IMPACT OF CYBER ATTACKS AND PANDEMIC ON HEALTH CARE

NATIONAL COMMMITTEE ON VITAL AND HEALTH STATISTICS (NCVHS)

JANUARY 25, 2022

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American people.

MISSION

CISA partners with industry and government to understand and manage risk to our Nation's critical infrastructure.

OVERALL GOALS

GOAL 1

DEFEND TODAY

Defend against urgent threats and hazards

seconds | days | weeks

GOAL 2

SECURE TOMORROW

Strengthen critical infrastructure and address long-term risks

months | years | decades

We are the Nation's Risk Advisor

The Cybersecurity and Infrastructure Security Agency (CISA) is the pinnacle of national risk management for cyber and physical infrastructure.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

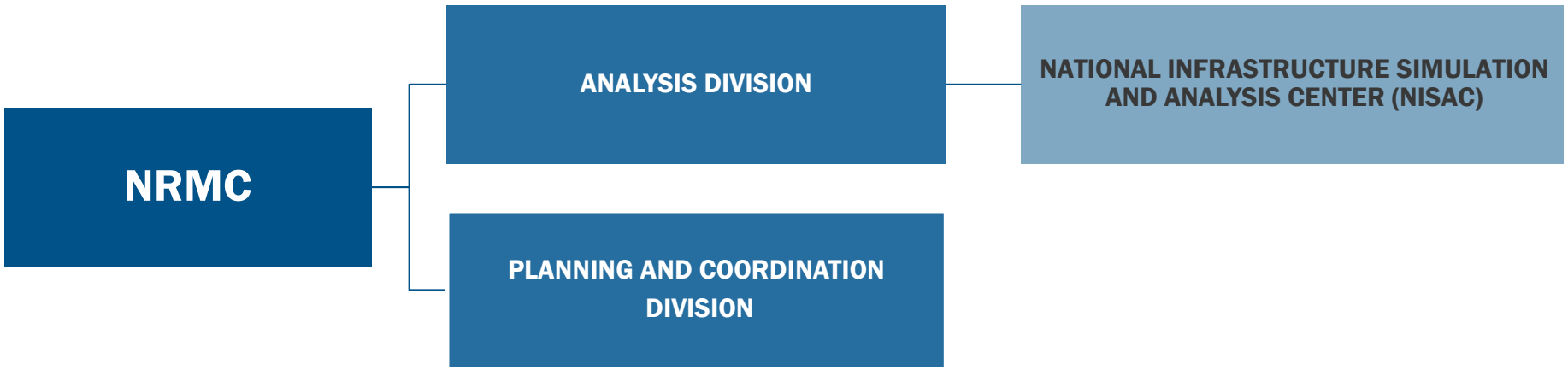
National Risk Management Center

The NRMC is a planning, analysis, and collaboration center. CISA coordinates with the critical infrastructure community to identify; analyze; prioritize; and manage risks to National Critical Functions, which are vital to the United States.

MISSION PRIORITIES:

- Analyzes most strategic risks to our Nation's critical infrastructure
- Leads public/private partnership initiatives to manage priority areas of national risk
- Collaborates with the private sector and other stakeholders to better understand future threats.

