ESCC
Electricity Subsector Coordinating Council

The ESCC's Cyber Mutual Assistance Program

The Electric Power Industry Shares Expertise To Counter Cyber Attacks

Cyber Defense: Building on the Industry's Culture of Mutual Aid

The North American energy grid is a complex interconnected network of generation, transmission, and distribution systems operated by thousands of organizations. Protecting the energy grid and ensuring a reliable and affordable supply of energy are the top priorities of the electric power industry. Creating a "defense-in-depth" approach requires partnerships and coordination with the government and other critical infrastructure sectors. To coordinate security strategies with the federal government and other stakeholders, the electric power industry has created a CEO-led partnership called the Electricity Subsector Coordinating Council (ESCC).

For decades, the electric power industry has operated voluntary mutual assistance programs that work collaboratively to restore electricity following storms, earthquakes, wildfires, and other natural disasters. These mutual assistance programs provide a formal, yet flexible, process for companies to request assistance from one another.

Today, the industry's culture of mutual assistance is a model for creating responses to cyber threats to the energy grid. Based on lessons from major destructive cyber incidents overseas, and from exercises in North America, the ESCC recommended the formation of a Cyber Mutual Assistance (CMA) Program: a series of initiatives that are a natural extension of the electric power industry's longstanding approach of sharing critical personnel and equipment when responding to emergencies. By coordinating with the government and providing mutual assistance to address cyber threats, the electric power industry is greatly enhancing our nation's ability to defend and protect against threats and to meet customers' expectations.

Delivering and Coordinating Cyber Mutual Assistance: How It Works

- The first initiative undertaken by the CMA Program is the creation of a Pool of industry cyber experts who are able to provide voluntary assistance to each other in the event of cyber disruptions to the energy grid.
- Participation in the Pool is open to all organizations that provide or materially support the provision of electricity.
- Participation in the Pool and response to requests for assistance made within the Pool are voluntary. There is no cost for organizations to participate in the Pool (other than the reimbursement of the expenses incurred in providing emergency cyber assistance).
- To participate in the Pool, organizations must execute a mutual non-disclosure agreement so that all participants are assured that confidential information they may share will be protected.
- Each participant in the Pool must designate one employee with appropriate cyber skills and experience, and the necessary authority, to represent the participant in the Pool (the CMA Coordinator).
- Cyber mutual assistance is intended to be advisory and short-term. It may include services, personnel, and/or equipment.

Frequently Asked Questions About Cyber Mutual Assistance

What is the Cyber Mutual Assistance Program?

The Cyber Mutual Assistance (CMA) Program refers to a series of industry initiatives developed at the direction of the ESCC to provide emergency cyber assistance within the electric power industry. The first initiative under the CMA Program is the development of a Pool of industry cyber experts who can provide voluntary assistance to other organizations in the event of a disruption to the energy grid due to a cyber emergency. As the CMA Program develops, additional initiatives will be considered and implemented based on the needs and input of the entities participating in the CMA Program.

How can I participate in the CMA Program?

In order to participate in the CMA Program, each participating entity must (1) sign a Mutual Non-Disclosure and Use of Information Agreement, and (2) also designate a Cyber Mutual Assistance Coordinator (CMA Coordinator).

What does a CMA Coordinator do?

A CMA Coordinator is a participant's single point of contact for all matters related to the CMA Program, including the Pool. He or she is responsible for assessing his/her organization's cyber resources and responding to another participant's request for assistance, or making a request for emergency assistance on behalf of his or her company. He or she also is responsible for preparing and coordinating internal resources in connection with any assistance that his or her participating entity elects to provide.

What are the qualifications for a CMA Coordinator?

A CMA Coordinator must be a senior-level employee of a participating entity with the authority to act on behalf of the participating entity it represents. In addition, he or she must be an expert who possesses or manages sufficient cybersecurity, operating technology, and information technology skills and experience in order to be able to request, or respond to a request for, a broad range of emergency cyber needs in the context of a potentially complex and evolving cyber emergency. He or she must have sufficient understanding of the cyber functions, security, recovery processes, and available resources at his or her participating entity.

How does the Pool work?

In the event of a cyber emergency, any participant may make a direct request for assistance through its CMA Coordinator to any other CMA Coordinator, or may make a broader request to multiple or all CMA Coordinators.

What kind of assistance is provided by the Pool?

In responding to a request for assistance, a participating entity's response is voluntary, intended to be advisory in nature, and provided on a short-term basis. Assistance may include services, personnel, and/or equipment.

