



FACT SHEET

Energy and policy- driven authorization: NERC CIP

What is NERC CIP?

NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) is a set of security standards that regulate, enforce, monitor and manage North America's Bulk Electric System (BES). Specifically, they apply to the cybersecurity aspects of the system to provide a framework to identify and secure critical assets, which can impact the efficient and reliable supply of electricity.



Policy-driven authorization and NERC CIP

[Policy-driven authorization](#) plays a crucial role in NERC CIP compliance.

Policy-driven authorization is used to grant access based on a user's location, role, the time of day, the device being used, the resource in question, and the desired action, ie., all the attributes necessary to enforce secure authorization in real-time. In the context of NERC CIP, [attribute-based access control \(ABAC\)](#) ensures only authorized individuals or systems have access to critical infrastructure components.

Six ways policy-driven authorization fits into NERC CIP

1. Fine-grained access control

Policy-driven authorization includes [fine-grained access control](#), which means you can define very specific rules about who can access what resources under what specific conditions. Finegrained access control is synonymous with ABAC and [policy-based access control \(PBAC\)](#).

2. Access decision at runtime

ABAC takes into account various attributes like user roles, environmental conditions, time of access, and more to make a decision at runtime. While this sounds similar to the first point, the difference here is that many access solutions in use today base these decisions only on static attributes that were assigned to the user in the past, such as a role. This dynamic approach to access is essential in the context of NERC CIP because it allows for adaptive access control based on ever-changing circumstances.

3. Compliance with NERC CIP standards

NERC CIP requires robust access controls to protect critical infrastructure. Policy-driven authorization provides a powerful mechanism to implement these controls, ensuring only authorized personnel can access sensitive systems and information. Visualization of a policy decision tree is an easy way to demonstrate an organization's compliance with the standards.

4. Mitigating insider threats

NERC CIP places significant emphasis on protecting against insider threats. Policy-driven authorization enables organizations to define policies that consider not only a user's role but additional attributes such as job function, location, and specific conditions. Equally as important is that these policies don't prevent key users from performing emergency actions during a 'break-glass' scenario. A good policy-driven authorization solution needs to be able to account for such scenarios by factoring in specific emergency attributes (i.e. fire alarm, temperature threshold, risk level) while still maintaining security.

5. Auditability and accountability

A robust policy-based authorization solution should include detailed logging and auditing capabilities. This is crucial for compliance with NERC CIP, as organizations must demonstrate that their access control policies are continuously enforced and that any unauthorized access attempts are logged.

6. Adapting to evolving threats

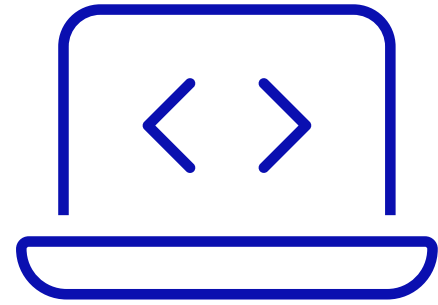
Cybersecurity threats are always evolving. ABAC's dynamic nature allows for organizations to adapt their access control policies to respond to new and emerging threats, which helps to maintain the security of critical infrastructure.



Take the next steps

Learn how a security vendor can help secure your access control while allowing you to focus on your core business initiatives.

[Meet with our solution experts for a demo](#) of our Axiomatics Authorization Management Platform and discuss how our approach can save your organization time and money.



Stay connected and informed

Get the latest insights, announcements, and assets from our thought leaders and customer success team:



[Blog articles](#)



[Press releases and announcements](#)



[Resources, solution briefs, and tools](#)



[Join us on LinkedIn](#)



[Subscribe to our LinkedIn Newsletter](#)



[Subscribe to our YouTube channel](#)

Axiomatics - a Leonardo Company is the originator and leading provider of runtime, fine-grained authorization delivered with attribute-based access control (ABAC) for applications, data, APIs, and microservices.

The company enables enterprises to effectively and efficiently connect Axiomatics' award-winning authorization platform to critical security implementations, such as Zero Trust or identity-first security. The world's largest enterprises and government agencies continually depend on Axiomatics' award-winning authorization platform to share sensitive, valuable, and regulated digital assets – but only to authorized users and in the right context.

Follow us on LinkedIn: <https://linkedin.com/company/axiomatics>

Join us on YouTube: <https://youtube.com/@axiomatics>

Learn more or request a demo of our solution:

axiomatics.com

info@axiomatics.com

US Office: +1 (312) 374-3443 | Europe Office: +46 8 51 510 240