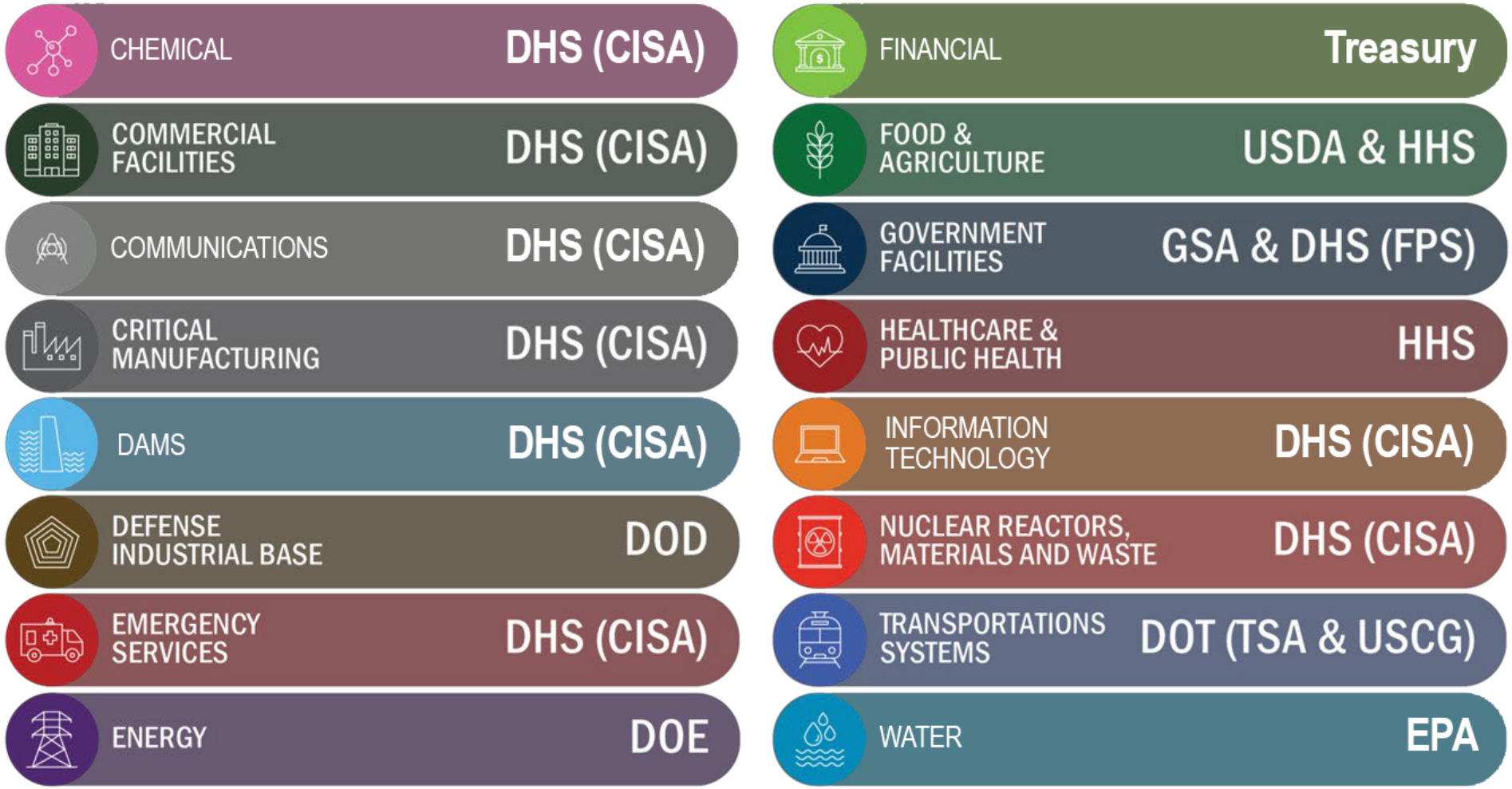
National Risk Management Center



The **ANALYSIS DIVISION** performs risk assessments, modeling, and data management and visualization to understand cross-cutting critical infrastructure risks.

