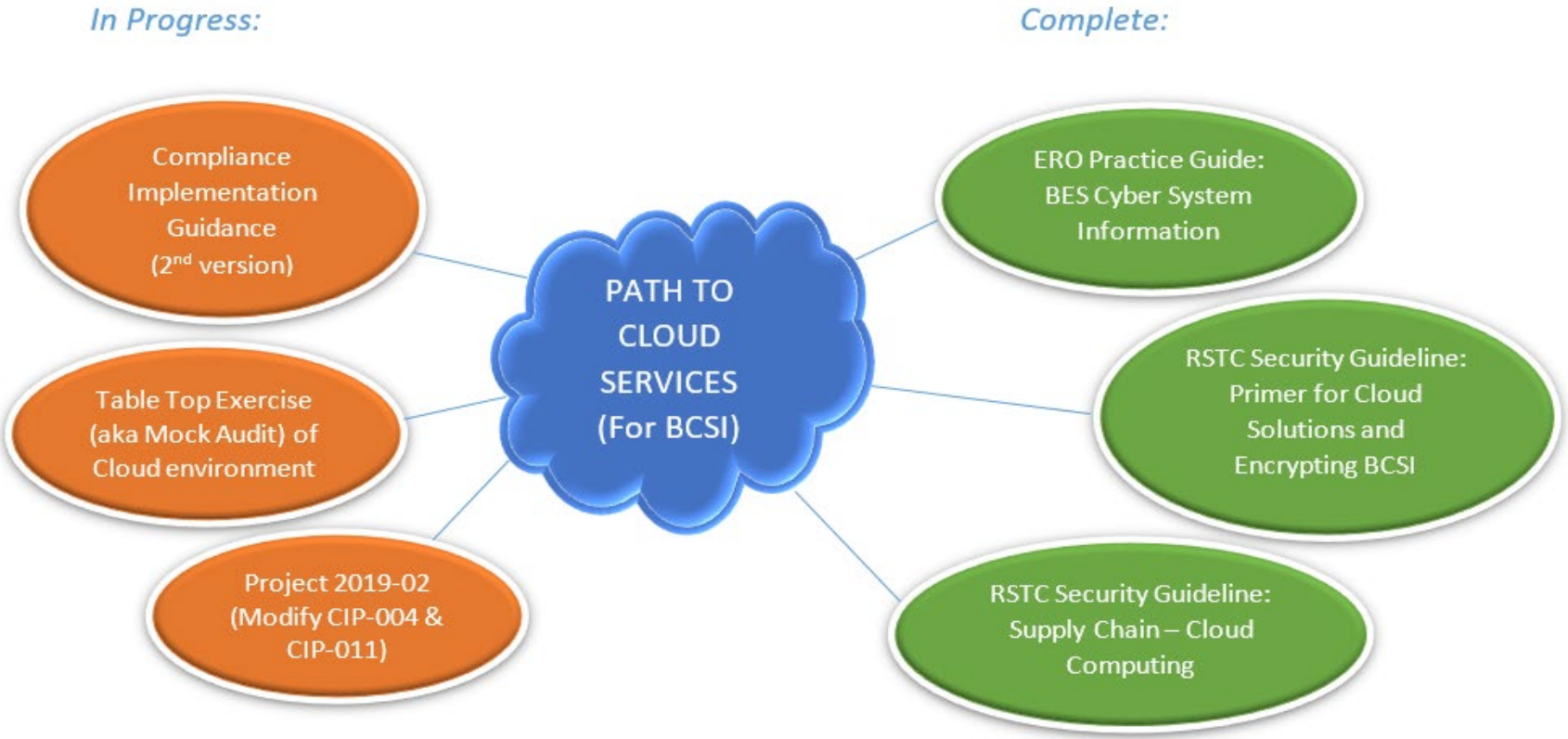
What do we mean by “the Cloud”?

- Data, applications, etc. that is hosted for two or more companies on a 3rd party’s system.

- This is NOT an entity’s own virtualized system.

