“Powering Through

From Fragile Infrastructures to Community Resilience”

* InfraGard Convention 2018

“Powering Through”

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

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

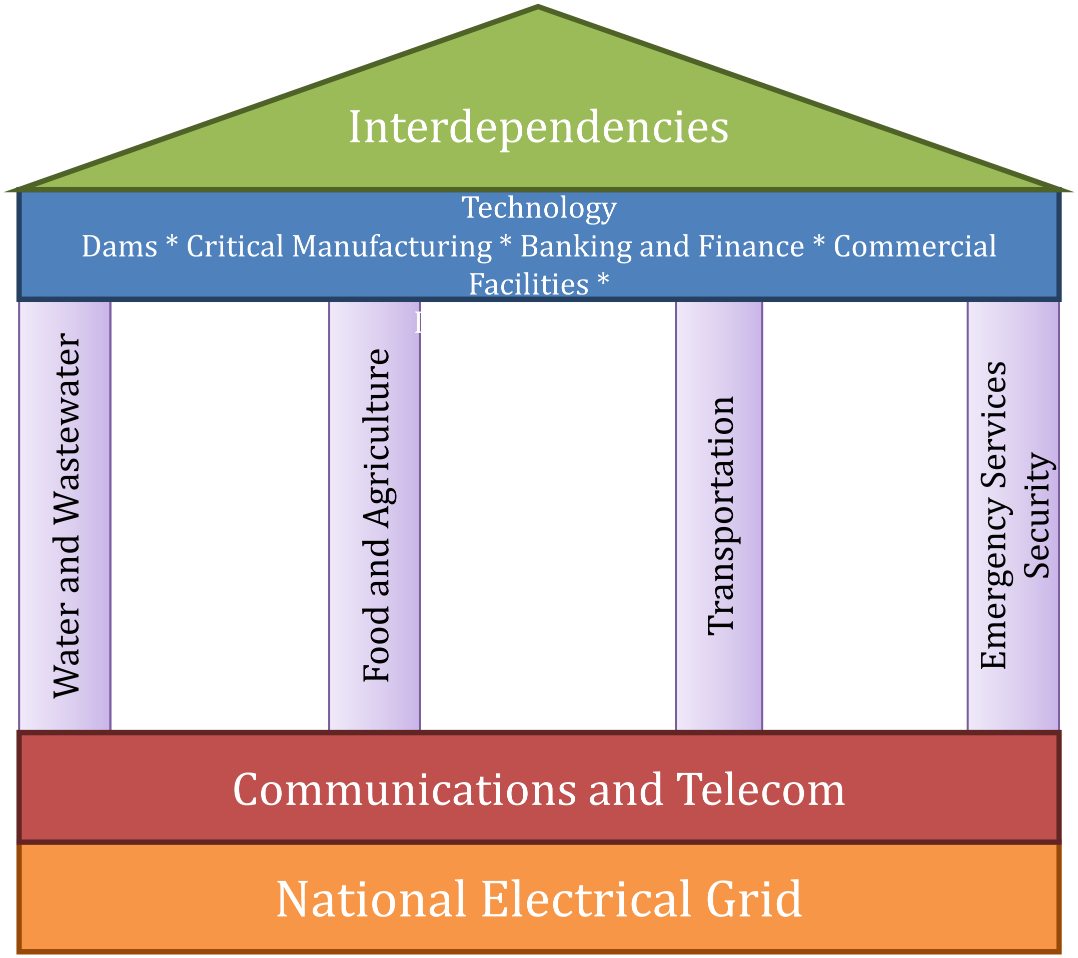
*** FBI Director Wray, DHS Secretary Nielsen and ODNI Director Travers each said a cyber Attack was #1**

Grid Length of Outage

How long to replace ……

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

Interdependencies



Interdependencies

Technology
Dams * Critical Manufacturing * Banking and Finance * Commercial Facilities *