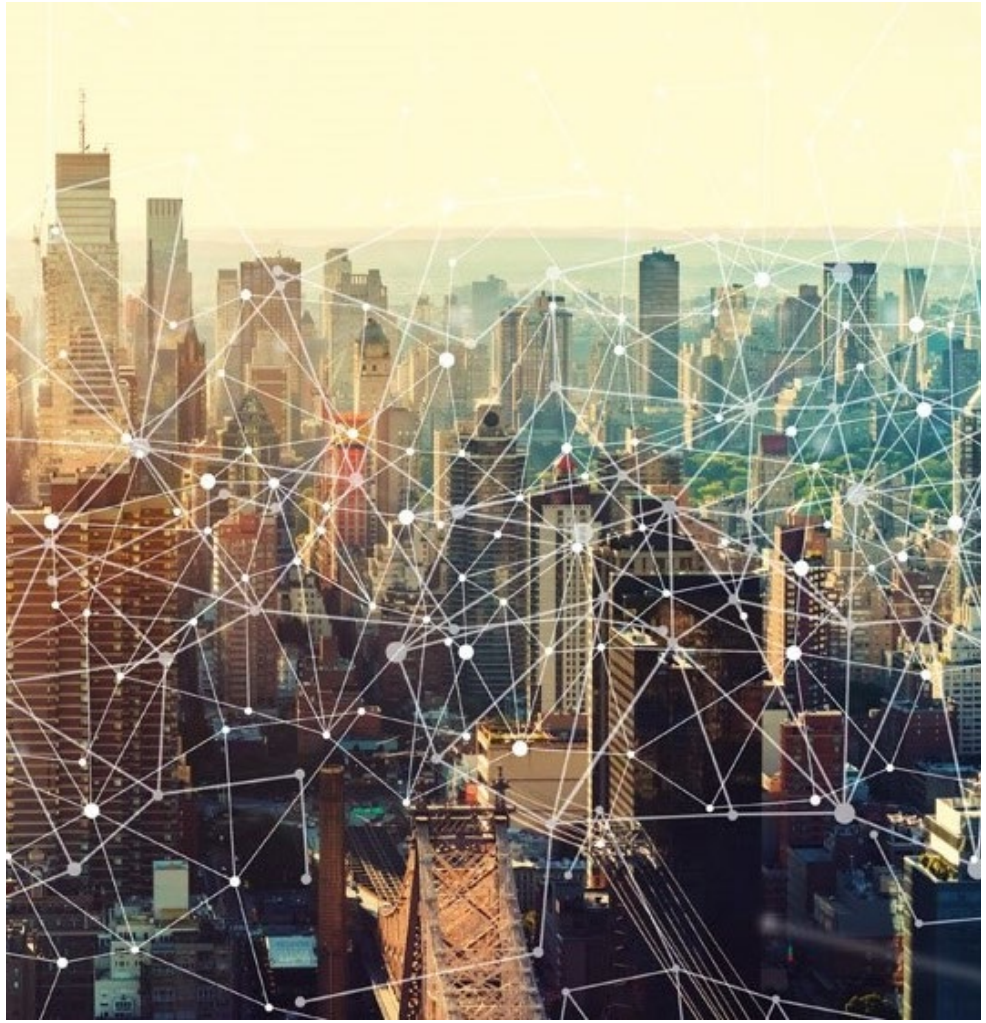
The **PLANNING AND COORDINATION DIVISION** actively engages with stakeholders to better understand critical infrastructure operations and manages some of CISA's top risk management initiatives (e.g., ICT Supply Chain and Pipeline Cybersecurity).

Critical Infrastructure Sector Construct



55 National Critical Functions

The NCFs are the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.



