CYBERSECURITY IN THE ELECTRIC POWER SUPPLY SECTOR

Report produced by the Electric Power Supply Association (EPSA)

EPSA

ABOUT THE ELECTRIC POWER SUPPLY ASSOCIATION (EPSA)

Launched over 20 years ago, EPSA is the national trade association representing leading independent power producers and marketers. EPSA members provide reliable and competitively priced electricity from environmentally responsible facilities using a diverse mix of fuels and technologies. Power supplied on a competitive basis collectively accounts for 40 percent of the U.S. installed generating capacity.

EPSA seeks to bring the benefits of competition to all power customers.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Cyber and physical security are essential to electricity generation operations and represent a clear and extensive commitment by EPSA members, competitive suppliers, and independent power producers in the delivery of safe and reliable power to customers across the U.S. The electric power supply sector recognizes that its operations are the targets of increasingly sophisticated cyberattacks executed by a variety of attackers including nation-states and organized international criminals and is taking broad-based action to confront and prevent known and emerging threats.

The U.S. power grid is an interconnected system encompassing both the transmission and distribution networks, with utilities electrically tied together during normal system conditions to provide a synchronized transfer of power. There are seven regional transmission organizations (RTOs) and independent system operators (ISOs), formed at the direction of the Federal Energy Regulatory Commission (FERC), which operate the region's electricity grid, administer the region's wholesale electricity markets, and provide reliability planning for the region's bulk electricity system (BES). This structure not only prevents the manipulation of the electric power supply but ensures a high level of oversight and continuity for both cyber and physical security.

As such, electric power suppliers operate under a myriad of cyber and physical security regulatory regimes. Notably, they each participate in the development of, and comply with, North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards, which work to ensure the appropriate security measures are in place to protect the entirety of the BES.

Partnership between competitive suppliers and government agencies responsible for cybersecurity exists at every stage of operations. Generation companies are represented on the Electricity Subsector Coordinating Council (ESCC), the principal liaison between leadership across multiple federal agencies and the electric power sector. Companies also participate in bi-directional information sharing with the U.S. intelligence community via the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and its National Cybersecurity & Communications Integration Center (NCCIC) and are actively involved in the FBI InfraGard program.

Competitive suppliers multiply their efforts by participating in the Electricity Information Sharing and Analysis Center (E-ISAC) as well as events and training exercises including NERC GridEx and trainings offered by private experts, some of which are offered free of charge to encourage participation from electric suppliers of all sizes and resource levels. Companies are also engaged with the seven Regional Entities designated under NERC which hosts conferences and monthly and/or quarterly meetings.

Outside of these formal processes, competitive suppliers contract third party vendors to conduct cyber compromise assessments, and security subject matter personnel and officers attend an array of security conferences and seminars for education and to share information among similarly situated energy companies and across the electricity industry broadly.

Ensuring that all cyber and physical security considerations are fully addressed is central to the operations of all participants in the delivery of electricity to consumers, particularly independent power producers and competitive power suppliers who rely on capacity, energy and ancillary market revenues for service supplied to continue to operate, rather than guaranteed cost recovery from ratepayers.

Competitive suppliers recognize the challenge of balancing traditional societal electricity goals of reliability and reasonable costs with the critical goal of ensuring security. Given the diversity of power providers, business models, and asset portfolios, it is necessary to allow a level of flexibility to companies across the country to prioritize and address critical security matters. Multiple factors influence analyses and decisions regarding critical asset identification and risk threat assessments by individual companies, and while this concern is standard operating procedure for all generators, additional cost recovery avenues or mechanisms may merit consideration should the government opt to vastly ramp up or change cyber and physical security requirements.

COMPREHENSIVE CYBERSECURITY APPROACH

The electric sector takes seriously the responsibility to protect critical infrastructure in order to provide reliable energy for society. Companies recognize that their operations are the targets of increasingly sophisticated cyberattacks. As a result, competitive suppliers understand and treat cyberattacks as presenting enterprise-level risks and as such have implemented comprehensive approaches to cybersecurity.

STANDARDS + FRAMEWORKS

The cyber and physical security regulatory regimes under which energy suppliers operate ultimately shape each supplier's cybersecurity system operations and incident response approach. Most notably, each supplier participates in the development of, and complies with, NERC CIP standards.

