

“Powering Through From Fragile Infrastructures to Community Resilience”

1



“Powering Through”

2

The United States is vulnerable to a long-term wide spread electric grid failure

- Weeks
- Months
- Years

Powering Through develops actions for everyone to be prepared for this vulnerability

Authors are 24 experts from across the county

Grid Security Events

3

- Accidents
- Insider Threats
- Physical Attacks
- Cyber Attacks*
- Solar Storms
- Directed Energy Weapons
- High Altitude Electromagnetic Pulse (HEMP)
- Combined-Arms Attacks

* FBI Director Wray, DHS Secretary Nielsen and ODNI Director Travers each said a cyber Attack was #1

Grid Length of Outage

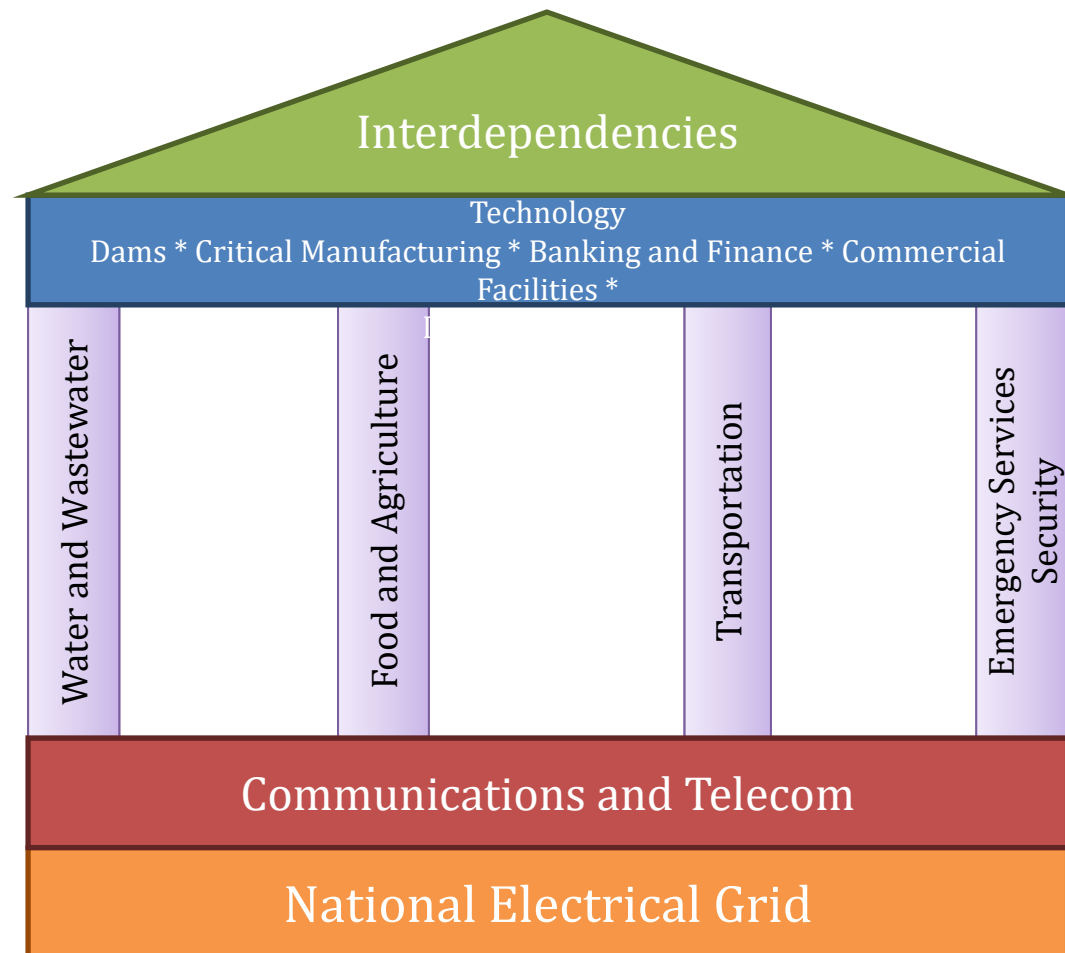
4

How long to replace

- Gas pipeline compressors
- Transformers
- Telecom switching
- Cellular base station electronics
- Industrial control systems
- Sensors

