A PUBLICATION OF GDS ASSOCIATES, INC.

CIP 100-Series

Newsletter

JULY 2026

1850 PARKWAY PLACE SUITE 800 MARIETTA GEORGIA 30067 | 770.425.8100 | @gdsassociates.com

TABLE OF CONTENTS

BACKGROUND

As noted in the 2020 FERC Notice of Inquiry, the vast majority of new products from vendors are cloud-based solutions placing increased pressure on NERC registered entities to securely operate the BES. Concurrently, from an operational and reliability perspective, the modern power grid landscape is changing, driven by rapid grid modernization, digital transformation, decentralization of electric resources, and decarbonization targets. These factors are increasing the data volumes required to continue operating a reliable and resilient grid and thus increasing the need for data analytics and resources such as computing, network, and storage.

Increasing data storage requirements and processing requirements of grid modernization are driving the need for cloud services. Cloud services offer fault-tolerant system design capabilities in which operations and data can be replicated and run in independent application stacks in geographically dispersed locations along with other benefits, including reliability, resilience, and security.

As explained in NERC's 2019 whitepaper on Virtualization and Future Technologies, the reliance on physical assets in the current standards prevents the use of cloud services in a compliant manner for some systems such as those defined as BES Cyber Systems or EACMS. The Project 2016-02 SDT (Standard Drafting Team) developed this white paper to explain the need to change the cyber security CIP Reliability Standards. This white paper has not been approved or endorsed by NERC and is solely the views of the Project 2016-02 SDT.

To address these issues, Project 2023-09 Risk Management for Third-Party Cloud Services, proposes to establish risk-based, outcome-driven requirements that place cloud services on par with other third-party resources already used for CIP-regulated systems including for BES operations and supporting cyber assets. The goal is to create a new set of standard(s), CIP 100-Series, to add clarity in allowing for the adoption and auditability of cloud services used for the BES.

CIP 100-SERIES TECHNICAL RATIONALE SUMMARY

Previously the proposed solution to address these issues with virtualization was a full embrace of the cyber system concept (retiring device level terms like Cyber Asset and BES Cyber Asset) and writing the technical requirements (e.g. CIP-005, CIP-007, CIP-010) at a more objective level. However, through industry feedback several important issues came to light, such as eliminating the BES Cyber Asset definition and moving to the BES Cyber System as the sole foundational object with no further granularity would cause a complete overhaul and "do-over" of entities' CIP-002 processes with insufficient benefit for the effort required.

The future concept is to leave the foundational definitions largely unmodified. And BES Cyber Systems would remain as-is and allow for all the various ways entities have used that concept to date.

The direction remains to establish objective level requirements but these need to be written at the appropriate level. For example,

- If CIP-005 R1 were written as "*Mitigate the risk of unauthorized network access*", it is certainly an objective but is too high level to be measurable. No one would be able to state when, or to what degree this objective had been accomplished.
- If CIP-005 R1 were written as "*Only allow known good layer 3 IP addresses into or out of the network and implement this only at a Cyber Asset interface located only at the network edge*", that would be a prescribed topology and a prescriptive "how" that should be avoided as it precludes much of the newer technologies available in the industry. The latter is essentially the CIP-005 R1 of today and is one of the primary requirements that needs to change to remove this prescriptive topology and "how's".
- An example of an alternative objective requirement that clearly describes a measurable "what" but avoids prescriptive "how's" for CIP-005 R1 could conceptually be:
    - *Deny all access to and from the networks on which high and medium impact BES Cyber Systems and their associated PCAs are connected and only allow network communication that has documented access permissions including the reason for granting access.*
    - This is a much clearer objective to accomplish but avoids telling the entity how or where they must implement it or how their network must be architected.
    - *As for backward compatibility, an entity could still define an ESP with designated EAPs and provide firewall configurations as they do today. However, an entity using the advanced virtualization techniques, or future techniques to control network access that have not yet been contemplated can still show they meet this same objective.*

Hence, the CIP standards require some changes to:

- ❖ Address risks unique to virtualized environments such as the sharing of hardware resources and management plane access.
- ❖ Provide clarity around how to identify and categorize the various types of cyber assets in a virtualized infrastructure and scope requirements appropriately.
- ❖ Allow entities to fully implement newer security techniques in these environments that can provide higher levels of access control that are easier to manage, and don't require purchasing extra hardware to show compliance with prescribed topologies.

EXAMPLE USE CASES

The first use case below exemplifies a theoretical, new CIP-102 standard for the identification and categorization of BES Cyber Systems and Services; the second use case examines new CIP-105, the network security standards, at a high level.