North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Program

The NERC CIP program defines the reliability requirements for planning and operating the North American BES.[1] Standards are developed using a results-based approach that focuses on performance, risk management, and entity capabilities, and are constantly being updated to address emerging threats. The program, and compliance by electric sector companies, ensures the appropriate security measures are in place to protect the BES.

The NERC CIP program standards comprise 45 requirements that cover the security of all electronic perimeters as well as the protection of vital cyber resources, and ultimately shape provider systems and response approaches across all levels of operation including:

- Program Development and Management
- Compliance Audits and Assessments
- Patch Management
- Vulnerability Assessment and Management
- Incident Reporting of Cybersecurity Events and Quick Response Planning
- Mock Audits
- On-the-Spot and Unplanned Audits
- Asset Identification and Configuration Management
- Reliability Standard Audit Worksheet Development
- Systems Security Assessments and Management
- Personnel Training
- Policy, Process and Procedure Planning
- Development, Documentation and Evidence Reporting
- Security Information and Event Management
- Recovery Planning

Details of each standard including its purpose can be found in Appendix A.

NERC CIP STANDARDS

- CIP-002-5.1a: BES Cyber System Categorization
- CIP-003-7: Security Management Controls
- CIP-004-6: Personnel & Training
- CIP-005-5: Electronic Security Perimeter(s)
- CIP-006-6: Physical Security of BES Cyber Systems
- CIP-007-6: System Security Management
- CIP-008-5: Incident Reporting and Response Planning
- CIP-009-6: Recovery Plans for BES Cyber Systems
- CIP-010-2: Configuration Change Management and Vulnerability Assessments
- CIP-011-2: Information Protection
- CIP-014-2: Physical Security

The CIP program coordinates all of NERC's efforts to improve the North American power system's security. Beyond the development of standards, these efforts include compliance enforcement, risk and preparedness assessments, critical information dissemination, and key security issue awareness. The program applies not only to energy suppliers but to all entities that materially impact the reliability of the BES including owners, operators and users of any portion of the system.

Under the CIP program, entities are required to identify critical assets and to regularly perform risk analyses of those assets. In addition, the program requires entities to use firewalls to block vulnerable ports and the implementation of cyberattack monitoring tools. Entities are also required to enforce IT controls protecting access to critical cyber assets. Systems for monitoring security events must be deployed, and organizations must have comprehensive contingency plans for cyberattacks, natural disasters and other unplanned events.[2]

NERC utilizes compliance monitoring and an enforcement program to monitor, assess and enforce uniform compliance. At any time, electric providers—each a Registered Entity—may be subject to an audit or spot check for compliance with all applicable CIP Standards.

FERC has oversight and approval authority over this regime and is therefore well informed of the extensive work taking place at NERC in the development of new standards and constant improvement of existing standards. For instance, FERC Order No. 848 requires NERC to update CIP-008, the standard for cybersecurity incident reporting, which will require ISOs/RTOs to update practices and procedures associated with cybersecurity event investigations and incident investigation and reporting.

SPOTLIGHT ON: FERC OVERSIGHT

NERC and its Regional Entities regularly report to FERC on current and evolving activities to address system reliability, including threats or risks to the security of the system. As an example, on May 10, 2019, the Commission issued a Supplemental Notice of Technical Conference for its annual Reliability Technical Conference (Docket No. AD19-13-000). The first panel on the agenda featured leadership from NERC and its Regional Entities reporting to the Commission on current trends and risks to reliability, whether additional resources or steps are needed for certain types of risks, and how evolving threats are or should be addressed.

PUBLIC-PRIVATE COLLABORATION

Competitive suppliers work closely with cybersecurity-focused government agencies to ensure collaboration and communication at every available point. Industry-government collaboration on cybersecurity is part of the sector's all-encompassing approach to prepare for, respond to and recover from a wide array of threats and hazards. Initiatives and activities include classified briefings to share threat and risk information; organizing structures to improve information sharing; threat-specific and function-specific drills and exercise programs; ongoing information exchanges; and situational awareness reports.

