Defense Critical Electric Infrastructure

Jennifer DeCesaro, Director, Recovery and Resilience

Johanna Zetterberg, DCEI Action Officer

U.S. DOE Office of Electricity, Transmission Permitting & Technical Assistance

Electricity Advisory Committee

October 14, 2020

U.S. DEPARTMENT OF ENERGY | OFFICE OF ELECTRICITY

"Our adversaries and strategic competitors will increasingly use cyber capabilities to seek political, economic, and military advantage over the United States and its allies and partners."

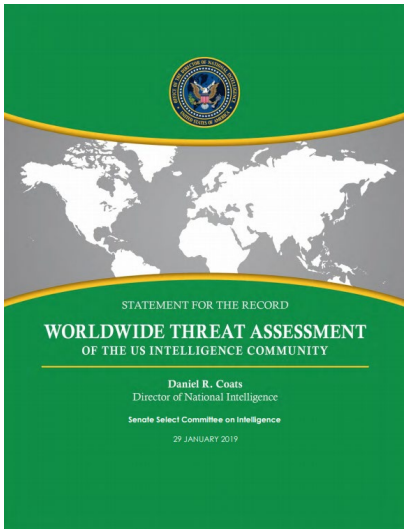
"**China has the ability** to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure in the United States."

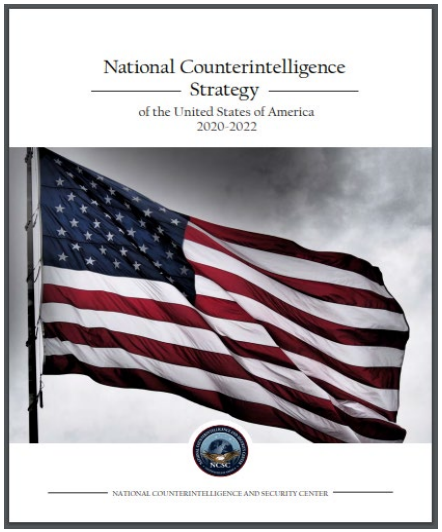
"**Russia has the ability** to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure…. Moscow is mapping our critical infrastructure with the long-term goal of being able to cause substantial damage."

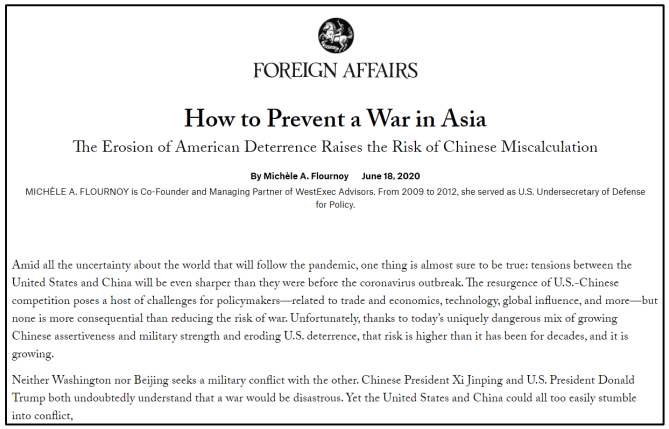
Daniel R. Coats, Director of National Intelligence
Testimony to Senate Select Committee on Intelligence, January 29th 2019

Energy Sector Threats to U.S. National Security

- Peer-level adversaries are capable, determined, and active
- Hybrid warfare tactics include system destruction warfare targeting C4ISR networks
- Cyberattacks and all hazards threaten U.S. military OPLANs as well as the health and safety of American civilians







FOREIGN AFFAIRS

How to Prevent a War in Asia

The Erosion of American Deterrence Raises the Risk of Chinese Miscalculation

By Michèle A. Flournoy June 18, 2020

MICHÈLE A. FLOURNOY is Co-Founder and Managing Partner of WestExec Advisors. From 2009 to 2012, she served as U.S. Undersecretary of Defense for Policy.

Amid all the uncertainty about the world that will follow the pandemic, one thing is almost sure to be true: tensions between the United States and China will be even sharper than they were before the coronavirus outbreak. The resurgence of U.S.-Chinese competition poses a host of challenges for policymakers—related to trade and economics, technology, global influence, and more—but none is more consequential than reducing the risk of war. Unfortunately, thanks to today's uniquely dangerous mix of growing Chinese assertiveness and military strength and eroding U.S. deterrence, that risk is higher than it has been for decades, and it is growing.

Neither Washington nor Beijing seeks a military conflict with the other. Chinese President Xi Jinping and U.S. President Donald Trump both undoubtedly understand that a war would be disastrous. Yet the United States and China could all too easily stumble into conflict,

What is DCEI – Part I / Federal Power Act

Critical Defense Facility

"critical to the defense of the United States," and "vulnerable to a disruption of the supply of electric energy provided to such a facility by an external provider"

Defense Critical Electric Infrastructure

"any electric infrastructure that serves" a Critical Defense Facility, "but is not owned or operated by the owner or operator of such facility"

Current statutory definitions for these terms include a specification that they are located in any of the 48 contiguous States or the District of Columbia

DOE Approach to DCEI

Defense Critical Electric Infrastructure:

- Is a **priority** for the Department of Energy
- Requires **unity of effort and a structured approach** for a whole-of-government, coordinated public/private response to evolving, dynamic and intensifying threats
- Must be differentiated from the broader energy system with risk management based on a **Mission Assurance framework**

What is DCEI – Part II / Mission Assurance

Additional considerations for program scope:

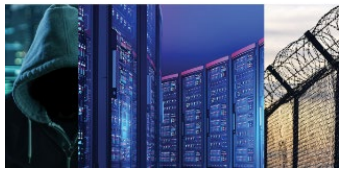
1. Transparency and coordination across the fence line
2. Energy system interdependencies
3. Highest priority/risk equipment and components
4. Other (non-energy sector) critical infrastructure

Key DOE Authorities Supporting DCEI

Authority / Directive	Capabilities Enabled	Source	Lead Office
Statutory			
Designation of Critical Defense Facilities	Identification and protection of DCEI	Federal Power Act Sec. 215A	OE
Grid Security Emergency Orders	Maintaining or accelerating restoration of electricity service to CDFs	Federal Power Act Sec. 202(c)	OE
Executive			
Bulk-power system (BPS) cybersecurity risk management	Prohibits potentially manipulated equipment from the BPS based on risk	Executive Order 13920	OE
Energy sector cybersecurity of critical infrastructure	Leverage federal authorities and capabilities to support cybersecurity of "Section 9 entities"	Executive Order 13800	CESER
Sector-Specific Agency for the energy sector	Coordination of national effort for critical infrastructure security and resilience, response to cyber incidents involving government or private sector	FAST Act, PPD-21, PPD-41	CESER

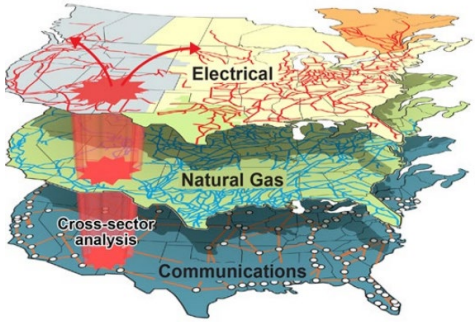
Example DOE Technical Capabilities Relevant to DCEI

GridEx V
GRID SECURITY EXERCISE 2019



ENERGY TRANSITIONS INITIATIVE

FEMP
Federal Energy Management Program



Advanced Grid Research
OFFICE OF ELECTRICITY
US DEPARTMENT OF ENERGY

GRID MODERNIZATION LABORATORY CONSORTIUM
U.S. Department of Energy

Mature

Nascent

Modeling & Analysis

Technical Assistance

DCEI Program Pillars - Year 1

Critical defense and security missions are energy-assured such that priority operational plans are consistently resilient to threats to power or fuel supply disruptions.

1. Establish a DCEI Coordinated Program Platform

A. Program goals, strategy, work plans and resources

B. Maintenance of Critical Defense Facility designations

C. Comprehensive review of authorities and capabilities at DOE, national labs, and partner organizations

D. Gap analyses and plans / resources to address gaps

2. Develop DCEI Funding Strategies

E. Explore all potential sources for DCEI funding and financing
Including federal sources, innovative and alternative financing, state programs and traditional sources of grid investments.

F. Develop strategies to access funding for DCEI
Based on opportunities at installation, utility service territory, regional, national or other levels.

3. Create and Maintain Key Partnerships

G. Refine needs for partner and stakeholder information sharing, coordination and collaboration.
CDF owners and operators; DCEI owners and operators; SLTT governments; PMAs; security, intelligence and law enforcements communities; grid reliability organizations; technical assistance providers; other federal agencies and others.

4. Guide and Support Analytical Capabilities

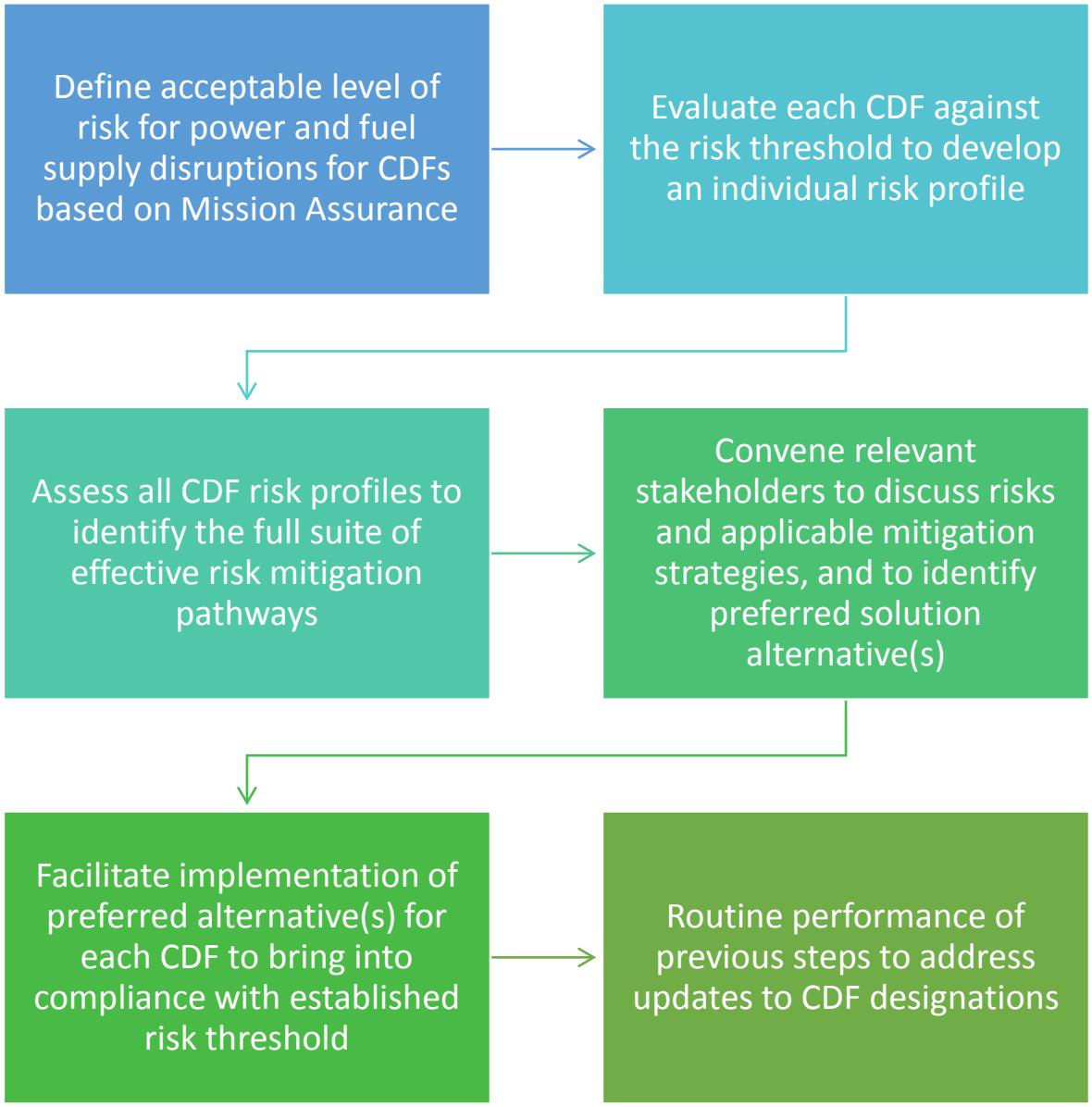
H. Support continued development of NAERM for DCEI program success.

I. Guide and support the development of DCEI investment assessment tools and methods
Beyond established reliability approaches and suitable for unpredictable but anticipated high-consequence resilience events.

DCEI Program Activity Highlights – Year 1

Activity	Anticipated Outputs	Program Pillars
Defense Community Partnerships	Through targeted technical assistance with well-defined outcomes and substantial involvement from DOE, demonstration of successful and repeatable approaches to facilitating the implementation of DCEI risk mitigation measures in selected locations/ communities, including stakeholder engagement and identifying funding for solution implementation.	1, 2, 3, 4
DCEI Investment Decision Support	Through the GMLC *Energy Assurance for Mission Assurance* project and in partnership with Dominion Energy, NRECA members 3 DoD installations and relevant stakeholders, development of quantifiable metrics that adequately reflect the consequences of grid disruptions to defense critical infrastructure.	1, 2, 3, 4
Analysis of Critical Infrastructure Dependencies	Identification of specific energy and other critical infrastructure dependencies strategically selected in partnership with CDF owners/operators, using mission disaggregation analyses and other methods.	1, 4
President's FY2021 budget request of $1.65M for DCEI program (proposed)	Establishment of line item DOE funding for DCEI program foundational technical analysis.	1, 4

Illustrative DCEI Risk Management Process



Leverage templated solutions where feasible for economies of scale, but recognize the need for unique or varied solution approaches based on mission, site environment, stakeholder considerations, etc.

Discussion

- To advance key partnerships for DCEI, how can DOE most effectively engage with stakeholders and partners including the electric utility industry as DCEI owners and operators?

- What are priorities and key approaches that may be needed for foundational program technical analysis, for example threat analyses, risk assessments, and the identification and evaluation of risk mitigation options?

- Any other insights or suggestions related to the read-ahead memo or this presentation?

Thank You

Jennifer DeCesaro
Director, Recovery & Resilience
Jennifer.DeCesaro@hq.doe.gov
202-586-1040

Johanna Zetterberg
DCEI Action Officer
Johanna.Zetterberg@hq.doe.gov
202-288-7414