FDA-NCVHS: CURRENT ISSUES IN CYBER SECURITY

L, Reuven Pasternak, MD, MPH, MBA
Senior Advisor, National Risk Management Center
U.S. Department of Homeland Security

July 20, 2022

reuven.pasternak@cisa.dhs.gov

Critical Infrastructure Sector Construct

CHEMICAL	DHS (CISA)
COMMERCIAL FACILITIES	DHS (CISA)
COMMUNICATIONS	DHS (CISA)
CRITICAL MANUFACTURING	DHS (CISA)
DAMS	DHS (CISA)
DEFENSE INDUSTRIAL BASE	DOD
EMERGENCY SERVICES	DHS (CISA)
ENERGY	DOE
FINANCIAL	Treasury
FOOD & AGRICULTURE	USDA & HHS
GOVERNMENT FACILITIES	GSA & DHS (FPS)
HEALTHCARE & PUBLIC HEALTH	HHS
INFORMATION TECHNOLOGY	DHS (CISA)
NUCLEAR REACTORS, MATERIALS AND WASTE	DHS (CISA)
TRANSPORTATIONS SYSTEMS	DOT (TSA & USCG)
WATER	EPA

National Critical Functions Set

CONNECT

- Operate Core Network
- Provide Cable Access Network Services
- Provide Internet Based Content, Information, and Communication Services
- Provide Internet Routing, Access and Connection Services
- Provide Positioning, Navigation, and Timing Services
- Provide Radio Broadcast Access Network Services
- Provide Satellite Access Network Services
- Provide Wireless Access Network Services
- Provide Wireline Access Network Services

DISTRIBUTE

- Distribute Electricity
- Maintain Supply Chains
- Transmit Electricity
- Transport Cargo and Passengers by Air
- Transport Cargo and Passengers by Rail
- Transport Cargo and Passengers by Road
- Transport Cargo and Passengers by Vessel
- Transport Materials by Pipeline
- Transport Passengers by Mass Transit

MANAGE

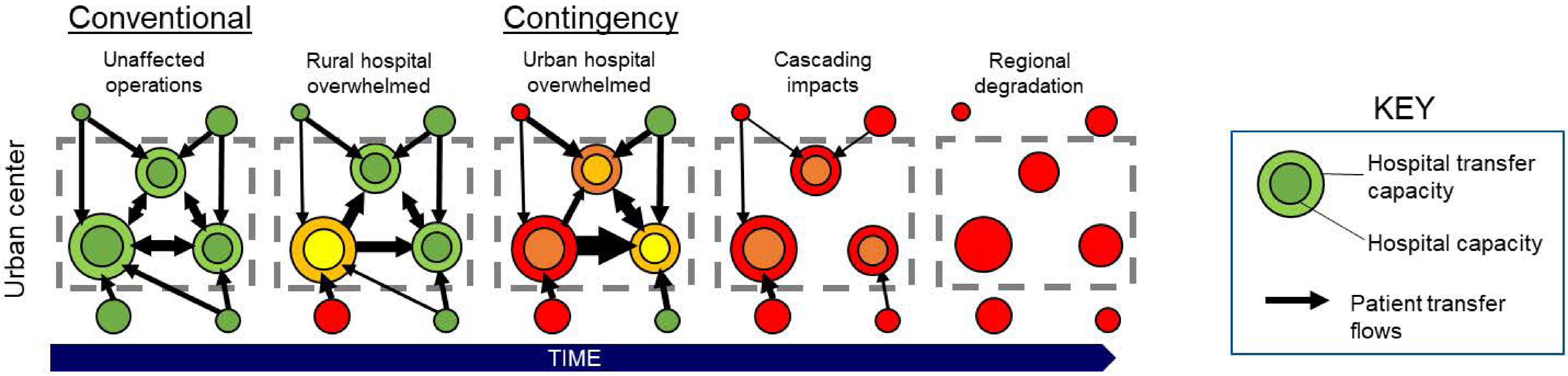
- Conduct Elections
- Develop and Maintain Public Works and Services
- Educate and Train
- Enforce Law
- Maintain Access to Medical Records
- Manage Hazardous Materials
- Manage Wastewater
- Operate Government
- Perform Cyber Incident Management Capabilities
- Prepare For and Manage Emergencies
- Preserve Constitutional Rights
- Protect Sensitive Information
- Provide and Maintain Infrastructure
- Provide Capital Markets and Investment Activities
- Provide Consumer and Commercial Banking Services
- Provide Funding and Liquidity Services
- Provide Identity Management and Associated Trust Support Services
- Provide Insurance Services
- Provide Medical Care
- Provide Payment, Clearing, and Settlement Services
- Provide Public Safety
- Provide Wholesale Funding
- Store Fuel and Maintain Reserves
- Support Community Health