Electricity Subsector Coordinating Council (ESCC)

The ESCC is a voluntary organization which was formed to support the nation's energy security and resilience mission in accordance with Presidential Policy Directive 21: Critical Infrastructure Security and Resilience; Executive Order 13636, Improving Critical Infrastructure Cybersecurity; and the National Infrastructure Protection Plan (NIPP).[3]

Competitive suppliers are represented on the ESCC through the participation of EPSA's CEO, who serves on the Council's nine-member Steering Committee. The ESCC functions as the principle liaison between leadership across multiple agencies in the federal government and in the electric power sector by convening CEO level decision-makers from all parts of the industry and government to coordinate efforts to prepare for national-level incidents or threats to critical infrastructure. At this forum, competitive suppliers and other electricity sector representatives are able to share clearance-level information and exchange best practices in order to better prepare for and protect against known and emerging threats.

RECENT PUBLIC POLICY ENABLES COMPETITIVE SUPPLIERS TO WORK COLLABORATIVELY WITH THE U.S. GOVERNMENT

EXECUTIVE ORDER 13636: Improving Critical Infrastructure Cybersecurity

Directs the Executive Branch to:

- Develop a technology-neutral voluntary cybersecurity framework
- Promote and incentivize the adoption of cybersecurity practices
- Increase the volume, timeliness and quality of cyber threat information sharing
- Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure
- Explore the use of existing regulation to promote cyber security

PRESIDENTIAL POLICY DIRECTIVE-21: CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Directs the Executive Branch to:

- Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time
- Understand the cascading consequences of infrastructure failures
- Evaluate and mature the public-private partnership
- Update the National Infrastructure Protection Plan
- Develop comprehensive research and development plan

NATIONAL INFRASTRUCTURE PROTECTION PLAN: PARTNERING FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes, including:

- Greater focus on integration of cyber and physical security efforts
- Closer alignment to national preparedness efforts
- Increased focus on cross sector and cross jurisdictional coordination to achieve results
- Integration of information-sharing as an essential component of the risk management framework
- Recognizing the key role and knowledge of critical infrastructure owners and operators

Cybersecurity and Infrastructure Security Agency (CISA) National Cyber Awareness System

Operating under DHS, the CISA provides extensive cybersecurity and infrastructure security knowledge and practices to its stakeholders, shares that knowledge to enable better risk management, and puts it into practice to protect the nation's essential resources.[4] The CISA oversees the National Cybersecurity and Communications Integration Center (NCCIC), which encompasses the functions previously performed independently by the U.S. Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to act as a hub for cybersecurity information and expertise.

CISA operates a National Cyber Awareness System to provide electric power suppliers and other stakeholders with 24/7 access to timely, actionable information about high-impact types of security activity affecting the community at large, as well as alerts about current security issues, vulnerabilities, and exploits available via email and RSS feed. They also provide stakeholders with weekly summaries of new vulnerabilities and patch information, when available, as well as in-depth cyber threat analysis reports.

FBI InfraGard Program

InfraGard is a partnership between the FBI and members of the private sector.[5] The program provides a vehicle for seamless public-private collaboration with government that expedites the timely exchange of information and promotes mutual learning opportunities relevant to the protection of critical infrastructure. Competitive suppliers join a diverse mix of InfraGard members including business executives, entrepreneurs, military and government officials, computer professionals, academics, and state and local law enforcement – each dedicated to contributing industry specific insight and advancing national security.

This forum serves as a platform for Chief Information Security Officers (CISOs), Chief Security Officers (CSOs), and their staffs from power and utility sector members to gather at regional, bi-monthly meetings to train and share intelligence and best practices to help protect their organizations and the grid. Each meeting has an assigned FBI special agent in attendance and typically also features an agent from DHS. Larger "all sector" InfraGard meetings are held in alternating months to maintain information sharing relationships with representatives from additional critical infrastructure sectors including transportation, oil and gas, healthcare and others.

FBI INFRAGARD PROGRAM OFFERINGS

The FBI InfraGard program bolsters the cybersecurity defenses of competitive suppliers through a myriad of offerings including:

- FBI and DHS threat advisories, intelligence bulletins, analytical reports and vulnerability assessments
- FBI and other government agency presentations to InfraGard chapters at member events
- Direct engagement with the FBI, other government agencies, and private sector experts at the local level
- Admittance to a members-only web portal providing access to the latest FBI intelligence as well as the opportunity to collaborate and share assessments and critical infrastructure protection information
- Opportunities to attend training events and briefings held by the FBI and its law enforcement partners
- Access to thousands of subject matter experts within critical infrastructure to share real time threat information as part of the sector chief program
- Invitations to regional and national InfraGard events

INFORMATION SHARING

Beyond their collaboration with government agencies, competitive suppliers participate in information sharing among sector stakeholders on security data gathering and analysis, incident management coordination, and communication mitigation strategies.

