

Turn Bulk-Power Equipment Risk into *Actionable Asset Intelligence*

How Axonius Cyber-Physical Assets and the wider platform help energy organizations build equipment and access context, prioritize risk, and support operational readiness.

What the order means for operators

Executive Order 14421 addresses national-security risk associated with bulk-power system electric equipment and related components, software, firmware, digital services, maintenance services, and remote-access capabilities supplied by a Covered Foreign Entity. It also extends to equipment already in service.

The operational challenge

The hard part is not simply finding devices. Operators need trustworthy asset context without introducing risk to live substations, control rooms, or generating environments.

Cyber-physical assets are frequently unmanaged or difficult to patch, use specialized protocols, and may support safety- or reliability-critical processes.

- Safe visibility: Use passive discovery rather than agents or intrusive scanning.
- Decision-ready context: Connect technical exposure to operational role and criticality.
- Faster response planning: Understand real communication paths before segmentation or isolation.
- Continuous evidence: Maintain current dashboards instead of relying only on point-in-time inventories.

Know what can access it and not only what is connected

Non-human identities (NHIs) are digital identities used by services, applications, workloads, devices, and automated processes; API keys, tokens, secrets, and certificates are common credentials used to authenticate those identities. Correlate equipment, identities, services, and providers to review ownership, privileges, approved remote access, credential lifecycle, and dormant or orphaned identities where source data supports it. Network observation alone cannot enumerate every identity, credential, or permission; connect identity, directory, secrets-management, PAM, and other authoritative management sources, and explicitly flag visibility gaps.

Evidence based readiness

Axonius supports evidence-based assessment and operational readiness; it does not determine legal applicability or certify compliance. Asset and access context supports customer procurement, security, and engineering decisions, not DOE approval or guaranteed uptime.

- Build passive visibility; validate selective active querying with operations.
- Link exposure and available access records to operational role and criticality.
- Validate observed communications and dependencies before segmentation or isolation.
- Keep dashboards, review evidence, and data-gap tracking current.

BOTTOM LINE

The order raises the urgency of knowing exactly what is connected, who made it, how it communicates, and which assets could create operational risk. Axonius provides a non-disruptive path to establish that foundation before new implementation requirements take effect.

KNOW WHAT YOU HAVE

Build an equipment inventory and correlate available NHI access records.

UNDERSTAND THE RISK

Add vendor, model, firmware, vulnerability, communication, and operational context.

PREPARE TO RESPOND

Support informed decisions to monitor, secure, isolate, disconnect, replace, or remove assets.

FROM ASSET CONTEXT TO OPERATIONAL READINESS

How Axonius Cyber-Physical Assets Supports the Mission

Cyber-Physical Assets (CPA) supplies OT/IoT asset and observed communication context. Axonius Identities and the wider platform correlate available identity and access records. Axonius Exposures consolidates findings and remediation context; optional AI capabilities can assist prioritization and recommend actions. These complementary capabilities support customer assessment and readiness, rather than determining statutory coverage or guaranteeing compliance.

MISSION ACTION	AXONIUS SUPPORTING EVIDENCE
IDENTIFY	CPA passively discovers connected cyber-physical assets and observes network activity without device agents.
INVENTORY	Fingerprints vendor, model, firmware, operating system, protocols, and operational role, then correlate the data into a unified asset record including NHI owners, services, providers, and associated credentials.
MONITOR	CPA continuously surface outdated firmware, insecure protocols, known vulnerabilities, and other exposure indicators.
PRIORITIZE	Combine equipment criticality and exposure with available identity findings: excess privileges, missing owners, dormant identities, and persistent vendor access to focus teams on the assets that matter most.
VALIDATE	Examine permissions alongside observed traffic and validate dependencies before proposing segmentation, isolation, or access changes.
REPORT	Track assessment evidence, NHI access reviews, data gaps, exceptions, and remediation for customer stakeholders through dashboards and connected workflows.

A practical starting point

Organizations do not need to wait for final implementing rules to improve readiness. A focused discovery and validation effort can establish the evidence needed for future policy, engineering, and replacement decisions.

1

ESTABLISH

Build a passive equipment inventory across substations, control rooms, and generating stations. Connect available identity and management sources to correlate NHI access records, validate ownership, and document gaps.

2

ENRICH

Capture vendor, model, firmware, ownership, location, operational role, and exposure. Add NHI owners, privileges, approved remote access, and credential lifecycle context where available. Where relevant, record AI-enabled monitoring or maintenance services, their providers, data access, and associated automation identities.

3

VALIDATE

Review high-risk equipment, permissions, excess privileges, missing owners, and persistent vendor access alongside observed traffic. Validate dependencies before changes to access or live equipment, obtain responsible engineering and operations approval, and follow change control. Track review evidence, exceptions, and remediation.

Trusted asset data for the AI era

Dependable power underpins AI and data-center workloads. Trusted asset and access data can support optional AI-assisted prioritization and evidence analysis; people approve changes affecting OT, reliability, and safety. This operational context is not an EO 14421 AI/NHI mandate or a promise of autonomous disconnection or privilege revocation.

Ready to assess your environment?

Engage your Axonius Federal Systems account team to review equipment visibility, NHI access, appropriate AI-supported workflows, and integration data gaps, then align a practical first step to your operational environment.

Validate federal and on-premises availability, supported integrations, licensing, and deployment configuration with your account team. Identity correlation and AI-assisted workflows are not assumed to be included in CPA alone; coverage depends on connected sources and configuration.