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

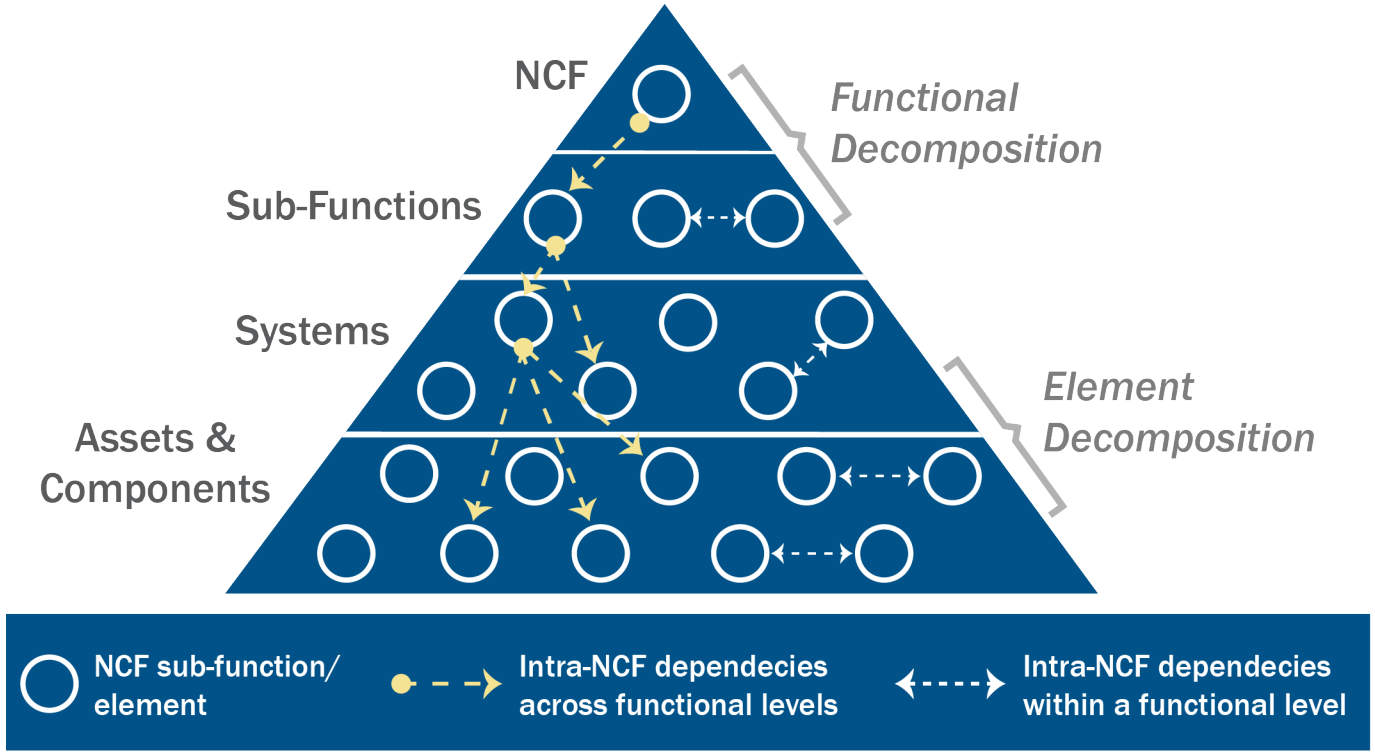
- Conduct Elections
- Develop and Maintain Public Works and Services
- Educate and Train
- Enforce Law
- Maintain Access to Medical Records
- Manage Hazardous Materials
- Manage Wastewater
- Operate Government
- Perform Cyber Incident Management Capabilities
- Prepare For and Manage Emergencies
- Preserve 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.

NCF Framework



The NCF Framework recognizes that critical infrastructure is increasingly cross-sector, and that a siloed approach is no longer sufficient to manage risk, particularly around cyber risks. It focuses on the key assets, systems, and networks that support the NCFs, as well as the critical technologies and dependencies that enable them.

National Critical Functions in Action – COVID-19

Highest Risk NCFs					
NATIONAL CRITICAL FUNCTION	Risk Drivers				
	1	2	3	4	5
NCF 1	High	High	High	Med	High
NCF 2	High	High	High	High	Med
NCF 3	High	High	High	Low	Med
NCF 4	High	High	Low	High	High
NCF 5	High	High	High	Low	Low
NCF 6	Med	Med	Low	Med	Med
NCF 7	Low	Med	High	Low	High
NCF 8	Low	Med	High	Low	High
NCF 9	Low	Med	High	Low	High

(U) Assessment Results Updated 7/30/2020

(U) The NCF judgments are updated on a weekly basis on Wednesdays as new information, insight, and data become available.

(U) Each NCF is assessed against a framework of High, Medium, and Low Risk against five drivers over the time horizon of the next 60 days.