The Cybersecurity Act of 2015 enabled cybersecurity threat indicators to be shared between and among companies and the U.S. Government, established the legal requirements and protections for sharing, and established DHS as the hub for government and private sector cybersecurity information sharing.6 While DHS leads the federal government's efforts on this front, ISACs were created as the government recognized the importance of public-private partnerships in mitigating and responding to cybersecurity risks and events.7

CYBERSECURITY ACT OF 2015

Establishing the legal framework for cyber information sharing:

- Requires companies to protect information and share according to certain protocols
- Provides legal protections to companies when these requirements are met
- Establishes DHS as a hub for information sharing, providing a conduit for cyber threat indicators to flow back and forth from the private sector to the U.S. Government, including intelligence agencies
- Incentivizes the work of Information Sharing and Analysis Centers (ISACs) such as the E-ISAC

Electricity Information Sharing and Analysis Center (E-ISAC)

The E-ISAC offers security services to owner and operator organizations of the electricity industry across North America.[8] E-ISAC reduces cyber and physical security risk to the electricity industry across North America by providing unique insights, leadership and collaboration.

The E-ISAC serves as the primary security communications channel for industry and enhances the ability to prepare for, and respond to, cyber and physical threats, vulnerabilities, and incidents in collaboration with the Department of Energy (DOE) and the ESCC. The E-ISAC gathers, analyzes, and shares security information provided by members and partners; coordinates incident management; enables member to member sharing; and communicates mitigation strategies with stakeholders across interdependent sectors and with government partners.[9]

All electricity asset owners and operators and select government and cross-sector partners in North America may participate in E-ISAC activities, and membership is free of charge in order to encourage participation by companies of all sizes and resource levels.

E-ISAC PRODUCTS AND SERVICES:

- Secure portal supporting collaboration in a virtual team environment
- Data analytics and analysis
- Reports focused at different levels from analysts to executives
- Cyber and physical bulletins
- Malware drop box
- Industry Engagement Program (IEP)
- Cross-sector shares
- Vulnerability reports
- Monthly webinars
- Critical Broadcast Program
- Unclassified threat workshop
- Biennial grid security exercise (GridEx)
- Annual grid security conference (GridSecCon)
- Cybersecurity Risk Information Sharing Program (CRISP)
- Cyber Automated Information Sharing System (CAISS)

EVENTS + TRAINING EXERCISES

Competitive suppliers participate in events and training exercises on cybersecurity and physical security to ensure best practice operations and the latest in cybersecurity and cyber risk mediation tactics.

GridEx

NERC's Grid Security Exercise (GridEx) brings together organizations from across the electric supply sector as well as law enforcement and government agencies to allow electric providers to demonstrate how they would respond to and recover from simulated coordinated cyber and physical security threats and incidents, strengthen their crisis communications relationships, and provide input for lessons learned.

The exercise, conducted every two years, provides an opportunity for companies to expand their local and regional responses, engage interdependent sectors and improve communications. It also provides a method of increasing supply chain participation and gathering lessons learned for long-term improvement of cybersecurity programs.

GridSecCon

Since 2001, GridSecCon, held by the E-ISAC under NERC authority, has brought together cyber and physical security experts from industry and government to share emerging security trends, policy advancements, and lessons learned related to the electricity industry.[10] The conference focuses on promoting reliability of the bulk power system through training and education; delivering cutting-edge discussions on critical infrastructure security threats, vulnerabilities, and lessons learned from senior industry and government leaders; and informing industry with security best-practice discussions on reliability concerns, risk mitigation, and cyber and physical security threat awareness.