CIP-102 – BCSS Identification and Categorization

CIP-102 addresses BES Cyber Systems or Services (BCSS). This proposed new term (BCSS) is intended to accommodate both traditional on-site Cyber Systems, as well as cloud-based services. This approach would provide consistency in the categorization of assets to be used for Cyber Systems or Services. It would also provide consistency in the categorization of BCSS and BCS by tying the BCSS impact category to the associated BES Assets. For example, Requirement R1 might be drafted as follows:

R1. Each Responsible Entity shall implement a process that identifies Cyber Systems as BES Cyber System or Service (BCSS) that, if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact one or more Facilities, systems, equipment or service, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the Reliable Operation of the Bulk Electric System. Redundancy of affected Facilities, systems, equipment, and services shall not be considered when determining adverse impact. [Violation Risk Factor: High] [Time Horizon: Operations Planning]

1.1.1. List each of the high impact BCSS according to Attachment 1, Section 1, if any;

1.1.2. List each of the medium impact BCSS according to Attachment 1, Section 2, if any; and

1.1.3. List each of the low impact BCSS according to Attachment 1, Section 3, if any.

CIP-105 Network Security

The proposed concept for these technical standards, such as CIP-105 Requirement R1, would take the form of:

R1. Each Responsible Entity shall implement one or more documented security plan(s) that accomplish the following objectives for its high impact and medium impact BCS.

R1.1. Permit network access to applicable systems based on need, documenting the reason, and denial of all other network access, excluding time sensitive communications of Protection Systems.

R1.2. Communication for applicable systems shall be monitored for detecting known or suspected malicious communications for both inbound and outbound communications.

R1.3. Protect access to configurations that impact access enforcement and monitoring to applicable systems.

R1.4. Authenticate connection attempts prior to permitting active session communication to applicable systems.

CONCLUSION

As cloud services come into focus for BES tasks, the CIP standards need a new foundation – one that can carry industry well into the future. Even with current entity-owned and maintained on-premise systems, technology is becoming more dynamic and services-based, rather than a statically configured, dedicated Cyber Asset.

Hence the drafting team has proposed the creation of an alternate suite of CIP standards that are written at an objective level such that they can incorporate third-party cloud services, on-premise systems, and other new innovations in technology at a more agile pace in a rapidly evolving cyber environment. This plan would leave the existing CIP standards as written and offer an ongoing option for companies that do not wish to utilize cloud services; however, it would provide an option for such companies to enable cloud services in CIP environments. The drafting team's project plan is to develop new standards that closely parallel to the existing standards as shown in Figure 1.

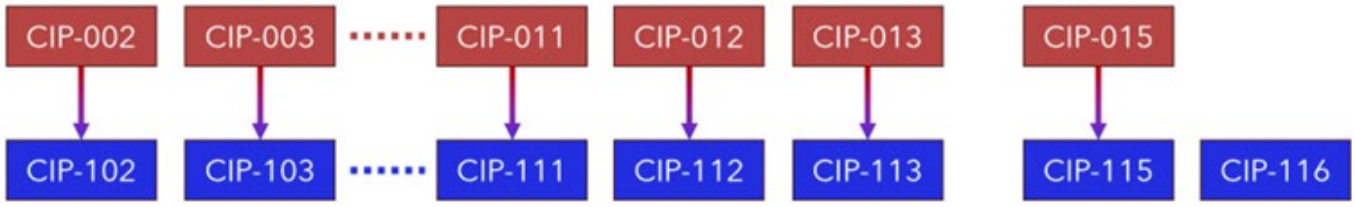

Figure 1

The new 100-series standards will be developed to stand alone and will not rely on the existing standards. The intent is for both series to result in the same security outcomes.

Note: An informal comment period for **Project 2023-09 Risk Management for Third-Party Cloud Services** is open through **8 p.m. Eastern, Friday, August 21, 2026** for the following Standards and Implementation Plan:

- CIP-102-1 — Cyber Security - BES Cyber Services and Systems Identification
- CIP-103-1 - Cyber Security — Security Management Controls
- CIP-105-1 — Cyber Security – System Protection
- CIP-113-1 — Cyber Security – Supply Chain Risk Management

REFERENCE MATERIAL

- 2023-09 Risk Management for Third-Party Cloud Services
- project-2023-09-risk-management-for-third-party-cloud-services-white-paper_121825.pdf
- project-2023-09_cip_100-series_definitions_technical_rationale_070726.pdf
- project-2016-02_virtualization_and_future_technologies_case_for_change_white_paper_04182019.pdf

CIP 100-Series

Newsletter

For more information about
GDS Associates, our services,
staff, and capabilities, please visit
our website **@gdsassociates.com**
or call 770.425.8100

1850 PARKWAY PLACE SUITE 800 MARIETTA GEORGIA 30067 | 770.425.8100 | @gdsassociates.com