(U) Risk Drivers				
Driver 1 *Commodity Shortage*	**Driver 2** *Shortage of Workers*	**Driver 3** *Increase in Demand*	**Driver 4** *Decrease in Demand*	**Driver 5** *Change in Other Function(s)*

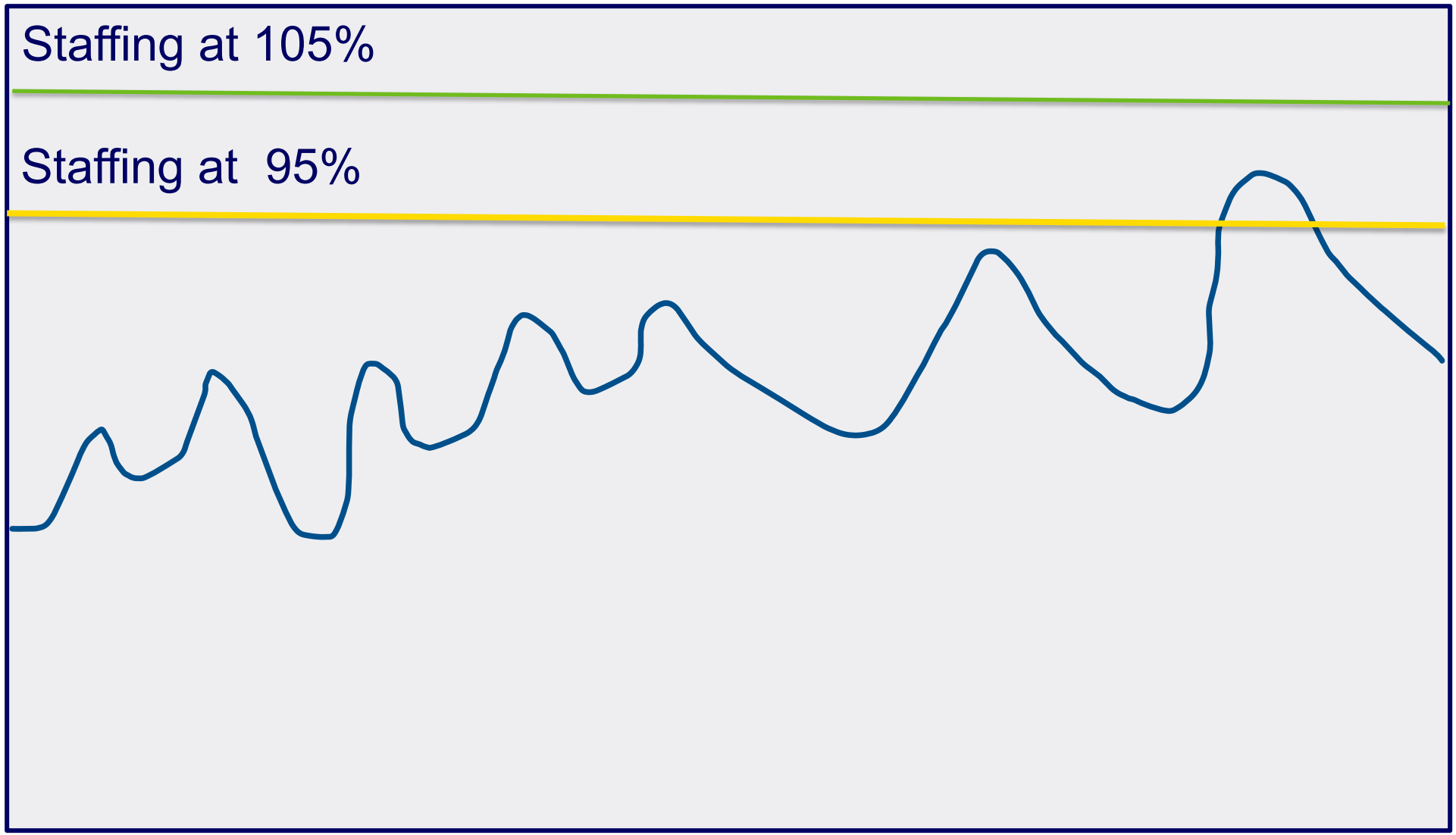
Areas of Emerging Risk					
NATIONAL CRITICAL FUNCTION	Risk Drivers				
	1	2	3	4	5
NCF 1	Low	High	Med	Med	Med
NCF 2	Med	High	Med	Med	Low
NCF 3	Med	High	Med	Med	Low
NCF 4	Low	Low	Low	Med	Low