NERC Regional Events

Under the auspices of NERC, there are Regional Entities through which competitive suppliers engage, each of which hosts conferences and monthly and/or quarterly meetings to address and educate market participants on region-specific issues, risks and threats.[11]

DHS CISA Trainings

Under the DHS CISA, US-CERT offers both on-demand online and instructor-led training courses.[12] Online courses cover topics including Cybersecurity within IT and ICS domains, Current Threats, Current Trends, Determining the Impacts of a Cybersecurity Incident, and Attack Methodologies. Instructor-led program training events consist of regional courses and workshops in various locations in addition to a 5-day training event held in Idaho Falls, Idaho. All ICS-CERT training courses are presented with no tuition cost to the attendee.

Third-Party Assessments

Outside of these formal processes, competitive suppliers contract third party vendors to conduct regular, proactive cyber compromise assessments to continually evaluate and improve their risk posture.

ENSURING SUSTAINABLE OPERATIONS

Ensuring that all cyber and physical security considerations are fully addressed is central to the operations of all participants in the delivery of electricity to consumers, particularly independent power producers and competitive power suppliers who rely on capacity, energy and ancillary market revenues for service rendered, rather than guaranteed cost recovery from ratepayers. Any day with a service disruption is a day that a competitive power supplier is not able to conduct its business or sell its product. Further, any day with a service disruption is a day that customers will not be able to conduct their business or make or sell their products. Neither is acceptable. As a result, competitive suppliers are deeply committed to producing safe and reliable energy for delivery to customers across the country in a manner as secure as possible on both the cyber and physical fronts.

Competitive suppliers recognize the challenge of balancing traditional societal electricity goals of reliability and reasonable costs with the critical goal of ensuring security. Given the diversity of power providers, business models, and asset portfolios, it is necessary to allow a level of flexibility to companies across the country to prioritize and address critical security matters. Factors including company size, extent of asset ownership, transmission configuration, physical location and design of facilities, presence in organized wholesale markets, regional resource and system constraints, and prior patterns of theft, vandalism, and other security-related activities all influence analyses and decisions regarding critical asset identification and risk threat assessments by individual companies. While this concern is standard operating procedure for all generators based on their current market model, should the government opt to vastly ramp up or change cyber and physical security requirements, additional cost recovery avenues or mechanisms may merit consideration for companies that operate in market-based rate regimes.

CURRENT AVENUES FOR SECURITY COST RECOVERY

Competitive suppliers are currently able to recover costs associated with cyber and physical security through a number of sources, whether through market-based rates collected in the organized electricity markets, retail revenues, provisions within power purchase agreements or other sources of revenue. Looking forward, however, issues around cyber security and physical security continue to rapidly evolve and therefore deserve continued observation and analysis as a strategic matter.

Competitive suppliers understand, as DOE has indicated, that changes to the regulatory regime are necessary.[13] Competitive suppliers also understand, as FERC Chairman Neil Chatterjee has pointed out, that "it is not possible or cost effective to design our energy infrastructures to withstand every type of attack that could possibly occur. Striking the right balance for consumers is a complex, but important undertaking."[14]

Competitive suppliers recognize the challenge of balancing the goals of electric reliability and reasonable costs while ensuring security. EPSA members are continually working at improving their security solutions to enhance and refine their practices to protect cyber and physical systems. Should government entities deem it necessary to implement new standards or requirements or change current standards or requirements, there must first be an assessment of the flexibility that can be afforded to market participants and resource owners in addressing critical security matters. Organizations must consider a number of business risks (e.g., compliance, financial, operational, and reputational) for continuity and security. Companies' risk management programs are focused on reducing all broader business risks that an organization might face, including cyber and physical threats, by taking measures to ensure that available (but limited) resources are targeted at reducing critical risks. However, should changes to existing standards or requirements include more prescriptive practices to address cyber and physical security, or should threat levels continue to rise and diversify, additional opportunities for cost recovery may be necessary.

Additional Avenues for Cost Recovery if Needed

While cyber and physical security issues can arise from individual decisions or errors, these issues can affect the entire electric system. For this reason, all participants in the supply chain are and must be focused on threats to the system as a whole, as well as to the individual parts under their control as integral parts of that system. Accordingly, should additional unforeseen costs be imposed upon competitive suppliers in order to protect the system broadly or to address new risks, it may be reasonable that these costs be recovered on a regional or system-wide basis. As such, an area that may merit consideration is to reflect those costs in ISO/RTO capacity constructs which are designed to address a resource's fixed costs, including Operations and Maintenance (O&M).