Water and Wastewater

Food and Agriculture

Transportation

Emergency Services
Security

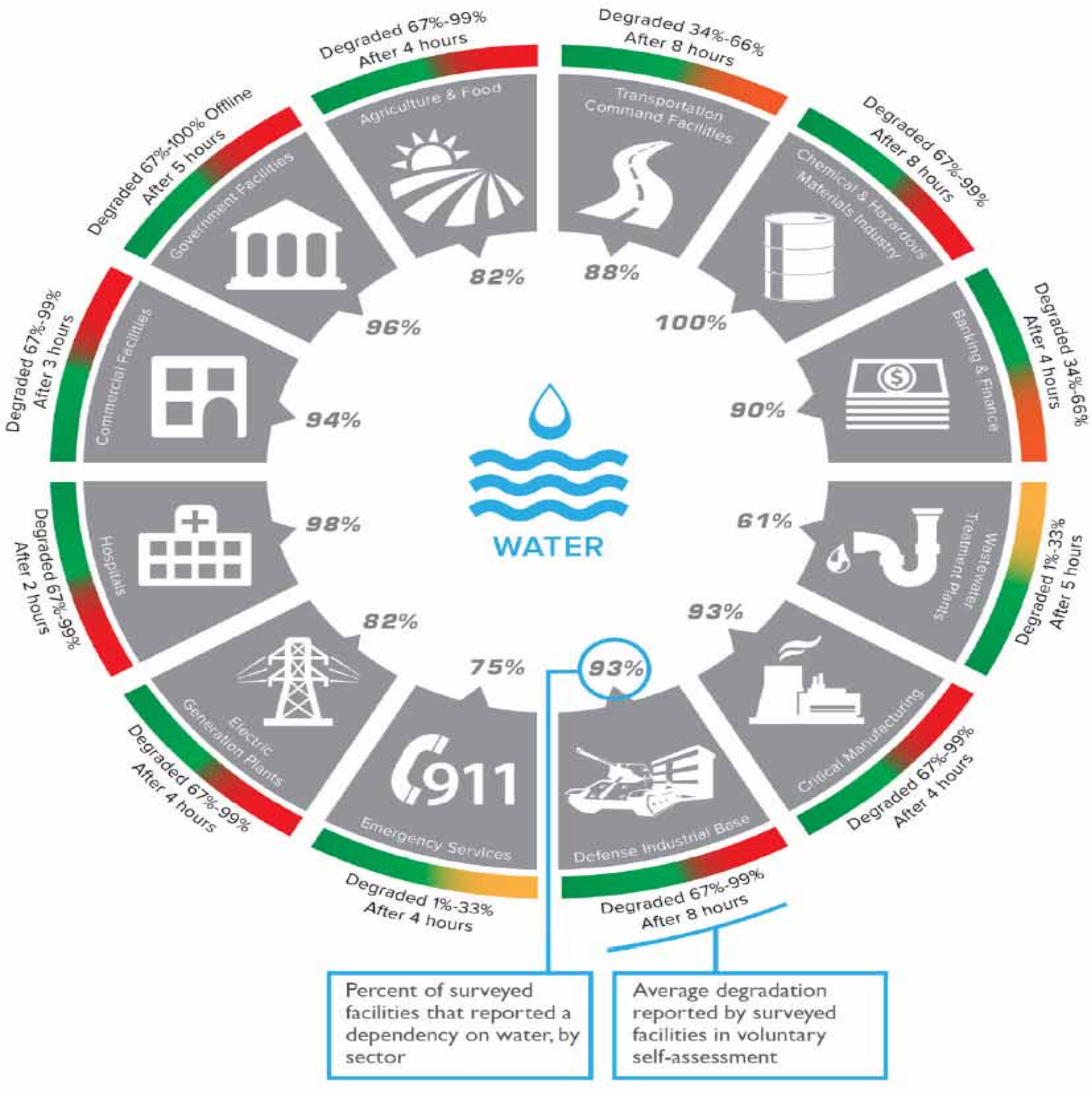
Communications and Telecom

National Electrical Grid

If NO Electrical Power…Water is an Issue

National Infrastructure Advisory Council (NIAC)

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


Degraded 67%-99% After 4 hours
Agriculture & Food
82%
Degraded 34%-66% After 8 hours
Transportation Command Facilities
88%
Degraded 67%-99% After 8 hours
Chemical & Hazardous Materials Industry
100%
Degraded 34%-66% After 4 hours
Banking & Finance
90%
Degraded 1%-33% After 5 hours
Wastewater Treatment Plants
61%
Degraded 67%-99% After 4 hours
Critical Manufacturing
93%
Degraded 67%-99% After 8 hours
Defense Industrial Base
93%
Degraded 1%-33% After 4 hours
Emergency Services
911
75%
Degraded 67%-99% After 4 hours
Electric Generation Plants
82%
Degraded 67%-99% After 2 hours
Hospitals
98%
Degraded 67%-99% After 3 hours
Commercial Facilities
94%
Degraded 67%-100% Offline After 5 hours
Government Facilities
96%
WATER

Percent of surveyed facilities that reported a dependency on water, by sector

Average degradation reported by surveyed facilities in voluntary self-assessment

Powering Through Version 2.0

- Drawing upon InfraGard's 58,000+ 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

- 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

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

By Dr. George Baker

RED – permanent

YELLOW – cascading

PINK – temporary

GRAY – uncertain

Being Prepared

- Local
  - Educate citizenry on preparedness (30-day survivability)
  - Coordinate with States on local shortfalls
  - Community planning
  - Communication plans
- State
  - Incentivize cities – resiliency (food/water/microgrids)
  - Regional planning
  - Plan for National Guard as a State resource
- Federal
  - Strategic federal plan
  - Allocation of resource to meet goals
  - National communications plan
  - Prioritization of long-term national recovery efforts

Critical Infrastructure

- Energy
  - Hardening the Grid – who pays?
  - Block grants, tax credits for resilience with new builds as the starting point
- 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

- Food/AG
  - Individuals take responsibility for basic food storage
  - Communities 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

- Healthcare & Public Health
  - Exercise using grid down situations to train on how maximize hospital survivability
  - Ensure "crisis standards of care" guidelines
  - 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 grid down scenario

Critical Infrastructure

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 tests that include Cyber and GRID outage planning
  - 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
  - Fail off state for denial of service emergencies

Critical Infrastructure

National Guard

- Coordinate with State for roles and responsibilities
- Ensure installation resiliency
- Participate in federal pilot programs
- Conduct routine communications exercises

- Emergency Management
  - Develop post messages now with community
  - Local and regional planning

FEMA National Business Emergency Operations Center

More than 80% of the energy critical infrastructure is owned by the private sector.

FEMA re-establishing ESF #14 Cross-Sector Coordination

NBEOC

- Coordinates with private sector
- Plan with FEMA, DHS and States
- Conduct exercise
- Increase private sector plan integration with State private sector liaisons
- Strengthen Regional and State partnerships

Public-Private Sector liaisons:

- Provide situational awareness
- Private sector provides information to Business EOCs
- Create Business EOCs at local, State, Regional, and National level.

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