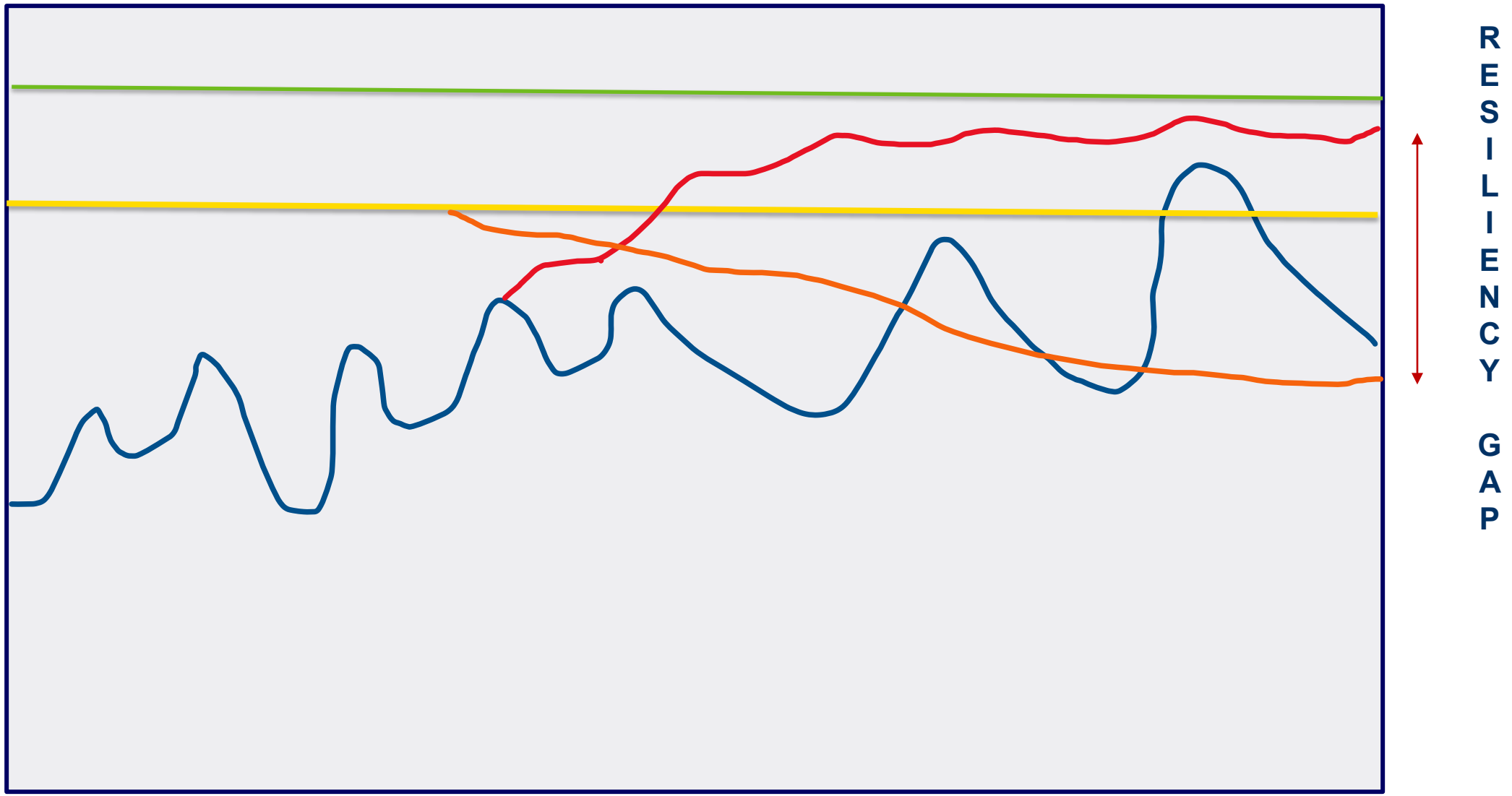
(U) Driver Scale	
Low	A low chance of national scale disruption or degradation at any point in time over the period of study occurring as a result of the identified driver (Roughly measured as a 0-10% chance of occurrence)
Medium	A moderate chance of national scale disruption or degradation at any point in time over the period of study occurring as a result of the identified driver (Roughly measured as a 11-25% chance of occurrence)
High	Greater than a moderate chance of national scale disruption or degradation at any point in time over the period of study occurring as a result of the identified driver (Roughly measured as greater than a 25% chance of occurrence)