While competitive suppliers recover costs through multiple organized wholesale markets, the markets come with parameters for which costs can and cannot be included in supplier bids. In the capacity markets, which are designed to address fixed costs for generation or supply resources, Net Cost of New Entry (Net CONE) is an estimate of the total project capital cost and annual fixed O&M expenses, over and above what can be earned in the energy and ancillary services markets, of a new generating plant of a type likely to provide incremental capacity in the forward delivery year or years addressed by the capacity auctions. As some of the cyber and physical security costs clearly fall into the O&M bucket, the capacity markets are where these costs should be appropriately priced and ultimately recovered. By reflecting these costs into Net CONE calculations, ISOs/RTOs will ensure that resources can be compensated through the capacity markets for their costs of doing business, including necessary cyber and physical security investments, when determining their expected revenues.

Additional Suggestions to Improve the Security of the Electric System and Individual Resources

Aside from cost recovery changes, there are additional aspects of the cyber and physical security regime that could be improved. One of the most effective tools in the security toolkit is the sharing of information, as the E-ISAC and ESCC demonstrate. However, even with robust programs like those in place, competitive suppliers have experienced a lag in receiving information about security incidents or specific threats which have taken place and may affect their own risk assessment. For instance, EPSA member companies have reported delays of 18-24 months from the date of an event before receiving notice that the event occurred, which makes preparing for and girding against these threats more difficult or not timely as the incident/threat may have already run its course or caused significant damage by the time they are briefed.

It is important that companies have access to the critical information needed to ensure that their systems and awareness are up to date. An important improvement would be to ensure that such information is not overly restricted as classified unless warranted, and that there are numerous persons at a company with the necessary security clearance to receive it. The security of the system is far too important to hinge on the availability of one or two people at a company with the necessary clearance to receive timely information. An efficient, timely process for granting security clearances is critical. This may require revisions or improvements to the clearance process, some of which could be specific to the energy industry. Such improvements would ensure that all affected entities receive the information needed, speed up the process of disseminating that information, and allow for faster response and mitigation.

CONCLUSION

Competitive suppliers prioritize cyber and physical security and have implemented comprehensive approaches to cybersecurity as a result. Through collaboration with government agencies responsible for cybersecurity and ongoing communication with industry partners, competitive suppliers are well equipped to address and to mitigate ongoing risk.

Competitive suppliers currently recover some of the costs they incur to meet and exceed regulatory requirements. Additional costs imposed on these entities may require additional avenues for cost recovery. Should such costs be imposed, alternative avenues must be considered while allowing for flexibility in complying with requirements in order to maximize an entity's resources, program, and approach to its own physical and cyber security.

Additionally, government must work to provide electric suppliers with timely access to the critical information needed to ensure that their systems and awareness are up to date, ensure that such information is not unnecessarily restricted, and that security clearances are available such that numerous persons at a company can receive such information.

Such improvements would allow for faster response and risk mitigation and strengthen the overall security of the nation's grid.

ACRONYMS AND ABBREVIATIONS

BES	Bulk Electric System
CIP	NERC Critical Infrastructure Protection Standards
CISA	Cybersecurity and Infrastructure Security Agency
CISOs	Chief Information Security Officers
CSOs	Chief Security Officers
DHS	U.S. Department of Homeland Security
DOE	Department of Energy
E-ISAC	Electricity Information Sharing and Analysis Center
EPSA	Electric Power Supply Association
FERC	Federal Energy Regulatory Commission
GridEx	NERC's Grid Security Exercise
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ISAC	Information Sharing and Analysis Center
ISOs	Independent System Operators
NCCIC	National Cybersecurity and Communications Integration Center
NERC	North American Electric Reliability Corporation
Net CONE	Net Cost of New Entry
NIPP	National Infrastructure Protection Plan
O&M	Operations and Maintenance
PPD	Presidential Policy Directive
RTOs	Regional Transmission Organizations
US-CERT	U. S. Computer Emergency Readiness Team

APPENDICES

APPENDIX A: NERC CIP CYBERSECURITY STANDARDS: STANDARD VERSION, TITLE AND PURPOSE

CIP-002-5.1a BES Cyber System Categorization

To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to mis-operation or instability in the BES.