The Path Towards BCSI in the Cloud

Individual Initiatives



BES Cyber System Information (BCSI) in the Cloud

CIP Compliance

Sharon Koller, Reliability Standards Compliance Strategist & Assurance Manager, American Transmission Company and MRO CMEPAC Member

Current State

CIP Compliance vs. BCSI in the cloud

- **Emerging technologies and enhanced security features are generating interest in cloud solutions**
- **Current enforceable CIP Standards have encumbered the implementation of cloud solutions for BCSI.**
- **NERC CMEP Practice Guide is bridging that gap.**
- **BES Cyber System Information Access Management SAR**
  - Approved in August 2019

Standards Authorization Request (SAR):

CIP Compliance vs. BCSI in the cloud

- **Purpose/Goal:**
  - Enhance BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage BCSI
  - Provide a secure path toward the use of modern third-party data storage and analysis solutions (aka cloud services)
  - Enable the CIP Standards to allows for alternative methods, such as encryption, to be utilized in the protection of BCSI
  - Clarify CIP-004 and CIP-011 requirements related to both managing access and protecting BCSI
  - Allow for methods other than storage location to be used, such as encryption, while still permitting Registered Entities to define how BCSI is protected.

Status and Next Steps:

CIP Compliance vs. BCSI in the cloud

- **2019-02 Project:**
  - **June 11, 2021:** Industry approved CIP-004-X and CIP-011-X to enable the CIP Standards for BCSI in the cloud.
  - **August 12, 2021:** NERC BOT Adopted; NERC preparing FERC petition.
  - FERC Approval and FERC Filing in the Federal Register will set the Effective Date
  - Implementation Plan carries two options:
    - Twenty-four months after effective date of the applicable governmental authority's order approving the standard
    - Early Adoption of revised CIP Standards following their approval by the applicable governmental authority, but prior to their Effective Date.

Future Enforceable Standards:

CIP Compliance vs. BCSI in the cloud

- **CIP-004-X**
  - Access Management
  - Enables Entity to choose how to manage access in their organization
    - Grouping (backwards compatible with storage locations)
    - Individually (File-level Rights and Permissions etc.)
- **CIP-011-X**
  - BCSI Protection
  - Enables entities to apply controls commensurate with risk profile of environment
    - On-prem (backwards compatible with storage locations)
    - Off-prem (risk mitigating technical controls certifications i.e., FedRamp, SOC1, SOC2)

Future Enforceable Standards:

CIP Compliance vs. BCSI in the cloud

- **CIP-004-X**
  - **R6**. BCSI Access Management
  - Two-prong method to qualify as ‘access’ (obtain and use)
  - Controls aligned with BCSI form factor (electronic v. physical)
- **CIP-011-X**
  - **R1.1** Focus on BCSI vs Cyber Asset
  - **R1.2** Controls to mitigate risks of compromising confidentiality

Additional Considerations:

CIP Compliance vs. BCSI in the cloud

- **Identify the need:**
  - Application functionality
  - Mobility options
  - Reduce impact to business and IT from regular large updates
  - Support needs
  - Cost Considerations
- **Assess the risk**
  - All clouds are not created equal
  - Our data
  - Compliance implications
  - Business Buy-in
  - Misconfiguration vs Vendor error