SUPPLY

- Exploration and Extraction Of Fuels
- Fuel Refining and Processing Fuels
- Generate Electricity
- Manufacture Equipment
- Produce and Provide Agricultural Products and Services
- Produce and Provide Human and Animal Food Products and Services
- Produce Chemicals
- Provide Metals and Materials
- Provide Housing
- Provide Information Technology Products and Services
- Provide Materiel and Operational Support to Defense
- Research and Development
- Supply Water

- **It's less about who you are and more about the functions you produce or enable.**
- **NCFs better capture cross-cutting risks and associated dependencies.**

Cascading Impact of Disruption(s)



Courtesy: CISA Covid-19 Pandemic Task Force

Level	Level	Sample Indicators	Disruptive Event(s)
1	• Normal Operations: provision of all routine clinical, support and administrative services. • Meeting routine, anticipated demand while maintaining service standards. • Able to accommodate additional demand with existing resources. ***(Meeting Need, High Resiliency)***	• Beds: <85% occupancy • Staff: hired to >95% of need, absentee rate <5% • All diagnostic, procedure, care areas with full capacity, immediately available resources • 120 days cash on hand • Physical plant without major deficit; preventive maintenance on schedule • Digital platform secured • No regional facilities or region overall under stress	**Resource** • Staff/Supplies/Equipment: inadequate supply or ability to meet expanded needs. • Financial challenge • Supplemental supply or service disruption (fuel, other energy, laundry, administrative services, other NCF disruption) **Cyber** • Ransomware\Sabotage • Technical Dysfunction **Sudden Increase in Acute Demand** • Infectious disease • Mass casualty • Chemical, biologic, radiation • Other HDO, regional stress **Environmental Event** • Hurricane • Tornado • Snow • Flood • Earthquake **Infrastructure** • Loss of power • Structural failure • Compromise of associated support functions
2	• Meeting enhanced demand while maintaining service standards. • Limited ability to absorb additional demand in all or parts of the system. ***(Meeting Need, Low Resiliency)***	• Minor delays for some clinical, administrative or support services. • Staff, facilities working at or near capacity.	
3	• Meeting service needs and standards in most but not all clinical, support and administrative areas. • Unable to absorb additional demand in all or parts of the system without expansion of resources or reduction of service availability. ***(Unable to meet all Need, No Resiliency)***	• Extended boarding of patients awaiting placement in alternative settings (e.g., ED). • Significant delays in services despite operating at capacity. • Cancellation and/or diversion of patients for elective care or urgent specialized care. • Reduction of service in a therapeutic or diagnostic area despite a demand for that service. • Staffing at ratios lower than routine to meet standards of service.	
4	• Unable to meet standard of service in most areas and/or in specialty units. • Unable to meet current demand without expansion of resources or reduction of service. • ***(Unable to meet all Need, No Resiliency)***	• Use of ED and other overflow areas to manage inpatients. • Cancellation of scheduled care and delay of urgent care. • Diversion of patients with urgent or specialized needs to other facilities. • Closure of major service, clinical, diagnostic unit.	
5	• Facility or system unable to provide care, requiring immediate transfer of patients to other locations and diversion of all services to other facilities. ***(Unit Fail, Unable to Provide Service)***	• Unable to provide service due to compromise of infrastructure and\or necessary support systems.	

Competing for Attention

- Finances
- Facilities
- Staffing
- Supply Chain
- Quality\Safety
- Fragmentation of System
- Digital Platform\Cyber Security