CIP-003-6 Security Management Controls

To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to mis-operation or instability in the BES.

CIP-004-6 Personnel & Training

To minimize the risk against compromise that could lead to mis-operation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

CIP-005-5 Electronic Security Perimeter(s)

To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to mis-operation or instability in the BES.

CIP-006-6 Physical Security of BES Cyber Systems

To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to mis-operation or instability in the BES.

CIP-007-6 System Security Management

To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to mis-operation or instability in the BES.

CIP-008-5 Incident Reporting and Response Planning

To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

CIP-009-6 Recovery Plans for BES Cyber Systems

To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

CIP-010-2 Configuration Change Management and Vulnerability Assessments

To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to mis-operation or instability in the BES.

CIP-011-2 Information Protection

To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to mis-operation or instability in the BES.

CIP-014-2 Physical Security

To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection.

REFERENCES

[1] **North American Electric Reliability Corporation.** "Critical Infrastructure Protection Standards," https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[2] **Search Compliance.** "NERC CIP," https://searchcompliance.techtarget.com/definition/NERC-CIP-critical-infrastructure-protection

[3] **Department of Homeland Security.** "Electricity Sub-Sector Coordinating Council Charter," https://www.dhs.gov/sites/default/files/publications/Energy-Electricity-SCC-Charter-2013-508.pdf

[4] **Cybersecurity and Infrastructure Security Agency (CISA).** "About us," https://www.us-cert.gov/about-us

[5] **Federal Bureau of Investigation.** "InfraGard," https://www.infragard.org/

[6] **U.S. Government.** "The Consolidate Appropriations Act, 2016," https://www.congress.gov/bill/114thcongress/house-bill/2029?q=%7B%22search%22%3A%5B%22%5C%22cybersecurity+act+of+2015%5C%22%22%5D%7D&r=2

[7] **Department of Homeland Security.** "Fact Sheet: Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD) 21 Critical Infrastructure Security and Resilience," https://www.dhs.gov/publication/eo-13636-ppd-21-fact-sheet

[8] **Electricity Information Sharing and Analysis Center.** https://www.eisac.com/

[9] **Electricity Information Sharing and Analysis Center.** "Products and Services Brochure," https://www.eisac.com/cartella/Asset/00007758/E-ISAC%20Brochure_March%202019.pdf?parent=119902

[10] **North American Electric Reliability Corporation.** "GridSecCon," https://www.nerc.com/pa/CI/CIPOutreach/Pages/GridSecCon.aspx

[11] **North American Electric Reliability Corporation.** "Regional Entity Compliance Programs ," https://www.nerc.com/pa/comp/Pages/Regional-Programs.aspx

[12] **Cybersecurity and Infrastructure Security Agency (CISA).** "Training Available Through ICS-CERT," https://www.us-cert.gov/ics/Training-Available-Through-ICS-CERT

[13] **Federal Energy Regulatory Commission/Department of Energy.** "Security Investments for Energy Infrastructure. Technical Conference, Docket No. AD19-12-000. Transcript," p. 165, DOE Assistant Secretary Bruce Walker, "[T]he status quo does not work." https://www.ferc.gov/CalendarFiles/20190426140022-Transcript%20032819FERC_DOESecurity.pdf