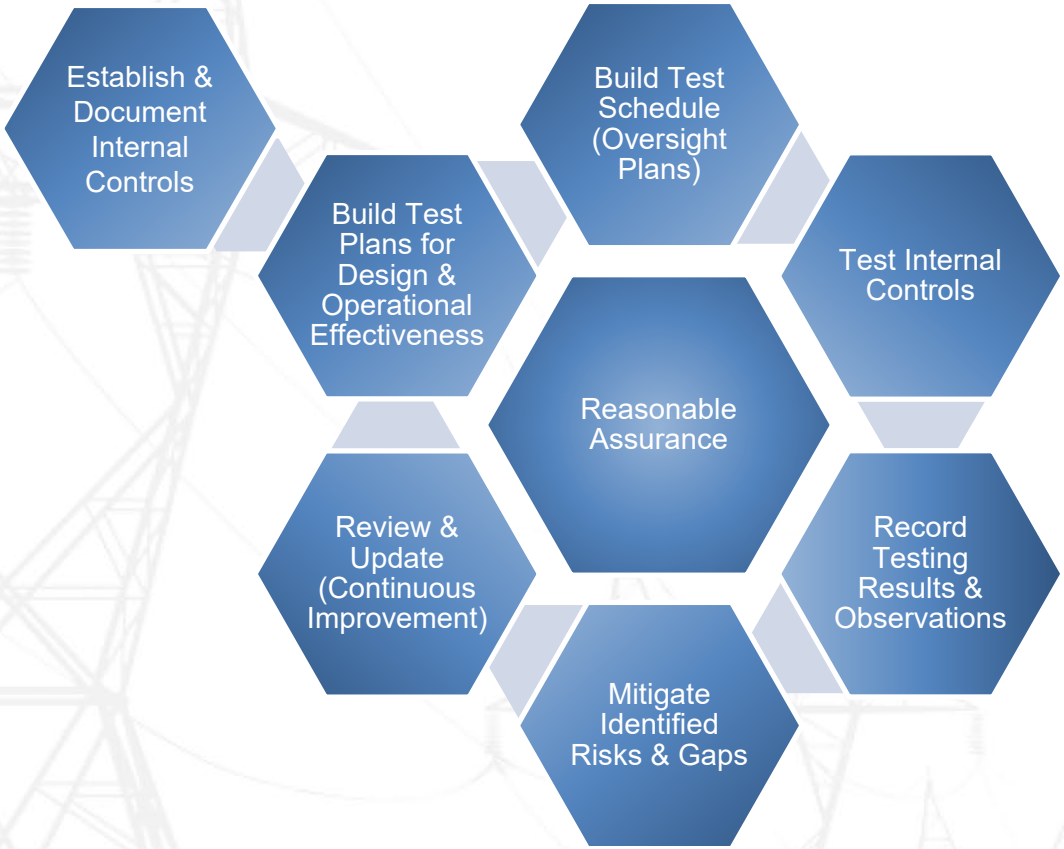
Additional Considerations:

CIP Compliance vs. BCSI in the cloud

- **Implement Controls:**
  - Logging/monitoring
  - Manage Users
    - Multi-factor Authentication
    - Privileged Identity Management
  - Manage Data
    - Encryption – who controls the keys
    - Sharing
    - Data Loss Prevention (DLP)
    - Document Classification and Custodian
    - DR/BR/IR
  - Updated standards, procedures and guides

Additional Considerations:

- **Provide Reasonable Assurance**
- **Repeat**

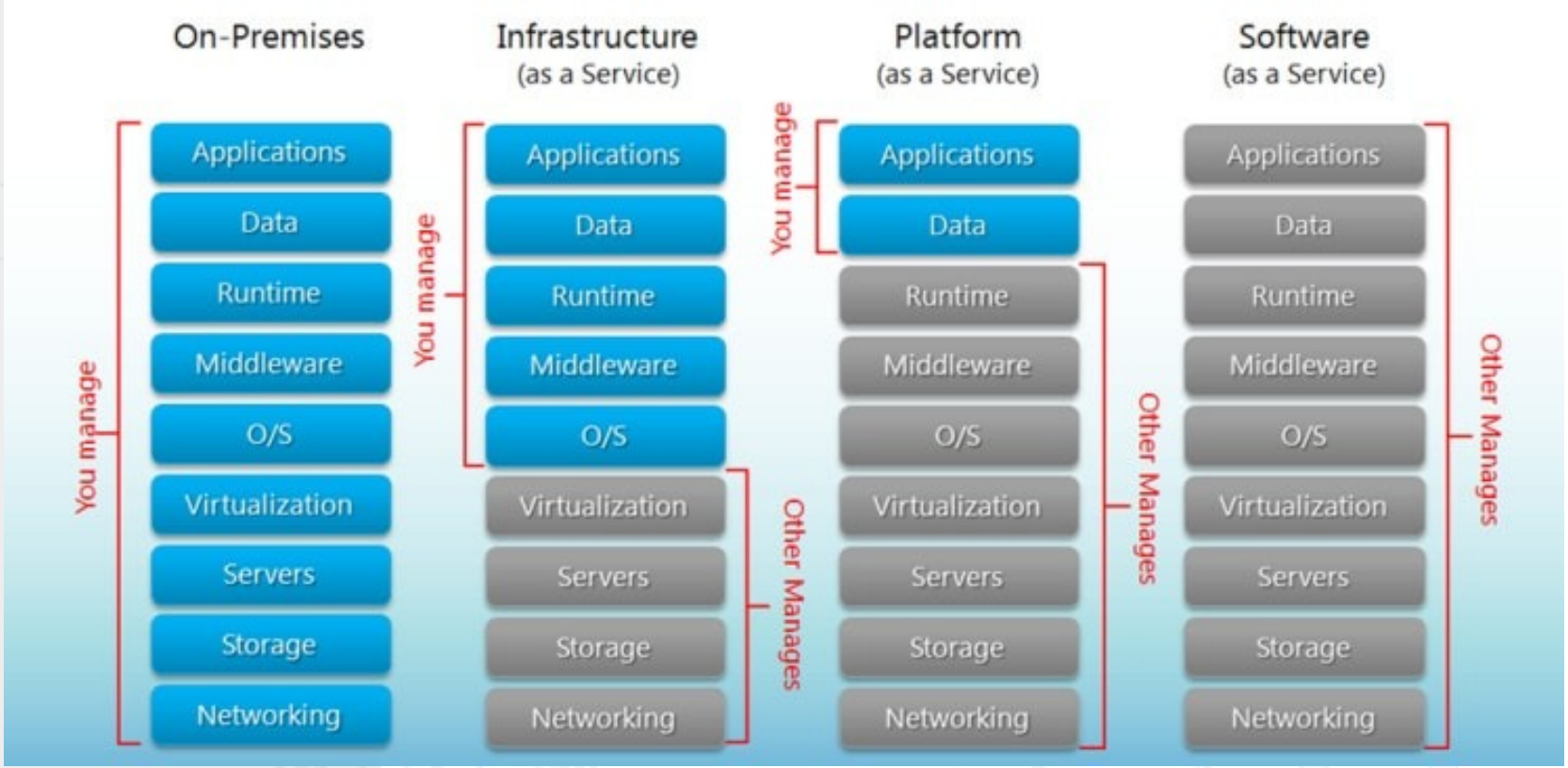


BES Cyber System Information (BCSI) in the Cloud

Cyber Security

Clayton Whitacre, Senior Systems Analyst, Great River Energy and MRO SAC Member

Cloud Types



https://www.bigcommerce.com/blog/saas-vs-paas-vs-iaas/#the-three-types-of-cloud-computing-service-models-explained

Cloud Terms

- Cloud Service Provider (CSP)
- Service Level Agreement (SLA)

Which Cloud is right for you?

- **Comparing Options**
- **Risk Analysis**
- **Administrative Training**
  - Consider low-risk migrations first

Training & Communication for Cloud Applications

- **Administrative Training**
  - •Proper Cloud administration
- **End-user training**
  - •Blurring between what is on-prem and Cloud based.
- **Tuning message**
  - •Proper Cloud usage focused

Data Loss Prevention

- **Data Tagging**
  - Pattern matching
  - Watermarking
- **DLP Types**
  - Host based
  - Network based
  - Cloud based

Encryption

- **In Transit**
  - Protects data as it traverses the network
- **At Rest**
  - Protects data as it rests on the disk
- **Key Management**

Encryption – In Transit

- **IaaS**
  - •Web - HTTPS
    - — Customer-implemented
  - •File Transfer - SFTP/FTPS
    - — Customer-implemented
  - •SSH
    - — Customer-implemented
- **SaaS**
  - •Web - HTTPS
    - —Default/Negotiated
  - •File Transfer - SFTP/FTPS
    - —Default/Negotiated
  - •SSH
    - —Default/Negotiated