For more information about the CMA Program or to become a participant, please visit www.electricitysubsector.org/CMA or contact cma@electricitysubsector.org.

April 2017

JUNE 2017

ESCC

Electricity Subsector Coordinating Council

Protecting the energy grid from threats that could impact national security is a responsibility shared by both the government and the electric power sector.

The Electricity Subsector Coordinating Council (ESCC) serves as the principal liaison between the federal government and the electric power sector, with the mission of coordinating efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure. The ESCC includes electric company CEOs and trade association leaders representing all segments of the industry. Its counterparts include senior Administration officials from the White House, relevant Cabinet agencies, federal law enforcement, and national security organizations.

Background

In October 2010, the National Infrastructure Advisory Council (NIAC) issued a report, *A Framework for Establishing Critical Infrastructure Resilience Goals*, that included nine recommendations. The first recommendation was:

> **NIAC Recommendation:** "The White House [will] initiate an executive-level dialogue with electric and nuclear sector CEOs on the respective roles and responsibilities of the private sector in addressing high-impact infrastructure risks and potential threats… ."

This recommendation was the impetus for initial meetings in July 2012 between an ad hoc group of industry CEOs and Department of Energy (DOE) Secretary Steven Chu and Department of Homeland Security (DHS) Secretary Janet Napolitano. These meetings resulted in a classified briefing for the industry in September 2012 and led to the formation of the Joint Electric Executive Committee, which was convened in January 2013 and which had a commitment to meet quarterly with the Deputy Secretaries of DOE and DHS.

Ultimately, the Joint Electric Executive Committee transitioned to its current official role as the ESCC.

ESCC Areas of Focus

Industry and government leaders have agreed to focus on four main areas that improve the security posture of the industry and the nation. To support the deployment of tools, improve the flow of threat information, prepare for incidents, and work closely with other interdependent infrastructure sectors, the ESCC has organized into strategic committees with the following missions:

Threat Information Sharing: Improve and institutionalize the flow of, and access to, actionable information among public- and private-sector stakeholders.

Industry-Government Coordination: Establish unity of effort and unity of messaging between industry and government partners to support the missions of the ESCC both during crises and in steady state.

Research & Development: Coordinate government and industry efforts on strategic infrastructure investments and R&D for resilience and national security-related products and processes.

Cross-Sector Liaisons: Develop strong partnerships at all levels of the Electricity, Communications (Telecommunications), Oil and Natural Gas (Downstream Gas), Financial Services, Transportation Systems, and Water and Wastewater Systems (Water) sectors to plan and respond to major incidents, to better understand and protect our mutual dependencies, and to share information effectively and efficiently to improve cross-sector situational awareness.

Security Executive Working Group

To support the mission of the ESCC, a Security Executive Working Group (SEWG) convenes by phone on a monthly basis and creates ad hoc teams to accomplish the goals identified by the CEOs and Deputy Secretaries. In parallel to this effort, the government also has organized around these goals with a commitment to align government and industry efforts.

ESCC Official Roster

June 2017

Leadership (3)

Tom Fanning, Southern Company (co-chair)
Kevin Wailes, Lincoln Electric System (co-chair)
Duane Highley, Arkansas Electric Cooperative (co-chair)

Steering Committee (9)

Sue Kelly, American Public Power Association
Sergio Marchi, Canadian Electricity Association
Tom Kuhn, Edison Electric Institute
John Shelk, Electric Power Supply Association
Andrew Ott, PJM (representing the ISO/RTO Council)
Mike Wallace, National Infrastructure Advisory Council
Jim Matheson, National Rural Electric Cooperative Association
Gerry Cauley, North American Electric Reliability Corporation
Maria Korsnick, Nuclear Energy Institute

Asset Owners
(19: 13 investor-owned electric companies; 3 electric cooperatives; 3 municipal electric companies)

Nick Akins, American Electric Power
Jim Torgerson, Avangrid
Scott Miller, City Utilities of Springfield
John McAvoy, Consolidated Edison
Tom Farrell, Dominion
Lynn Good, Duke Energy
Pedro Pizarro, Edison International
Gianna Manes, ENMAX Corporation
Chris Crane, Exelon Corporation
Greg Ford, Georgia System Operations Corporation
David Saggau, Great River Energy
Connie Lau, Hawaiian Electric Industries
William Fehrman, MidAmerican Energy Co.
John Bilda, Norwich Public Utilities
Jack Reasor, Old Dominion Electric Cooperative
Tony Earley, PG&E Corporation
Bill Spence, PPL Corporation
Lonnie Carter, Santee Cooper
Ben Fowke, Xcel Energy

ESCC Coordination

Coordination among senior government and industry executives helps to ensure an effective response, appropriate prioritization and allocation of resources, and support for deviation from standard procedures during an incident.

ESCC Stakeholders

Government

- Federal Agencies
- Regulators
- PMAs
- Law Enforcement
- State, Local, Tribal, & Territorial
- Canadian Agencies & Provinces

Industry

- Electric Companies
- Trade Associations
- ISOs & RTOs
- NERC
- E-ISAC
- Canadian Electric Companies

External Groups

- Other Critical Sectors
- Vendors
- Critical Customers
- Media

Coordination

- Security to support restoration
- Media and public affairs messaging
- Logistical support, staging

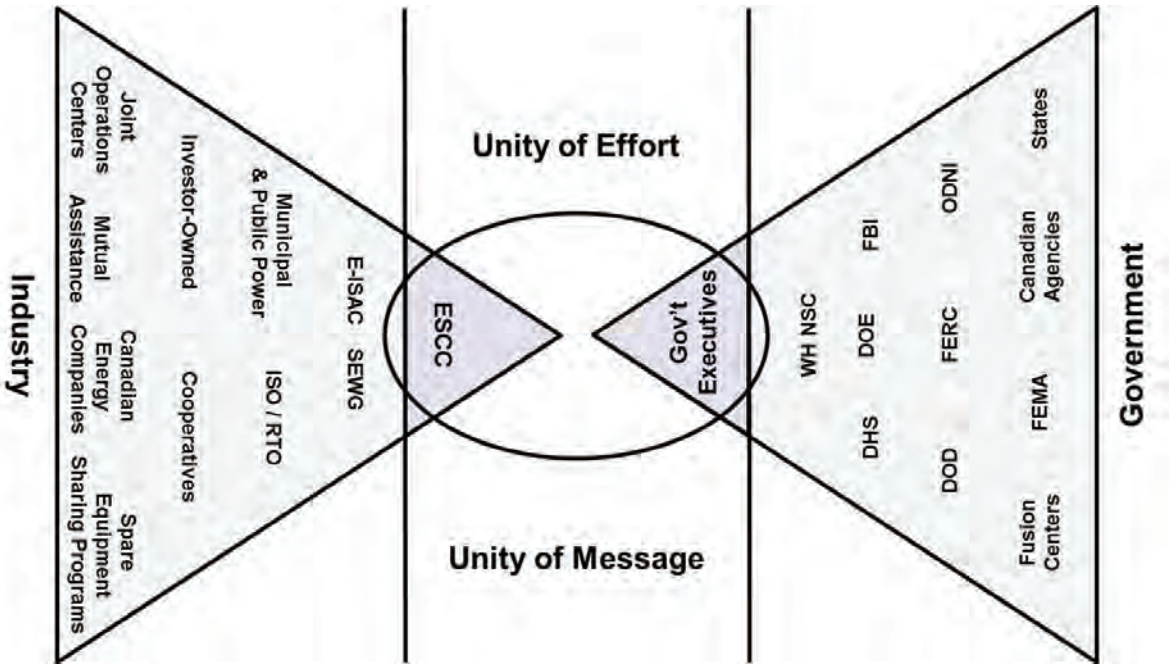
Resource Allocation

- Equipment, hardware, and materials
- Human resources and expertise

Conflict Resolution

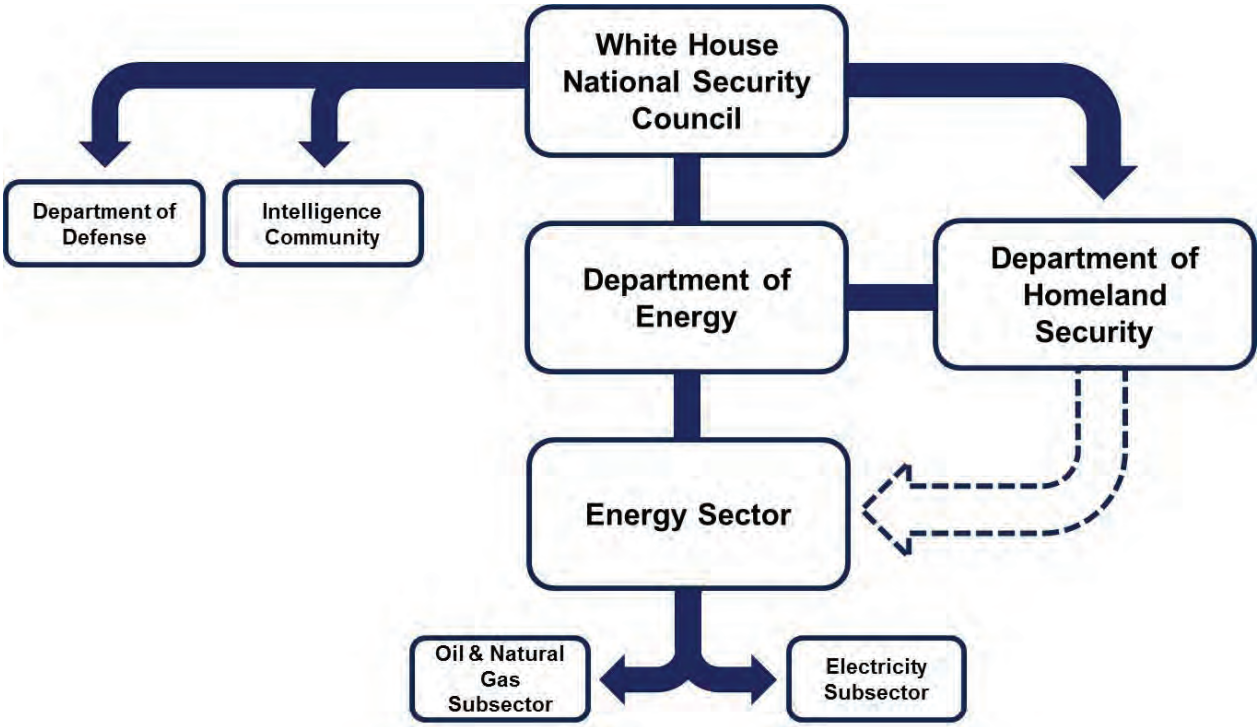
- Investigation versus restoration
- Prioritization of recovery
- Distribution of limited resources

Industry-Government Coordination



ESCC Member Structure

Energy Sector-Government Organizational Structure



ESCC
Electricity Subsector Coordinating Council

ESCC

Electricity Subsector Coordinating Council

The CEO-led Electricity Subsector Coordinating Council (ESCC) serves as the principal liaison between the federal government and the electric power industry, with the mission of coordinating efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure. The National Infrastructure Advisory Council called the ESCC a model for how critical infrastructure sectors can more effectively partner with government. The ESCC has been a catalyst for major initiatives that are improving the security posture of the industry and, by extension, the nation.

The ESCC is taking action on issues in three main areas: facilitating coordination with the government and other critical infrastructure sectors; improving information sharing capabilities, tools, and technologies; and enhancing resilience, response, and recovery efforts.

Industry-Government and Cross-Sector Coordination

The ESCC works across the electric power industry, with the government, and with other interdependent critical infrastructure sectors to improve planning for and response to major incidents. This includes conducting joint exercises, fostering a better understanding and protection of our mutual dependencies, and sharing information more effectively.

ESCC Playbook

The ESCC Playbook provides a framework for senior industry and government executives to coordinate response and recovery efforts and communications to the American public. The Playbook has been tested in a series of exercises.

Strategic Infrastructure Coordinating Council (SICC)

Given the criticality and interdependencies, the electric, communications, and financial services sector coordinating councils will form the SICC. The SICC will identify mutual priorities, develop and exercise cross-sector incident response plans and protocols, as well as align organizations, systems, processes, and technologies across sectors. The SICC also will serve as a focal point for government engagement with strategic infrastructure in steady-state and during crises. The SICC will convene a small group of senior executives representing the three sectors.

Supply Chain Security

The ESCC, in coordination with the government, has convened industry and government stakeholders, along with security and technology vendors, to identify and share best practices to address threats to the supply chain.

R&D Alignment

The industry is collaborating with the government, the national labs, and the investment community on resilience and infrastructure investments for grid security R&D.

Electromagnetic Pulse (EMP)

The ESCC has formed a task force to coordinate with the government and other critical infrastructure sectors on a national response to the threat of high-impact, low-frequency risks such as an EMP attack. The ESCC is supporting the Electric Power Research Institute's EMP Project, which will determine the vulnerability of and mitigation approaches for high-voltage and electronic equipment installed on the transmission system to various EMP threats; provide a scientific basis for investments to mitigate EMP threats to the energy grid; and inform response and recovery efforts.

Information Sharing and Tools and Technology

The ESCC works with the government and the private sector to deploy the latest tools and technologies to improve situational awareness and enable machine-to-machine information sharing.

Electricity Information Sharing and Analysis Center (E-ISAC) Member Executive Committee (MEC)

In 2015, the ESCC formed the MEC to advise the E-ISAC on ways in which the industry can speed delivery and analysis of potential threats to the power system. The MEC provides industry leadership and expertise to guide and support the E-ISAC vision and mission.

Cybersecurity Risk Information Sharing Program (CRISP)

CRISP is a public-private partnership co-funded by the Department of Energy (DOE) and industry and managed by the E-ISAC. CRISP seeks to facilitate timely bi-directional sharing of actionable unclassified and classified threat information, using advanced collection, analysis, and dissemination tools to identify threat patterns and trends across the electric power industry.

Other Information Sharing Programs

E-ISAC, DOE, and DHS are developing additional information sharing tool programs to pilot and bring to market (Enhanced Analytics, Operational Technology Pilot, Operational Technology Sensor Project, STIX/TAXII Pilot, etc.).

Response and Recovery

During an incident, the ESCC's role is to provide situational awareness, align messaging, and serve as a counterpart for government executives on response and recovery efforts.

Mutual Assistance Programs

The three segments of the electric power industry—investor-owned, municipal, and cooperative electric companies—have voluntary mutual assistance programs in place to allocate resources in support of power restoration to participating electric companies for severe weather events.

Cyber Mutual Assistance

The ESCC has established a task force to develop a cyber mutual assistance program to aid electric companies in restoring necessary computer systems in the event of a regional or national cyber incident. This program builds on the electric power industry's culture of mutual assistance to develop resource sharing relationships that provide surge capacity should a cyber incident exceed the capacity for an individual company to respond.

Spare Equipment Programs

Electric companies also regularly share transformers and other equipment. The industry is expanding equipment sharing programs—like the Spare Transformer Equipment Program, SpareConnect, and the newly formed Grid Assurance program—to improve grid resilience from a range of threats.

Transformer Transportation Emergency Support Guide

The ESCC, in coordination with other critical infrastructure sectors and the government, has developed a Transformer Transportation Emergency Support Guide to expedite the deployment of large spare equipment, such as transformers, quickly over our rails, roadways, and waterways in an emergency.

Supplemental Operating Strategies

Following GridEx III and the cyber incident affecting Ukrainian electric companies, there has been a focus on operating the energy grid under sub-optimal circumstances. Whether resorting to manual operations, engaging in planned separations, leveraging secondary and tertiary back-up systems, or operating in other degraded states, the ESCC has asked grid experts to explore "extraordinary measures" that can be anticipated, planned for, and practiced so these are not being contemplated for the first time during an incident.

Exercises

Electric companies plan and regularly exercise for a variety of emergency situations that could impact their ability to provide electricity. The industry has participated in many incident response exercises, including several national-level exercises since November 2015.

I. **Clear Path V** *(DOE, June 2017)* convened 200 plus participants from the Federal government and the electricity and natural gas subsectors, as well as the telecommunications sector to explore how industry and government would respond to a major hurricane strike on the Houston, TX region.

II. **FEMA Region III** *(FEMA, May 2017)* conducted a power outage exercise that focused on how Federal, state, and local emergency managers would work with the electricity industry to respond to a physical/cyber attack on the mid-Atlantic regions power grid.

III. **Joint Financial Services—Electric Sector Cyber Exercise** *(Treasury, August 2016)* examined incident response capabilities and interdependencies between the two sectors.

IV. **Cascadia Rising** *(FEMA, June 2016)* was a three-day exercise that tested first responders and government emergency personnel responses in the immediate aftermath of a significant earthquake.

V. **Cyber Guard** *(DOD/NSA, June 2016)* was a two-week exercise that tested the response capabilities of 1,000 energy, IT, transportation, and government experts to a major cyber attack.

VI. **GridEx III** *(NERC, November 2015)* gathered more than 360 organizations and 4,400 participants from industry, government agencies, and partners in Canada and Mexico. GridEx III also included an executive tabletop exercise where 32 electric sector executives and senior U.S. government officials worked through incident response protocols to address widespread outages.