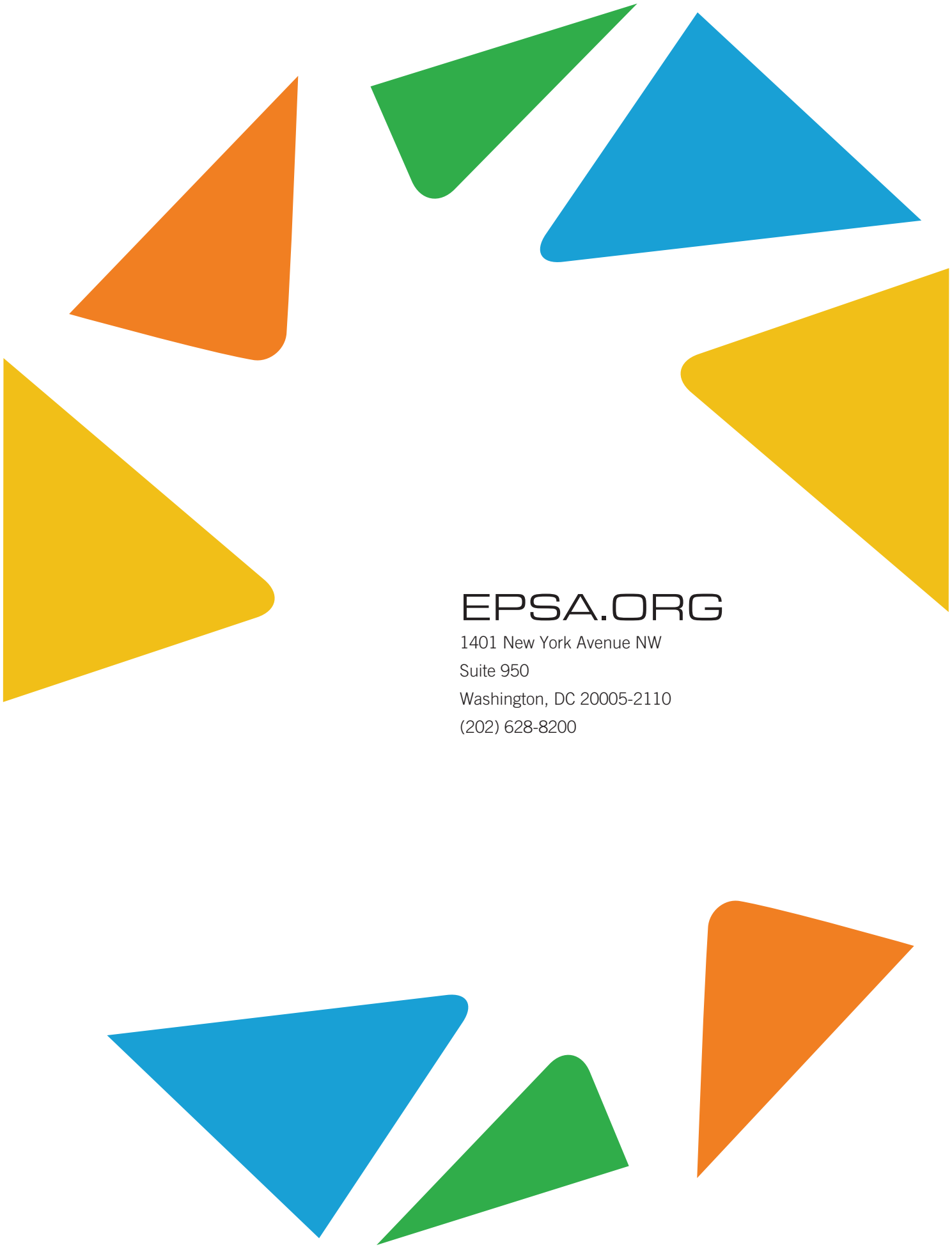
[14] **Ibid.** p. 9.

What is EPSA?

Since its inception, EPSA has grown to become the leading national trade association representing independent power producers and marketers.

EPSA's public policy advocacy has long focused on achieving and maintaining well-functioning and properly regulated competitive wholesale electricity markets. EPSA's efforts occur primarily at the federal level at the White House and before the U.S. Congress, Department of Energy, Federal Energy Regulatory Commission, Commodity Futures Trading Commission, and other Executive Branch agencies. EPSA is often a participant in federal court litigation over wholesale market regulatory issues, including roles in two leading U.S. Supreme Court decisions. In addition, EPSA is actively involved in select state-level proceedings that directly impact wholesale electricity markets and represents the competitive power sector at meetings of the National Association of Regulatory Utility Commissioners.

EPSA members provide reliable and competitively priced electricity from environmentally responsible facilities using a diverse mix of fuels and technologies, including natural gas, nuclear, coal and renewables. EPSA member company power generation assets are primarily located in the regions of the country with Independent System Operators and Regional Transmission Organizations because that approach provides better market access and investment signals. EPSA members have invested billions of dollars at their risk without ratepayer subsidies to achieve the goals Congress set out in the Energy Policy Acts of 1992 and 2005 to bring market forces to bear on the power sector. EPSA seeks to bring the benefits of competition to all power customers.



EPSA.ORG
1401 New York Avenue NW
Suite 950
Washington, DC 20005-2110
(202) 628-8200