Encryption – At Rest

- **IaaS**
  - Customer controlled
    - Initial setup configuration option
    - CSP may have access to default encryption keys
    - Manage/supply your own key possible
  - Additional layers possible
- **SaaS**
  - Cloud Service Provider Controlled
    - May or may not be available
    - CSP may have access to decryption keys
  - Dual Key Encryption
    - CSP held + Customer held key for secure documents

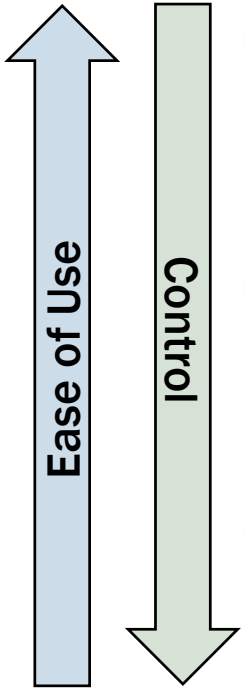
Key Management

"Cryptographic keys play an important part in the operation of cryptography. These keys are analogous to the combination of a safe. If a safe combination is known to an adversary, the strongest safe provides no security against penetration. The proper management of cryptographic keys is essential to the effective use of cryptography for security."

- NIST SP 800-57 Part 1 Rev. 5 – Recommendations for Key Management

- **Encryption Key Terms**
  - Hardware Security Module (HSM) – Generation, storage, usage of keys
  - FIPS 140-2 / 140-3 – NIST certification of encryption modules

Key Management



- **Cloud Service Provider Managed Keys**
  - Default option in most IaaS and some SaaS models
- **Customer Managed Keys**
  - Keys stored and maintained in CSP key-management solution
- **Customer Supplied Keys**
  - Most control over key access/usage

Data Disposition/End of Cloud Service

- **Data Disposition**
  - Assurance from CSP
- **End of Cloud Service**
  - Secure export/migration of data

BES Cyber System Information (BCSI) in the Cloud

Additional Resources

Alice Ireland, Sr. Manager, Reliability Compliance, Tri-State Generation and Transmission Assoc., Inc.

Proposed Compliance Implementation Guidance: BCSI - Encryption in the Cloud

- **Summary of the Compliance Implementation Guidance:**
  - Purpose is to provide examples for how encryption can be utilized to secure and restrict access to BES Cyber System Information in various commonly used cloud services, along with evidence examples. (Microsoft 365, ServiceNow, Amazon Web Services, CommVault, IBM)

Proposed Compliance Implementation Guidance: BCSI - Encryption in the Cloud

- **Development History:**
  - **June 2020** - First version was presented to the NERC CIPC/RSTC, and approved.
  - **June 2020** - First version was submitted to the ERO for endorsement.
  - **Oct. 2020** - ERO Enterprise did not endorse the document, but provided detailed feedback to SWG sub-team
  - **April 2021** - SWG sub-team modified the document to address ERO Enterprise feedback
  - **June 2021** – RSTC approved and filed with NERC for endorsement
  - **August 2021** – ERO Enterprise reviewed, non-endorsed

Proposed Compliance Implementation Guidance: BCSI - Encryption in the Cloud

- **Next Steps**
  - Not endorsed due to non-significant items
  - NERC RSTC Executive Committee is taking up the Compliance Guidance process issues with NERC leadership

Table Top Exercise: BCSI in the Cloud

- Learning exercise for the entity and the ERO Enterprise
- Evaluated compliance with CIP-004 & CIP-011
- Evaluated various risk areas
- Under review by NERC Security Working Group
- Will be posted for industry use

Additional Resources and Links

- 2019-02 Project Page
- CMEP Practice Guide BES Cyber System Information
- NIST Definition of Cloud Computing
- NIST Recommendations for Key Management
- Security Guideline: Primer for Cloud Solutions and Encrypting BCSI
- Security Guideline: Risks Related to Cloud Service Providers

Your feedback is very important to us. Please provide your feedback using the link or QR Code below or the link below:

https://www.surveymonkey.com/r/87RXRQG

Thank You!