Unique Challenge of Health Sector

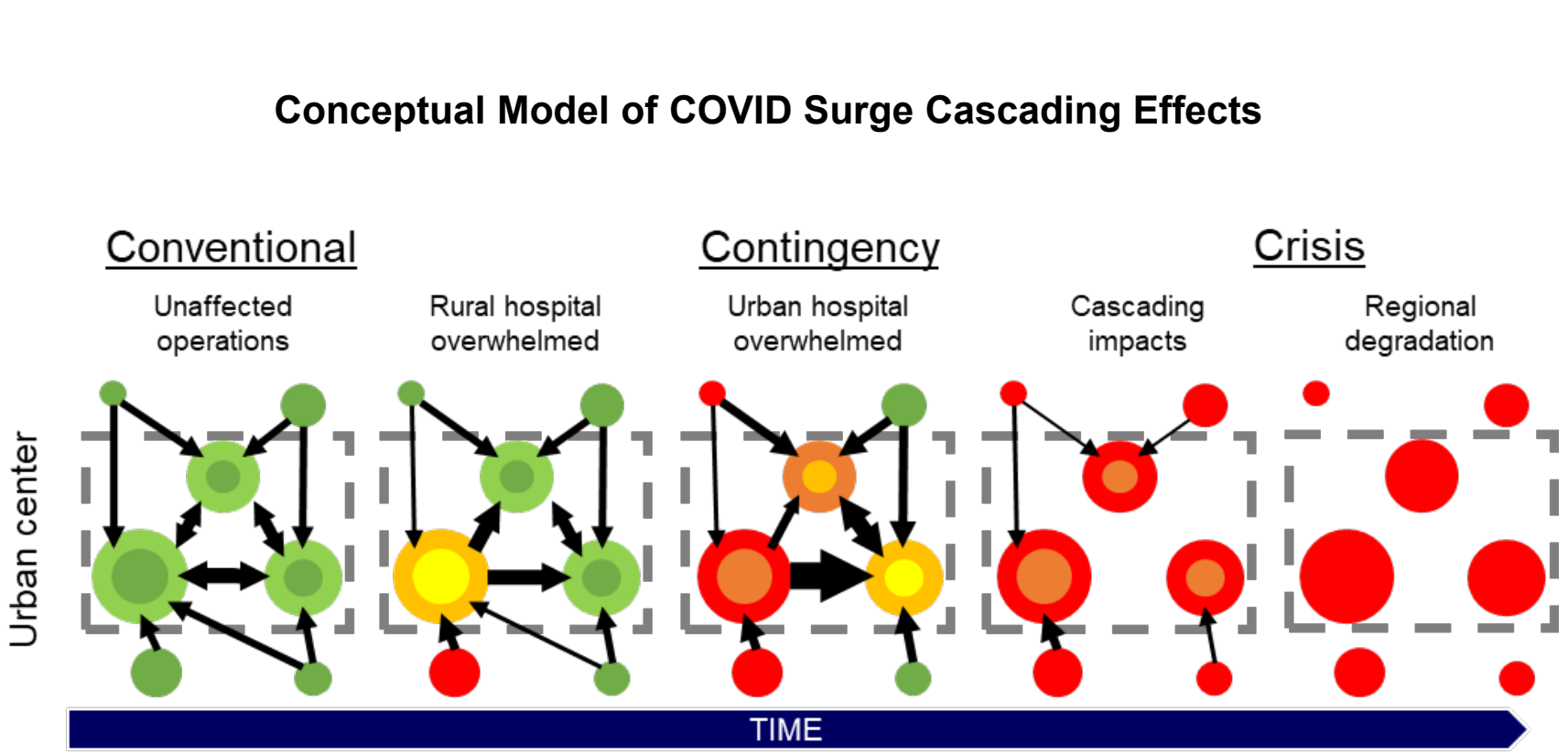
- 18 % of GDP
- Impact:
  - Immediate
  - Pervasive
  - Profound
- Fragmented
  - Public\Private
  - Jurisdictions
- High degree of restructure, increasing complexity

Data reporting overload (?)