Interdependencies

5

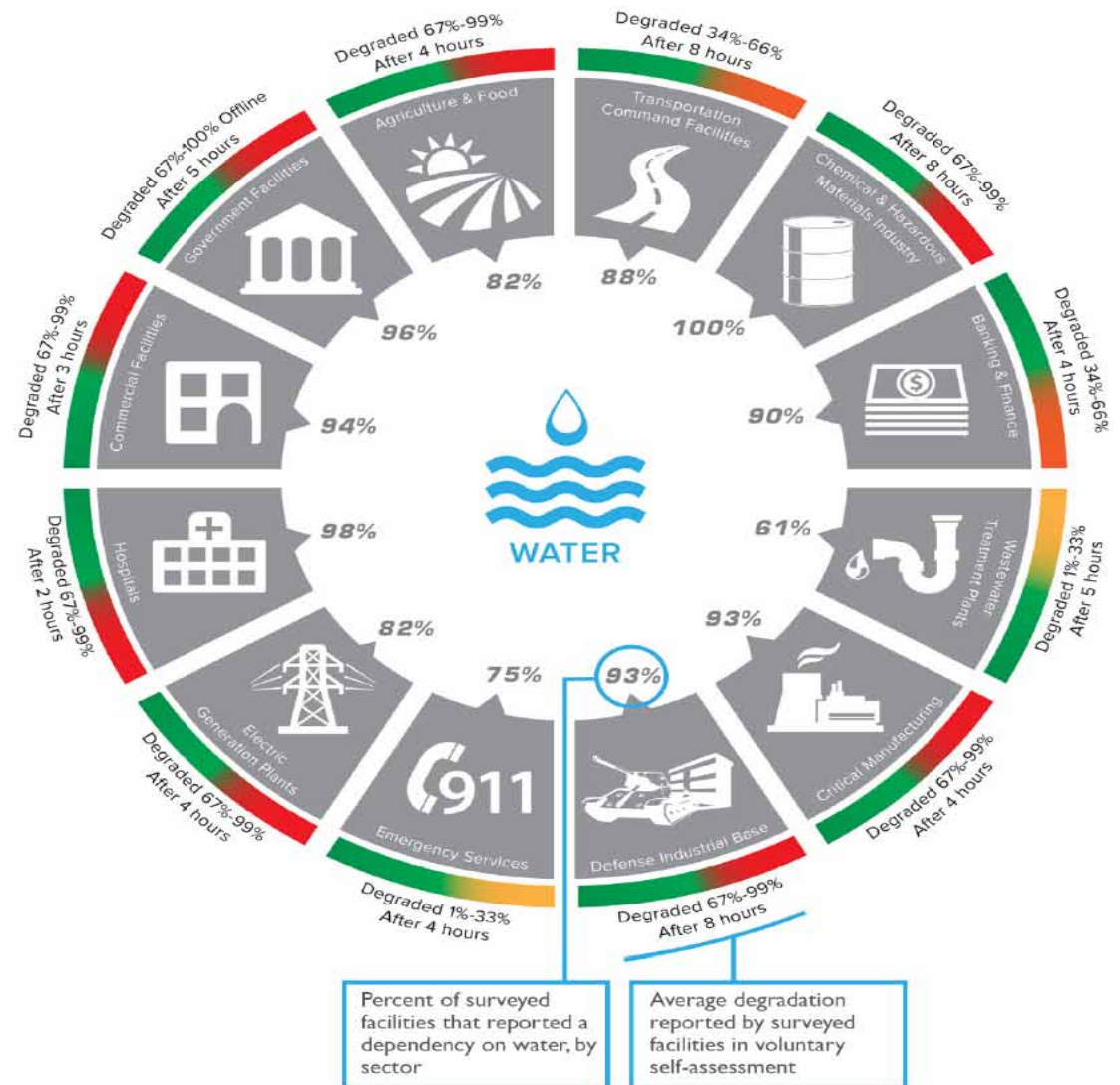


If NO Electrical Power...Water is an Issue

6

National Infrastructure Advisory Council (NIAC)

- Critical infrastructure dependence on water and potential function degradation following loss of water services
 - *Cascading impacts*
 - *Degradation timeline*



Powering Through Version 2.0

7

- Drawing upon InfraGard's 56,000+ member base with those experts in all the critical infrastructure
- Focus on Critical Infrastructure
 - Interdependencies
- Looked at three questions:
 - What happens if the electric power is out? – considering EMP as the worst case
 - How can that CI help the energy sector get the electric power restored?
 - What can be done now to be more prepared?

Authors

8

- Energy – Ed Goldberg
- Telecommunications – David Winks
- Water & Wastewater – Steve Bieber
- Food & Agriculture – Janet Thomas
- Transportation – Bruce Churchill
- IT Security – Dave Christensen
- Healthcare – Rich Krieg
- National Guard – Greg Hertz
- Emergency Management – Mary Lasky & Chuck Nettleship
- Chemical – Jim LeBlanc

Why Are We Concerned

9

Equipment at Risk	EMP (Nuclear)	Solar Storm	Cyber	Physical Attack	Radio Frequency Weapons	Pandemic	Major Earthquake
Transformers	R	R	R- Y	R	R- Y	Y	Y
Generator Stations	R	G	R	R	R	Y	Y
SCADA / Industrial Controls	R	R	R	R	R	Y	Y
Utility Control Centers	R	R	R	R	R	Y	Y
Telecommunications including cell phones	R	R	R	Y	Y	Y	Y
Radio Emergency Communications	R	P	Y	Y	Y	Y	Y
Emergency SATCOM Communications	R	P	Y	Y	Y	Y	Y
Internet	R	R	R	Y	Y	Y	Y
GPS	R	P	R	Y	Y	Y	Y
Transportation	R	Y	Y	Y	Y	Y	Y
Water	R	Y	R-Y	Y	Y	Y	Y
Financial Services	R	R	R	Y	Y	Y	Y
Agriculture	R - Y	Y	Y	Y	Y	Y	Y
Banking and Finance	R	R	R	Y	Y	Y	Y
Healthcare	R	Y	Y	Y	Y	Y	Y
Data Centers	R	Y	Y	Y	Y	Y	Y
Chemical	R	Y	Y	Y	Y	Y	Y

By Dr.
George Baker

RED –
permanent

YELLOW –
cascading

PINK –
temporary

GRAY –
uncertain

Being Prepared

10

- **Local**
 - Educate citizenry on preparedness strategies (30-day survivability)
 - Coordinate with States on local capability shortfalls
 - Community planning – (provision of resource and support outlets)
 - Communication plans
- **State**
 - Incentivize cities – resiliency programs (food/water/micro-grids)
 - Regional planning with adjacent States and Federal partners
 - Plan for National Guard as a State resource (determine roles / responsibilities)
- **Federal**
 - Strategic federal plan (prioritize legislative and protective initiatives)
 - Allocation of resource to meet strategic goals (preparedness grants)
 - National communications plan
 - Prioritization of long-term national recovery efforts

Critical Infrastructure

11

- Energy
 - Hardening the Grid – who pays?
 - Block grants, tax credits for resilience with new builds as the starting point with existing technologies
- Telecom
 - Improve RF shielding for amplification points on fiber optic cables; harden switching centers and cellular base stations; use aerostats and drones, hardening cyber and comms for 5G
- Water & Wastewater
 - Backup generators at more facilities
 - Onsite, hardened microgrids - use risk scenarios to help prioritize resiliency actions

Critical Infrastructure

12

- Food/AG

- Individuals need to take responsibility for basic food storage
- Communities need to work together to create sustainable food production
- Partner with public and private sector for sustainable food distribution warehouses

- Transportation

- Components: physical infrastructure (rail, highways, runways, e.g.), control systems, vehicles
- Control systems are the weak link
- High dependence on Communications Sector
- Regional planning crucial for resilient supply chains

Critical Infrastructure

13

- Healthcare & Public Health
 - On a widespread basis, exercise using grid down situations to train on how maximize hospital survivability
 - Ensure that the allocation of health facility resources follows “crisis standards of care” guidelines
 - As a state-level priority, ramp up local hospital contingency planning for both potable and non-potable water supply
- Chemical
 - Plan for alternate power supplies, raw materials storage, work with advisory boards on this scenario

Critical Infrastructure

14

IT Sector

- Industrial Control Systems (ICS)
 - ▣ Eliminate access directly to the ICS
 - ▣ Do not let personal devices have access to the ICS
 - ▣ Avoid using cloud for operational functions
- Data Centers
 - ▣ Require DR tests that include Cyber and GRID outage planning
 - ▣ Least impact areas do not get focus – Tier1 systems get priority
- Internet of Things (IOT)
 - ▣ Managed security updates for Device Operating Systems or not allowed on network
 - ▣ Forced password change on admin setup should be required
 - ▣ Fail off state should be built in if too much traffic comes from device (flood condition)

Critical Infrastructure

15

National Guard

- Coordinate with State for roles and responsibilities
- Ensure installation resiliency
- Participate in federal pilot programs
- Conduct routine communications exercises (primary, secondary, and tertiary with State and Federal partners)

Emergency Management

- Develop post messages now that can be revised for actual situation, with community set priorities
- Local and regional planning

FEMA National Business Emergency Operations Center

NBEOC

- Coordinates/facilitates states with private sector and industry trade associations
- Increase integration with FEMA, DHS and States through planning and future exercise efforts
- Increase private sector plan integration with State private sector liaisons
- Strengthen Regional and State partnerships and participation in Community Lifeline resilience

Public-Private Sector liaisons:

- Maintain situational awareness of the restoration
- More than 80% of the energy critical infrastructure is owned by the private sector.
- National Business Emergency Operations Center and States with Business EOCs
- Crowdsourcing
- Economic Dashboards

FEMA re-establishing ESF #14 Cross-Sector Coordination

What Private Sector Can Do

Build Upon Partnership Efforts

- Become involved in sector-specific and information sharing partnerships (InfraGard, ISACs, ISAOs, state-local coalitions)
- Establish relationships with NBEOC/State EOC, local partners - emergency management
- Participate in training and exercises; attend webinars, conference calls, cross-sector events and listening sessions.

Innovate in Managing Risk

- Incorporate security and resilience into the design and upkeep of critical infrastructure
- Help develop analysis to better understand risks
- Adopt the Cybersecurity and Critical Infrastructure Frameworks thru DHS CISA state Protective Security Advisors (PSA)

Focus on Outcomes

- Identify shared goals, define success and document effective practices.
- Build security and resilience considerations into cost-benefit analysis to understand return on investment
- Business Continuity of Operations - develop, share and incorporate best practices