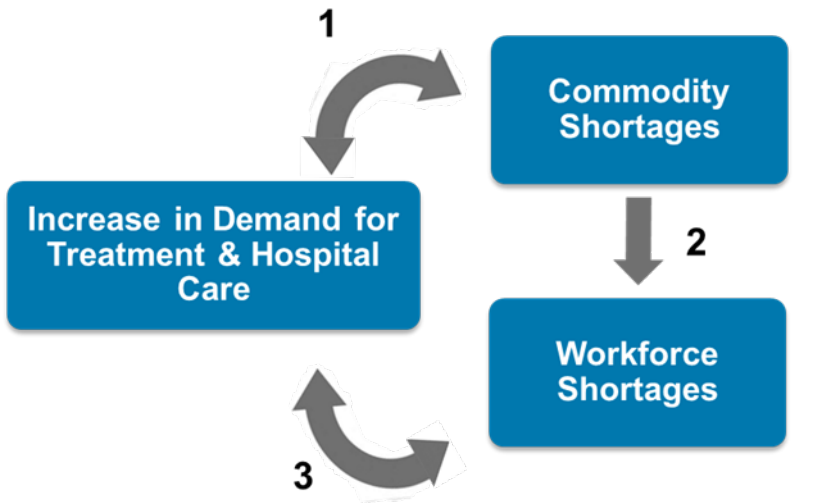

Staffing at 105%
Staffing at 95%
Volume
Time


Volume
Time
RESILIENCY GAP

COVID-19 Surge Effects



Functional Dynamics of COVID-19 Surges



Mutually Reinforcing Dynamics Further Strain *Provide Medical Care* NCF

This graphic is UNCLASSIFIED. Source: CISA

Standard of Care Continuum

Incident demand/resource imbalance increases →
Risk of morbidity/mortality to patient increases →
← Recovery

	Conventional	Contingency	Crisis
Space	Usual patient care space fully utilized	Patient care areas re-purposed (PACU, monitored units for ICU-level care)	Facility damaged/unsafe or non-patient care areas (classrooms, etc.) used for patient care
Staff	Usual staff called in and utilized	Staff extension (brief deferrals of non-emergent service, supervision of broader group of patients, change in responsibilities, documentation, etc.)	Trained staff unavailable or unable to adequately care for volume of patients even with extension techniques
Supplies	Cached and usual supplies used	Conservation, adaptation, and substitution of supplies with occasional re-use of select supplies	Critical supplies lacking, possible reallocation of life-sustaining resources
Standard of care	Usual care	Functionally equivalent care	Crisis standards of care[a]

Normal Operating Conditions

Indicators: Potential for contingency care

Indicators: Potential for CSC

Extreme Operating Conditions

Trigger(s): Decision point for contingency care

Trigger(s): Decision point for CSC

The graphic above is UNCLASSIFIED. Source: National Academy

Disruptive Event Level System

Level	Level	Sample Indicators	Disruptive Event(s)
1	• Normal Operations: provision of all routine therapeutic, diagnostic, and administrative services • Meeting routine standards of service without delays. • Able to accommodate additional demand with existing resources.	• 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 standards of service • Limited ability to absorb additional demand in all or parts of the system.	• 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.	• 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.	• 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.	• Unable to provide service due to compromise of infrastructure and\or necessary support systems.	

For more information:
www.cisa.gov

Questions?
Email:
reuven.pasternak@cisa.dhs.gov
Phone:
(202) 834-1630


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY