

# NASEM HPH CIP Workshop

## **Session 3 Examining High Priority Vulnerabilities and Strategies for Resilience: Built Environment, Water and Wastewater, Energy**

*Monday, December 9, 2024*

*Joshua Corman - @joshcorman  
IST - The Institute for Security and Technology  
Undisruptable27.org*



# ABOUT IST: *The Critical Action Think Tank*

IST unites technology and policy leaders to create actionable solutions for emerging security threats.

A banner with a blurred background of people and a smartphone in the foreground displaying a cityscape. The text "Geopolitics of Technology" is overlaid in white.

## Geopolitics of Technology

Emerging technologies can disrupt the international balance of power. As governments compete, they shape innovation, supply chains, prosperity, and national and international security. IST shapes the incentives and alleviates the impediments to a more secure collective future.

[Strategic Balancing Initiative](#)

A banner with a blurred background of people walking in a city. The text "Future of Digital Security" is overlaid in white.

## Future of Digital Security

Dependence on digital technologies generates systemic security risks. IST works to identify incentives and mitigate digital security market failures by proposing ways to build trust, safety, and security into digital technologies from the ground up and sustain them for the future.

[The Ransomware Task Force](#)  
[Applied Trust & Safety](#)  
[AI Foundation Model Access Initiative](#)

A banner with a dark purple background and a glowing arc of light. The text "Innovation and Catastrophic Risk" is overlaid in white.

## Innovation and Catastrophic Risk

Despite optimism about new technologies, some exacerbate or create existential threats to society. IST searches for solutions to the more severe risks introduced by technology, and strives to make technology itself a solution.

[CATALINK](#)  
[Nuclear Risk Reduction](#)



# I AM THE Cavalry

I Am The Cavalry is a grassroots organization focused on the intersection of digital security, public safety, and human life.

THE

Safer. Sooner. Together.

[iamthecavalry.org/about](https://iamthecavalry.org/about)





[CyberMedSummit.org](https://CyberMedSummit.org)

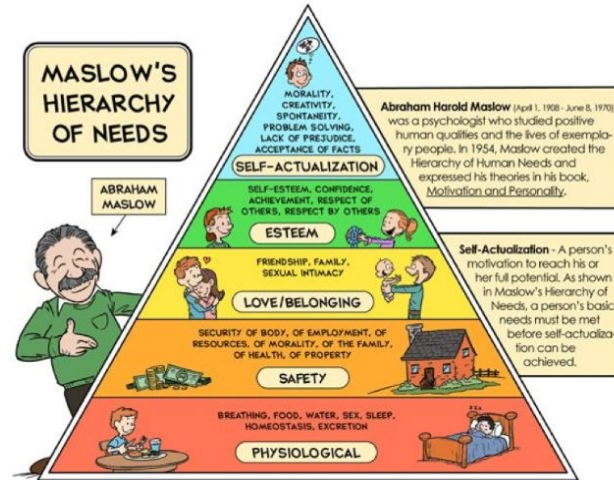


## Working Title: UnDisruptable27

Driving More Resilient Lifeline Critical Infrastructure for Our Communities

[UnDisruptable27.org](https://UnDisruptable27.org)

Through our **over dependence** on **undependable IT** , we have created the conditions such that the actions **any single outlier** can have a profound and asymmetric impact on **human life, economic, and national security** .



www.tlmvandevall.com | Copyright © 2013 Dutch Renaissance Press LLC.





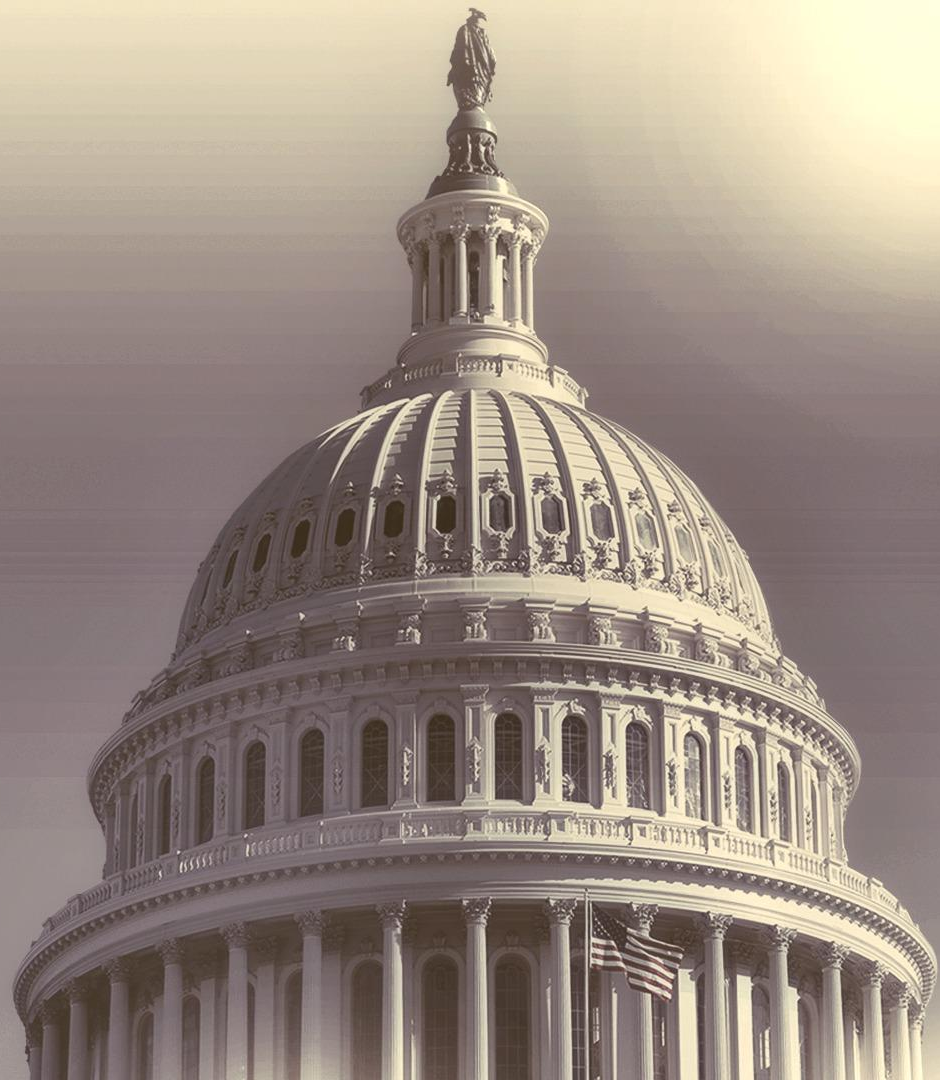












## *Patients of a Vermont Hospital Are Left 'in the Dark' After a Cyberattack*

A wave of damaging attacks on hospitals upended the lives of patients with cancer and other ailments. "I have no idea what to do," one said.



The University of Vermont Medical Center in Burlington, Vt., was the victim of a cyberattack in late October. Elizabeth Frantz for The New York Times



By Ellen Barry and Nicole Perlroth













1



2



3



4



IT Security



Supply Chain



OT Security



Insider Threat



Physical Security



Interoperable Communications

# CISA INSIGHTS



DEFEND TODAY.  
SECURE TOMORROW

## ***Provide Medical Care is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm***

*September 2021*

### **CRITICAL INFRASTRUCTURE DECISION SUPPORT**

As the COVID-19 pandemic reaches another phase, with increased and protracted strains on the nation's critical infrastructure and related National Critical Functions such as *Provide Medical Care*, CISA is undertaking a renewed push for cyber preparedness and resilience, as well as decision support for stakeholders within critical infrastructure sectors. Over time, we find these original insights increasingly valuable, and in service of timely decision support, we offer them to you in their original form. As British statistician George E. P. Box noted, "All models are wrong, but some are useful." We hope that these models and insights are useful to you and stimulate additional discussion and exploration for mutual benefit.

By late September, at least four states have declared Crisis Standards of Care (CSC), and an additional eight have delayed elective surgeries and/or are at risk of enacting CSC. Patient diversions across state lines further punctuate the dynamic we outlined in the Cascading failures model (see page 7).

This CISA Insight will speak to:

- Analysis and insights into strains on the nation's critical infrastructure, specifically through impacts to the National Critical Function *Provide Medical Care*,
- The compounding risks and harms that apply to all critical infrastructure sectors and the 55 National Critical Functions, through impact to essential critical infrastructure workers, and
- Our intention to share our preliminary analysis, enable decision support, and assist in risk reduction across multiple stakeholders and critical infrastructure sectors.

## Impact of Hospital Strain on Excess Deaths During the COVID-19 Pandemic — United States, July 2020–July 2021

Weekly / November 19, 2021 / 70(46):1613–1616

Geoffrey French, MA<sup>1</sup>; Mary Hulse, MPA<sup>1</sup>; Debbie Nguyen<sup>2</sup>; Katharine Sobotka<sup>3</sup>; Kaitlyn Webster, PhD<sup>2</sup>; Josh Corman<sup>1</sup>; Brago Aboagye-Nyame<sup>2</sup>; Marc Dion<sup>2</sup>; Moira Johnson<sup>2</sup>; Benjamin Zalinger, MA<sup>2</sup>; Maria Ewing<sup>2</sup> ([View author affiliations](#))

[View suggested citation](#)

### Summary

#### What is already known about this topic?

COVID-19 surges have stressed hospital systems and negatively affected health care and public health infrastructures and national critical functions.

#### What is added by this report?

The conditions of hospital strain during July 2020–July 2021, which included the presence of SARS-CoV-2 B.1.617.2 (Delta) variant, predicted that intensive care unit bed use at 75% capacity is associated with an estimated additional 12,000 excess deaths 2 weeks later. As hospitals exceed 100% ICU bed capacity, 80,000 excess deaths would be expected 2 weeks later.

#### What are the implications for public health practice?

State, local, tribal, and territorial leaders could evaluate ways to reduce strain on public health and health care infrastructures, including implementing interventions to reduce overall disease prevalence such as vaccination and other prevention strategies, and ways to expand or enhance capacity during times of high disease prevalence.

Surges in COVID-19 cases have stressed hospital systems, negatively affected health care and public health infrastructures, and degraded national critical functions (1,2). Resource limitations, such as available hospital space, staffing, and supplies led some facilities to adopt crisis standards of care, the most extreme operating condition for hospitals, in which the focus of medical decision-making shifted from achieving the best outcomes for individual patients to addressing the immediate care needs of larger groups of patients (3). When hospitals deviated from conventional standards of care, many preventive and elective

### Article Metrics

Altmetric:

Citations:

Views:

Views equals page views plus PDF downloads

[Metric Details](#)

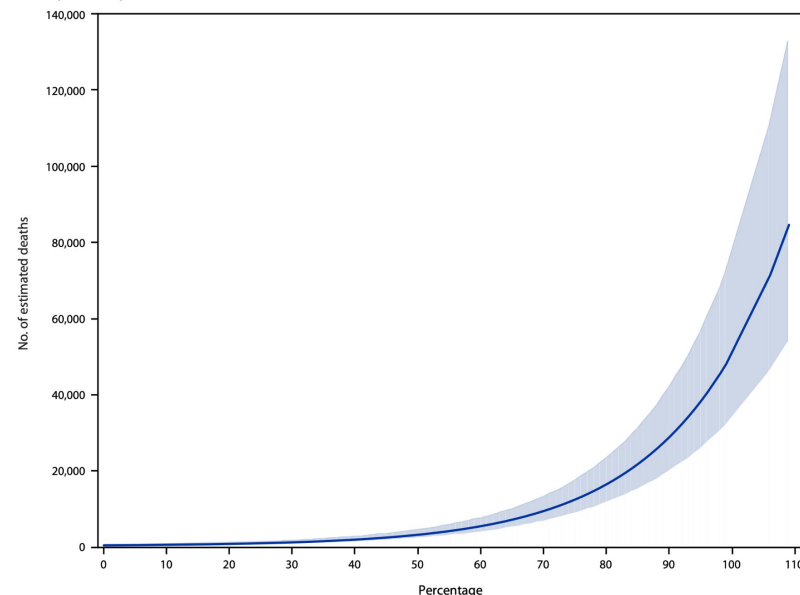
[Figure](#)

[References](#)

### Related Materials

[PDF](#) [319K]

FIGURE. Estimated number of excess deaths\* 2 weeks after corresponding percentage of adult intensive care unit bed occupancy — United States, July 2020–July 2021



\* Upper and lower boundaries of shaded area indicate 95% CIs.

Cybersecurity & Infrastructure Security Agency, unpublished data, 2021). As hospitals exceed 100% ICU bed capacity, 80,000 (95% CI = 53,576–132,765) excess deaths would be

health care and public health sectors, with excess deaths emerging in the weeks after a surge in COVID-19 hospitalizations. The results of this study support a larger body of evidence

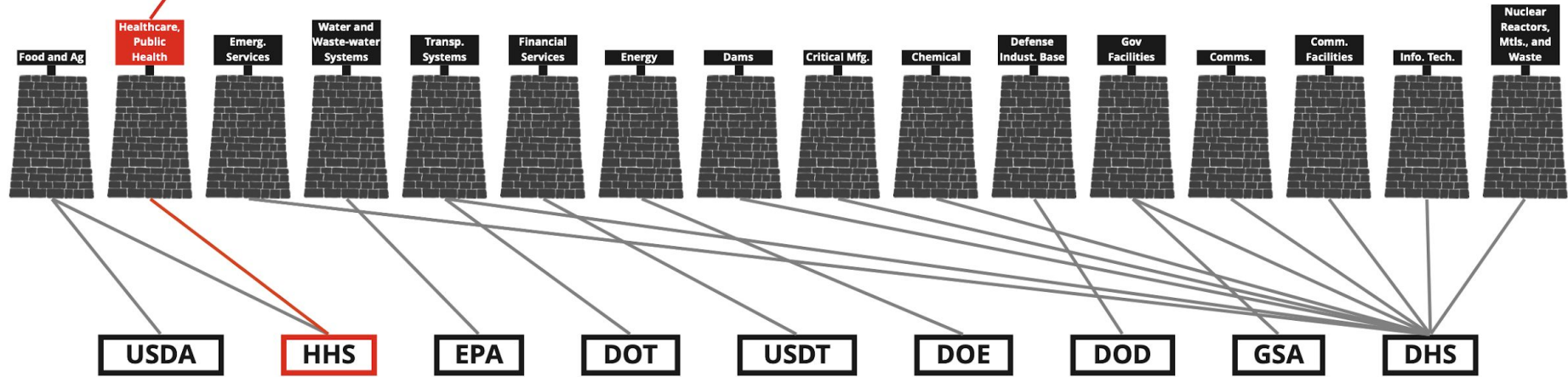


Cyber attacks lead to **1) IT network failure** and disrupt the ability of healthcare systems to access electronic health records (EHRs) and may close hospitals with IT network-based services—such as cardiac technology—and increase hospital strain (i.e., reduced capacity to take in new patients diverting critical care patients to further hospitals). **2) Ambulance diversion**, which is an important system-level interruption that causes delays in treatment and effecting time tolerance, lowering quality of care. In the long term, hospitals that experience cyber events are more likely to experience **3) hospital strain** (measured by ICU bed utilization), worsening health outcomes and contribute to **4) increased mortality**.



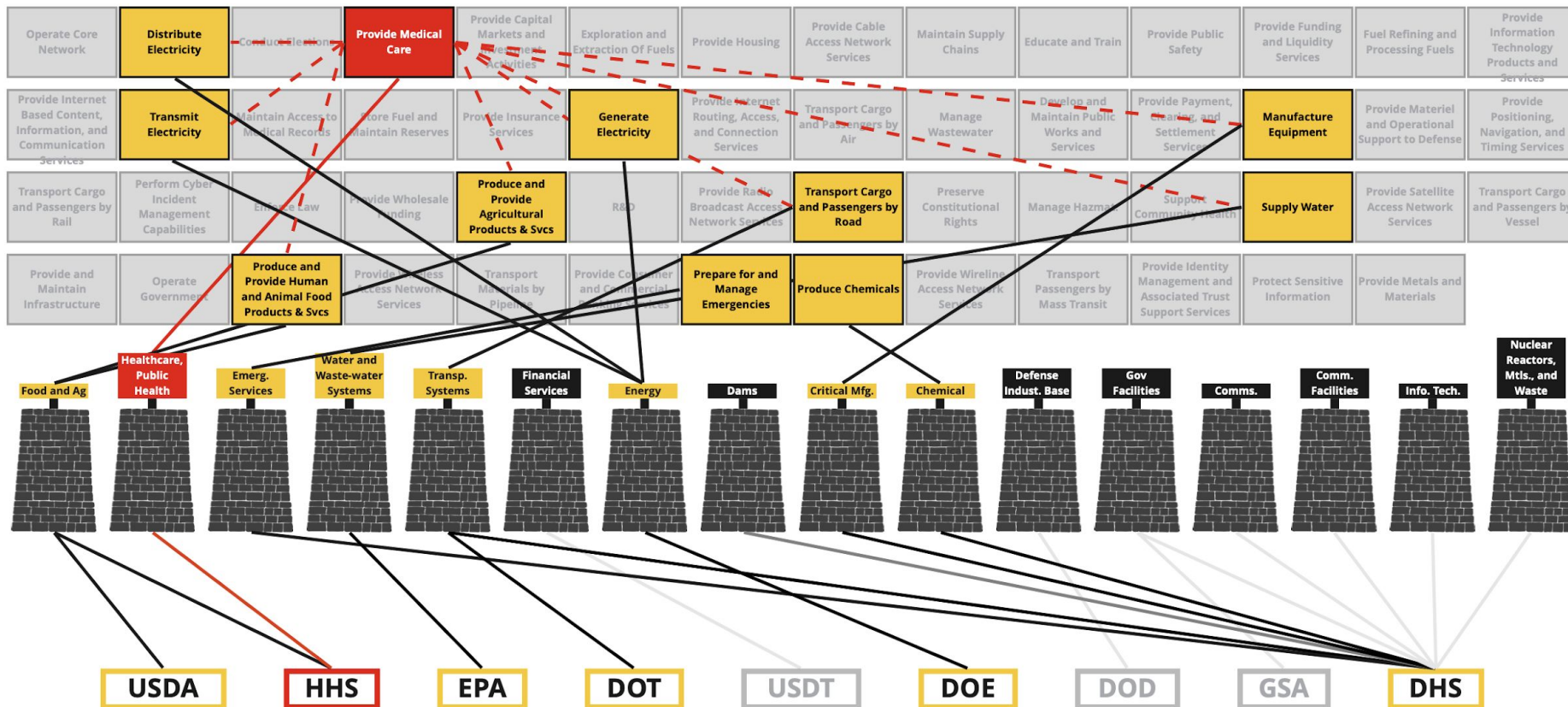
Figure 8 – Conceptual Model of Impact of Cyber Attack on Patient Outcomes

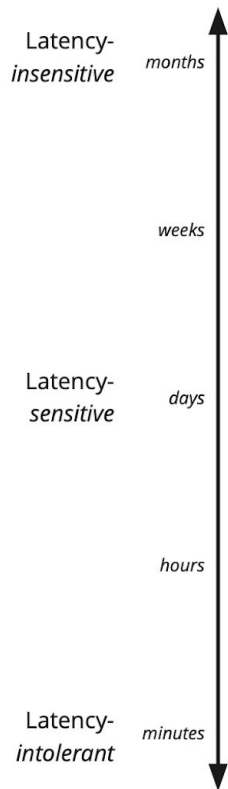
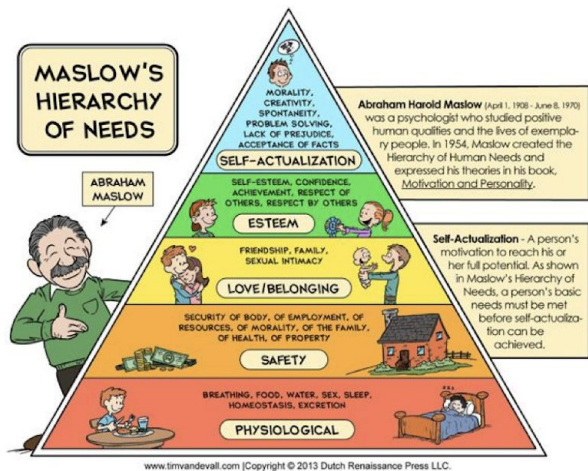
Operate Core Network	Distribute Electricity	Conduct Elections	Provide Medical Care	Provide Capital Markets and Investment Activities	Exploration and Extraction Of Fuels	Provide Housing	Provide Cable Access Network Services	Maintain Supply Chains	Educate and Train	Provide Public Safety	Provide Funding and Liquidity Services	Fuel Refining and Processing Fuels	Provide Information Technology Products and Services
Provide Internet Based Content, Information, and Communication Services	Transmit Electricity	Maintain Access to Medical Records	Store Fuel and Maintain Reserves	Provide Insurance Services	Generate Electricity	Provide Internet Routing, Access, and Connection Services	Transport Cargo and Passengers by Air	Manage Wastewater	Develop and Maintain Public Works and Services	Provide Payment, Clearing, and Settlement Services	Manufacture Equipment	Provide Materiel and Operational Support to Defense	Provide Positioning, Navigation, and Timing Services
Transport Cargo and Passengers by Rail	Perform Cyber Incident Management Capabilities	Enforce Law	Provide Wholesale Funding	Produce and Provide Agricultural Products and Services	R&D	Provide Radio Broadcast Access Network Services	Transport Cargo and Passengers by Road	Preserve Constitutional Rights	Manage Hazmat.	Support Community Health	Supply Water	Provide Satellite Access Network Services	Transport Cargo and Passengers by Vessel
Provide and Maintain Infrastructure	Operate Government	Produce and Provide Human and Animal Food Products and Services	Provide Wireless Access Network Services	Transport Materials by Pipeline	Provide Consumer and Commercial Banking Services	Prepare for and Manage Emergencies	Produce Chemicals	Provide Wireline Access Network Services	Transport Passengers by Mass Transit	Provide Identity Management and Associated Trust Support Services	Protect Sensitive Information	Provide Metals and Materials	



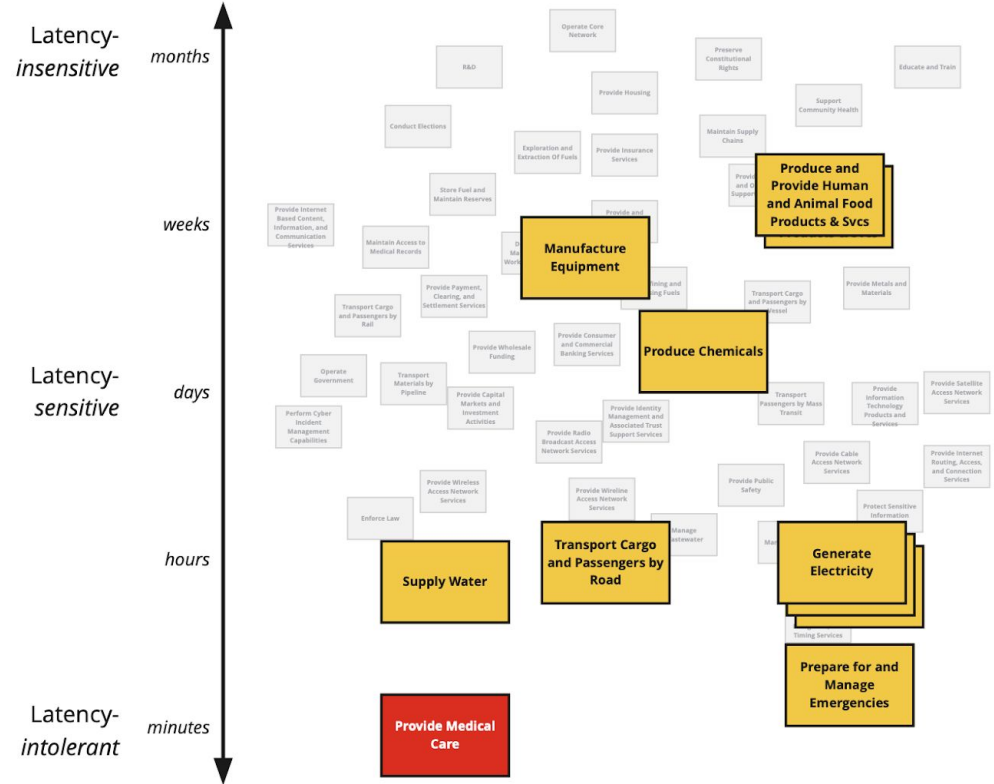
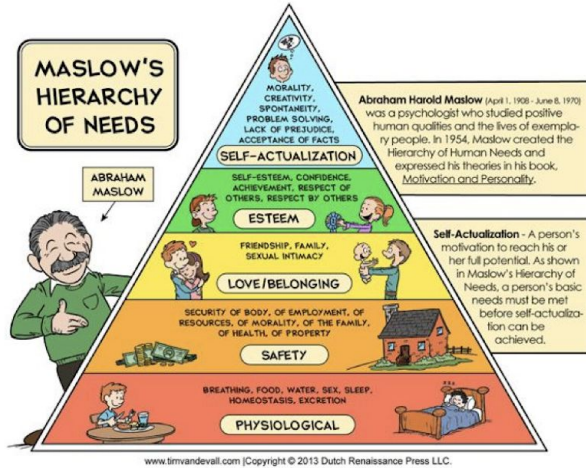


**No critical infrastructure is an island.  
Without multidisciplinary, multi-agency coordination, people die.**

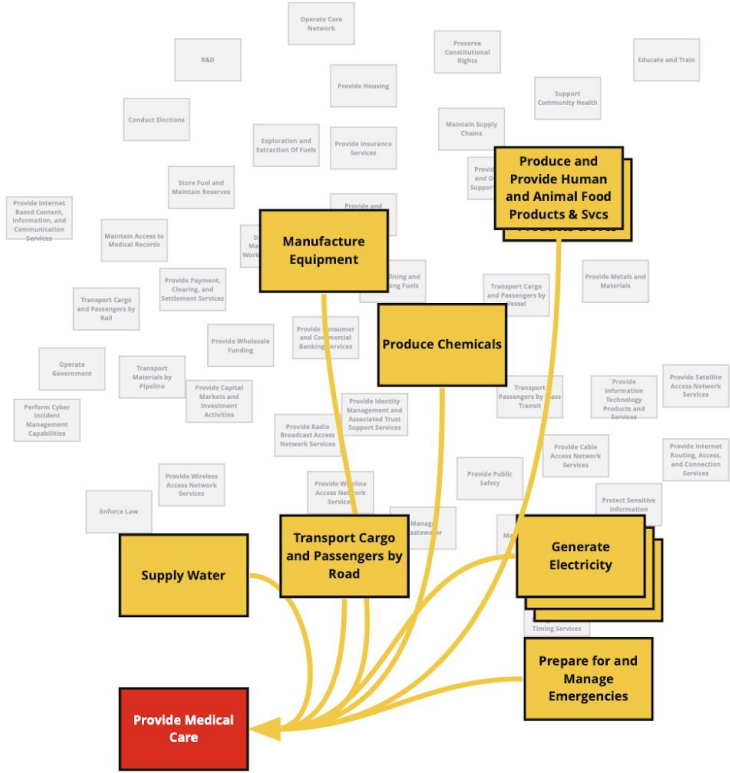
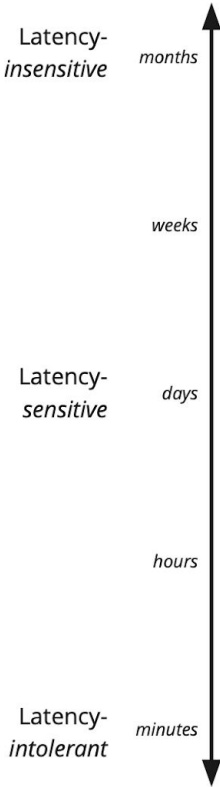
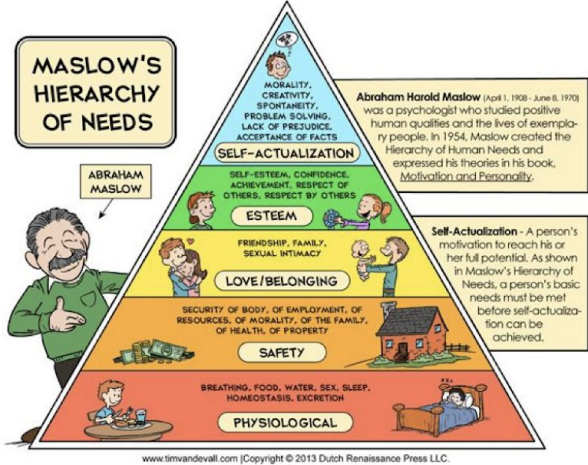


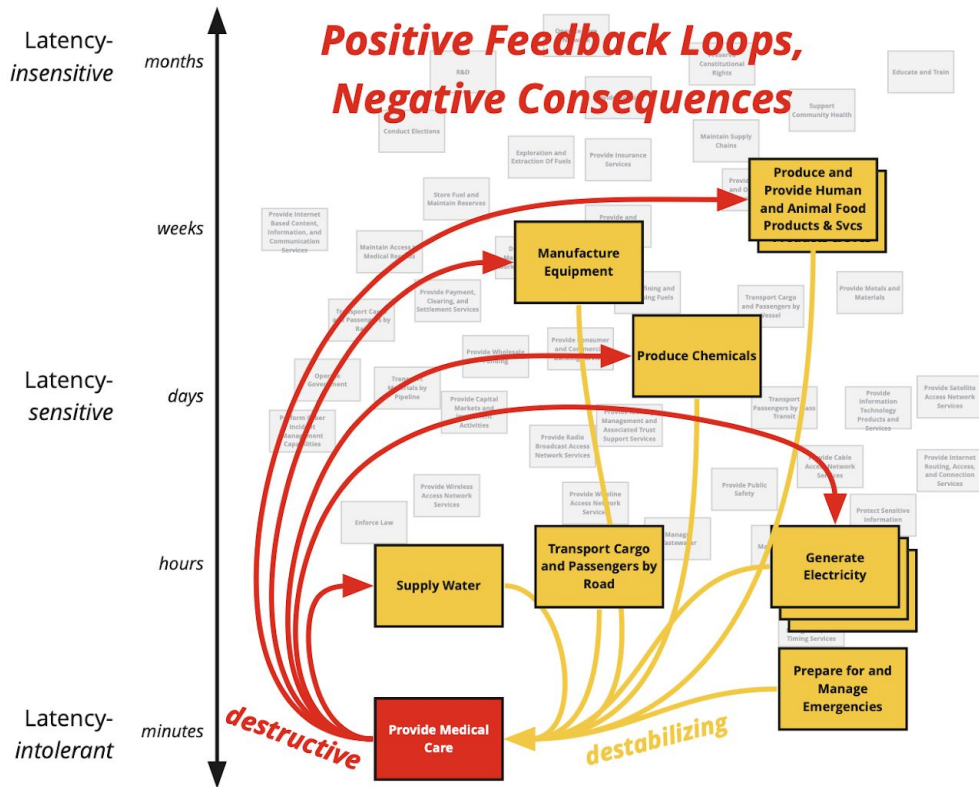
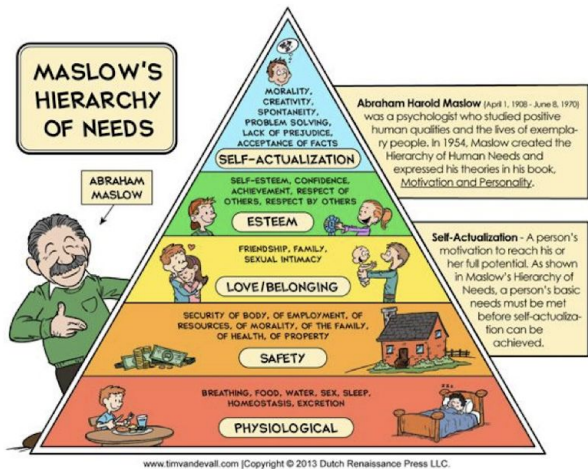












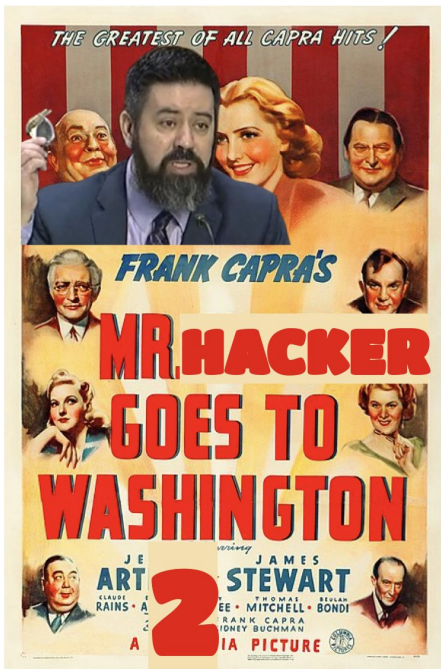
# *Target Rich; Cyber Poor*

*Information  
Incentives  
Resources*

[iamthecavalry.org](http://iamthecavalry.org)

I AM THE  
Cavalry

# CISA COVID Task Force



## BAD PRACTICES

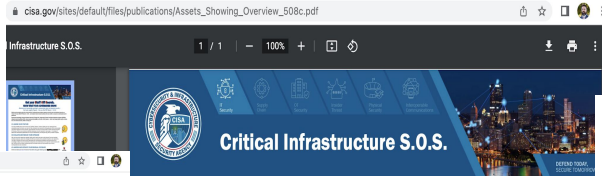


As recent incidents have demonstrated, cyberattacks against critical infrastructure can have significant impacts on the critical functions of government and the private sector. All organizations, and particularly those supporting designated Critical Infrastructure or National Critical Functions (NCF)<sup>1</sup> should implement an effective cybersecurity program to protect against cyber threats and manage cyber risk in a manner commensurate with the criticality of those NCFs to national security, national economic security, and/or national public health and safety.

CISA is developing a catalog of Bad Practices that are exceptionally risky, especially in organizations supporting Critical Infrastructure or NCFs. The presence of these Bad Practices in organizations that support Critical Infrastructure or NCFs is exceptionally dangerous and increases risk to our critical infrastructure, on which we rely for national security, economic stability, and life, health, and safety of the public. Entries in the catalog will be listed here as they are added.

1. Use of unsupported (or end-of-life) software in service of Critical Infrastructure and National Critical Functions is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety. This dangerous practice is especially egregious in technologies accessible from the Internet.
2. Use of known/used/default passwords and credentials in service of Critical Infrastructure and National Critical Functions is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety. This dangerous practice is especially egregious in technologies accessible from the Internet.
3. The use of single-factor authentication for remote or administrative access to systems supporting the operation of Critical Infrastructure and National Critical Functions (NCF) is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety. This dangerous practice is especially egregious in technologies accessible from the Internet.

While these practices are dangerous for Critical Infrastructure and NCFs, CISA encourages all organizations to engage in the necessary actions and critical conversations to address Bad Practices.\*



## Get your Stuff Off Search.

### KNOW WHAT YOUR ADVERSARIES KNOW!

Attackers are increasingly working to compromise cyber and physical security - Don't get caught off guard - Get your Stuff Off Search - S.O.S.!

While zero-day attacks draw the most attention, frequently less-complex exposures to both cyber and physical security are missed. Get your Stuff Off Search - S.O.S. - and reduce Internet attack surfaces that are visible to anyone on web-based search platforms.

Exposures increasingly include Industrial Internet of Things (IIoT), Supervisory Control and Data Acquisition systems (SCADA), industrial control systems (ICS), remote access technologies, and other critical assets - which may impact public safety, human life, and national security. CISA can help you:

### #1 ASSESS YOUR POSTURE

You have probably done a lot to secure your facilities. However, without visibility into your assets that are accessible across the Internet, you may not fully understand your potential for being attacked. While many people use search engines to find out pictures, cyber attackers commonly use similar tools to locate Internet-connected IIoT devices. In fact, once a device is identified, hacking is not even required in many cases - for example, if a device is not properly secured, it can be accessed via a default password or other weak security measures.

cisa.gov/known-exploited-vulnerabilities-catalog



## KNOWN EXPLOITED VULNERABILITIES CATALOG

Download CSV version

Download JSON version

Download JSON schema

Subscribe to the Known Exploited Vulnerabilities Catalog Update Bulletin

Back to previous page for background on known exploited vulnerabilities

CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date
CVE-2022-42091	Microsoft	Windows	Microsoft Windows Mark of the Web (MOTW) contains a security feature bypass vulnerability resulting in a	2022-11-08	Microsoft Windows Mark of the Web (MOTW) contains a security feature bypass vulnerability resulting in a	Apply updates per vendor instructions.	2022-11-29

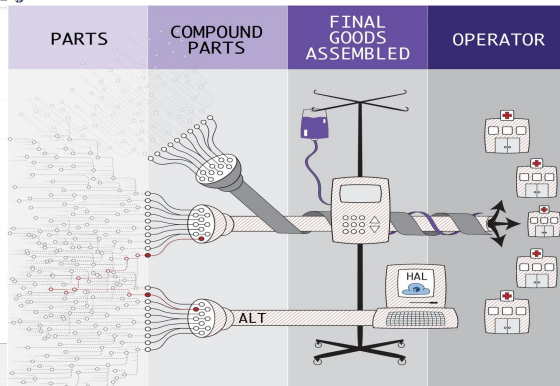


### 5.1 Mitigating Known Vulnerabilities

OUTCOME	RECOMMENDED ACTION
Reduce the likelihood of adversaries exploiting known vulnerabilities to breach organizational networks.	All known exploited vulnerabilities (listed in CISA's KEV catalog: <a href="https://www.cisa.gov/known-exploited-vulnerabilities-catalog">https://www.cisa.gov/known-exploited-vulnerabilities-catalog</a> ) in Internet facing systems are patched or otherwise mitigated within a risk-informed span of time, prioritizing more critical assets first.
TIP or RISK ADDRESSED	SCOPE
Active Scanning: Vulnerability Scanning (T1196, OOS) Default Public Facing Application (T1134, CS 19810) Exploitation of Remote Service (T1134, CS 10896) Supply Chain Compromise (T1195, CS 10862) External Remote Service (T1133, CS 10823)	Internet facing assets
⚠️ For assets where patching is either not possible or may substantially compromise availability or safety, compensating controls are applied (e.g., segmentation, monitoring) and recorded. Sufficient controls either make the asset inaccessible from the public Internet, or reduce the ability of adversaries to exploit the vulnerabilities in these assets.	

### 5.2 Vulnerability Disclosure/Reporting

OUTCOME	RECOMMENDED ACTION
Organizations more rapidly learn about vulnerabilities or weaknesses in	





SECURITY

# An Illinois hospital is the first health care facility to link its closing to a ransomware attack

A ransomware attack hit SMP Health in 2021 and halted the hospital's ability to submit claims to insurers, Medicare or Medicaid for months, sending it into a financial spiral.



St. Margaret's Health in Spring Valley, Ill. [Google Maps](#)

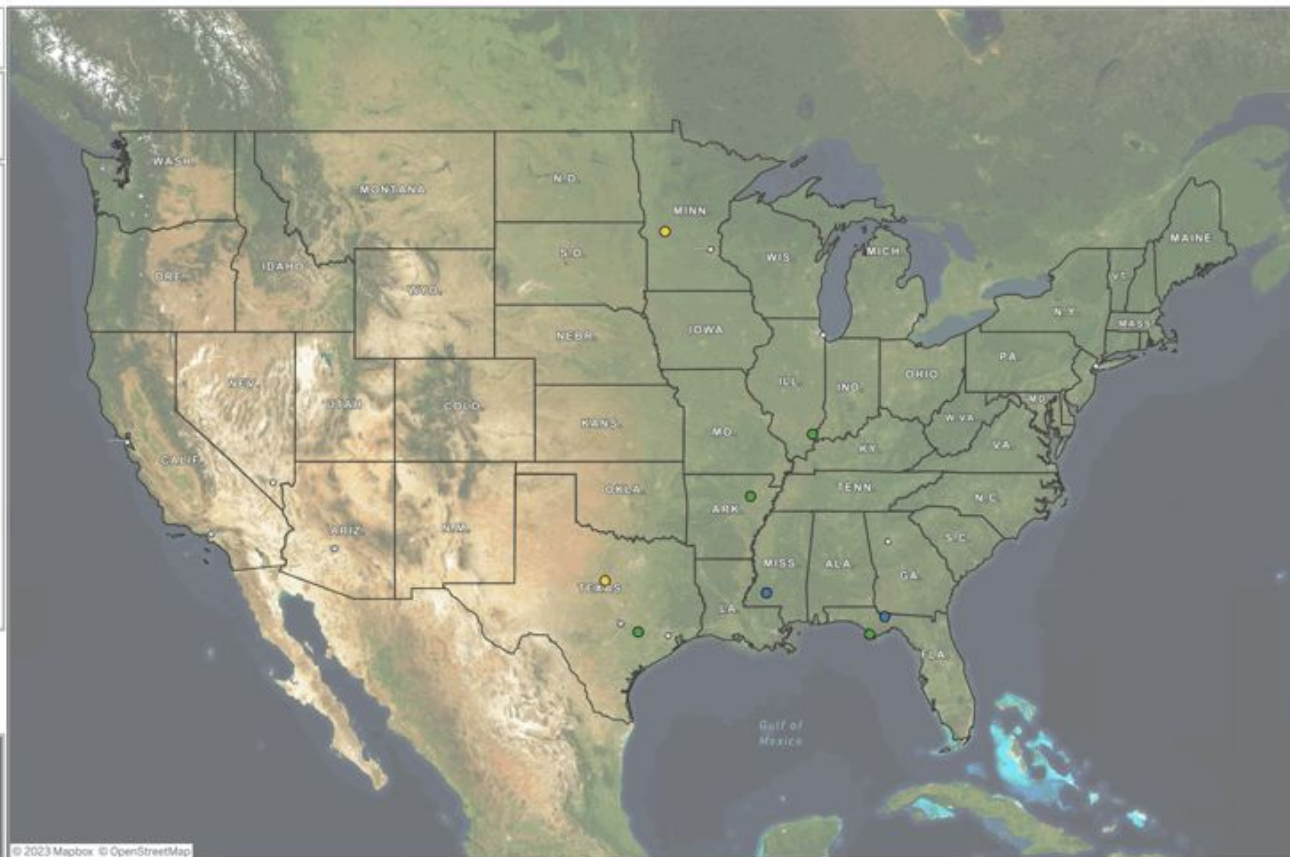
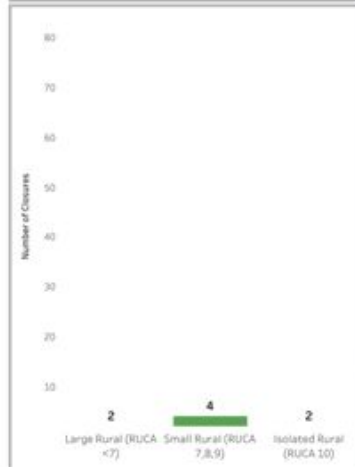


# Rural Hospital Closures Maps, 2005 – Present



Closure Year  
 2005  2005

Rurality  
 Large Rural (RUCA <7)  
 Small Rural (RUCA 7,8,9)  
 Isolated Rural (RUCA 10)



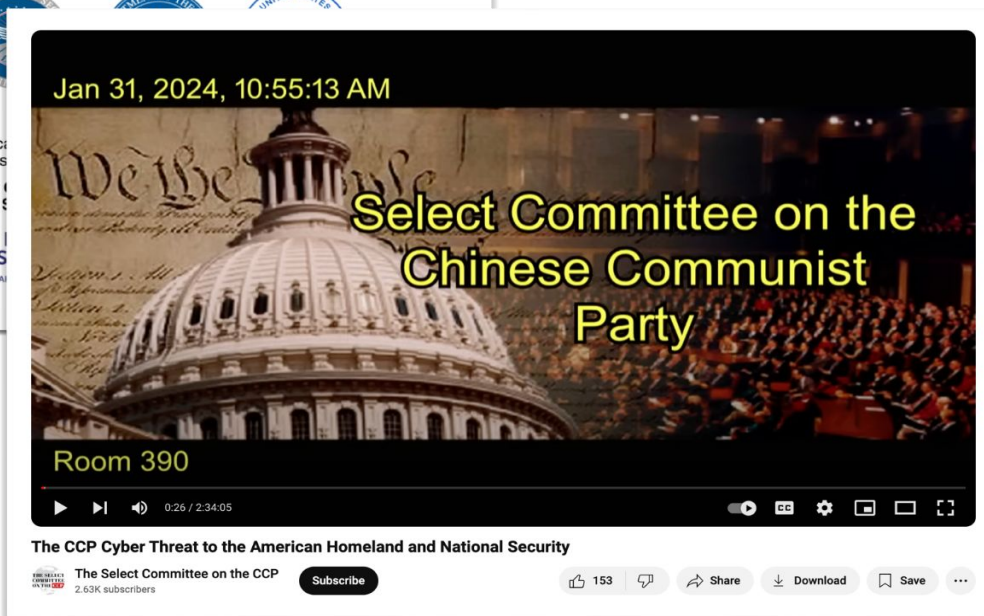


## Working Title: UnDisruptable27

Driving More Resilient Lifeline Critical Infrastructure for Our Communities

[UnDisruptable27.org](https://UnDisruptable27.org)

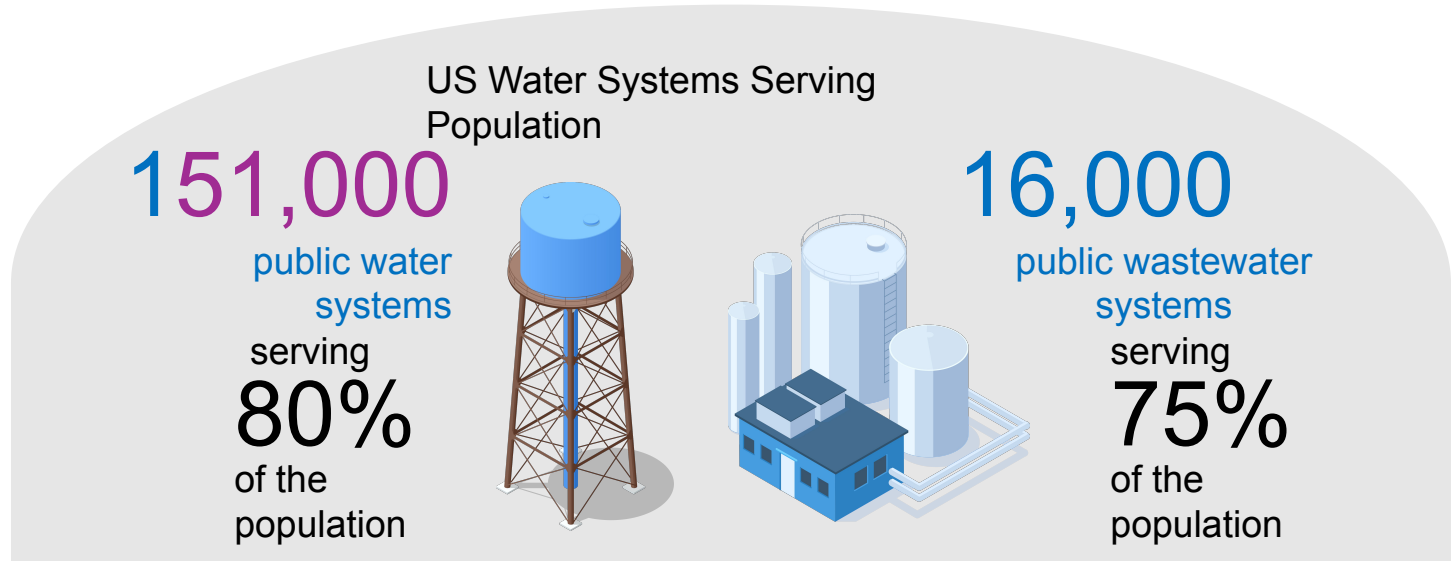
# Volt Typhoon 2027 (+/-) // China (Russia, Iran, DPRK)







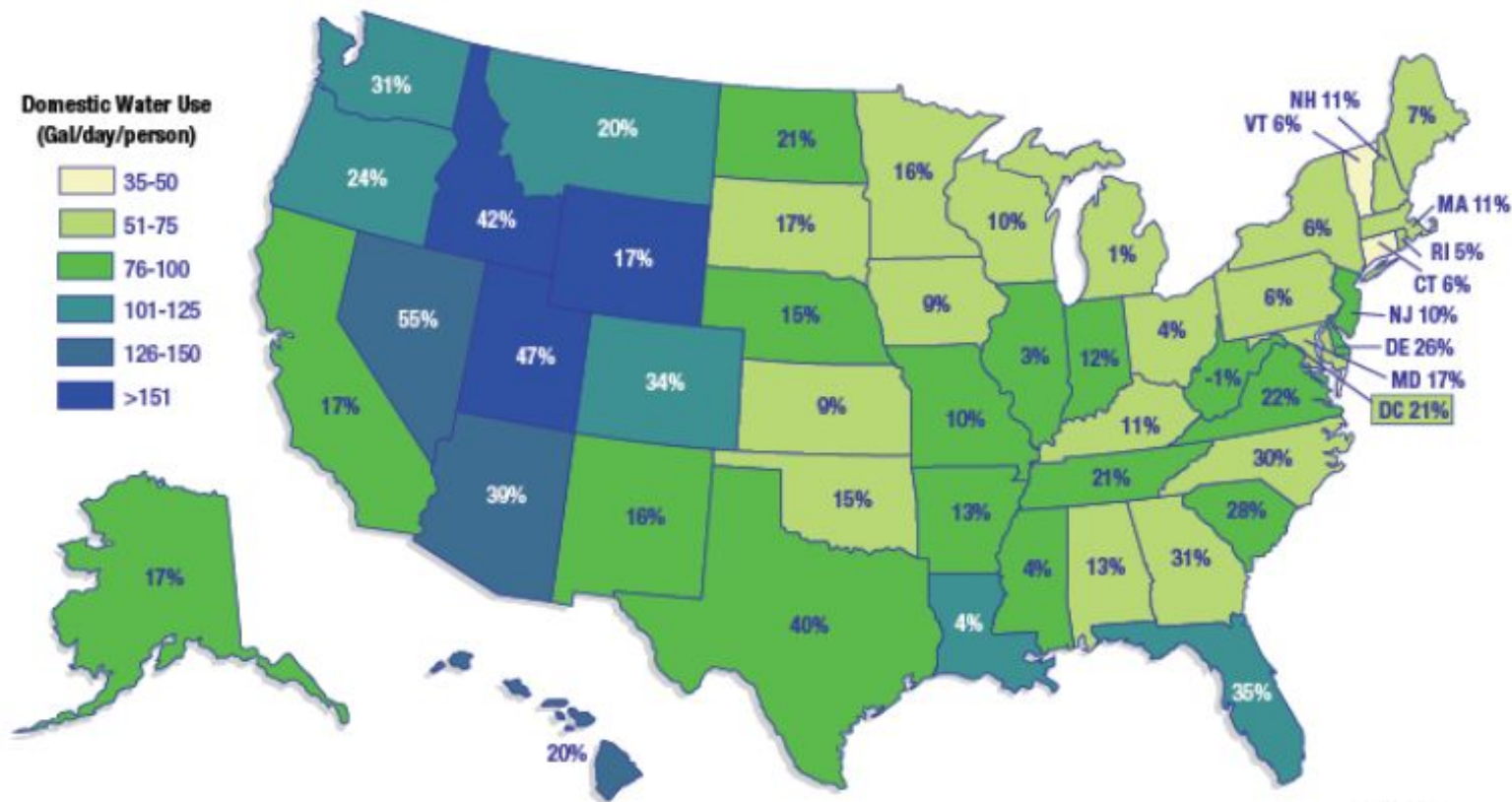




- Water systems are local. Nationwide grid does not exist.
- Failures can lead to specific and contained local collapse
- We must treat the waste side for sanitary and pollution reasons.



## Domestic Water Use in Gallons per Day per Person and Percent Population Growth from 2000 to 2020



Sources:  
U.S. Geological Survey, Circular 1441  
U.S. Census Bureau, Historical Population Change Data (2000-2020)

## U.S. Water Withdrawals

(million gallons per day)

Total 321,672.0

Thermoelectric

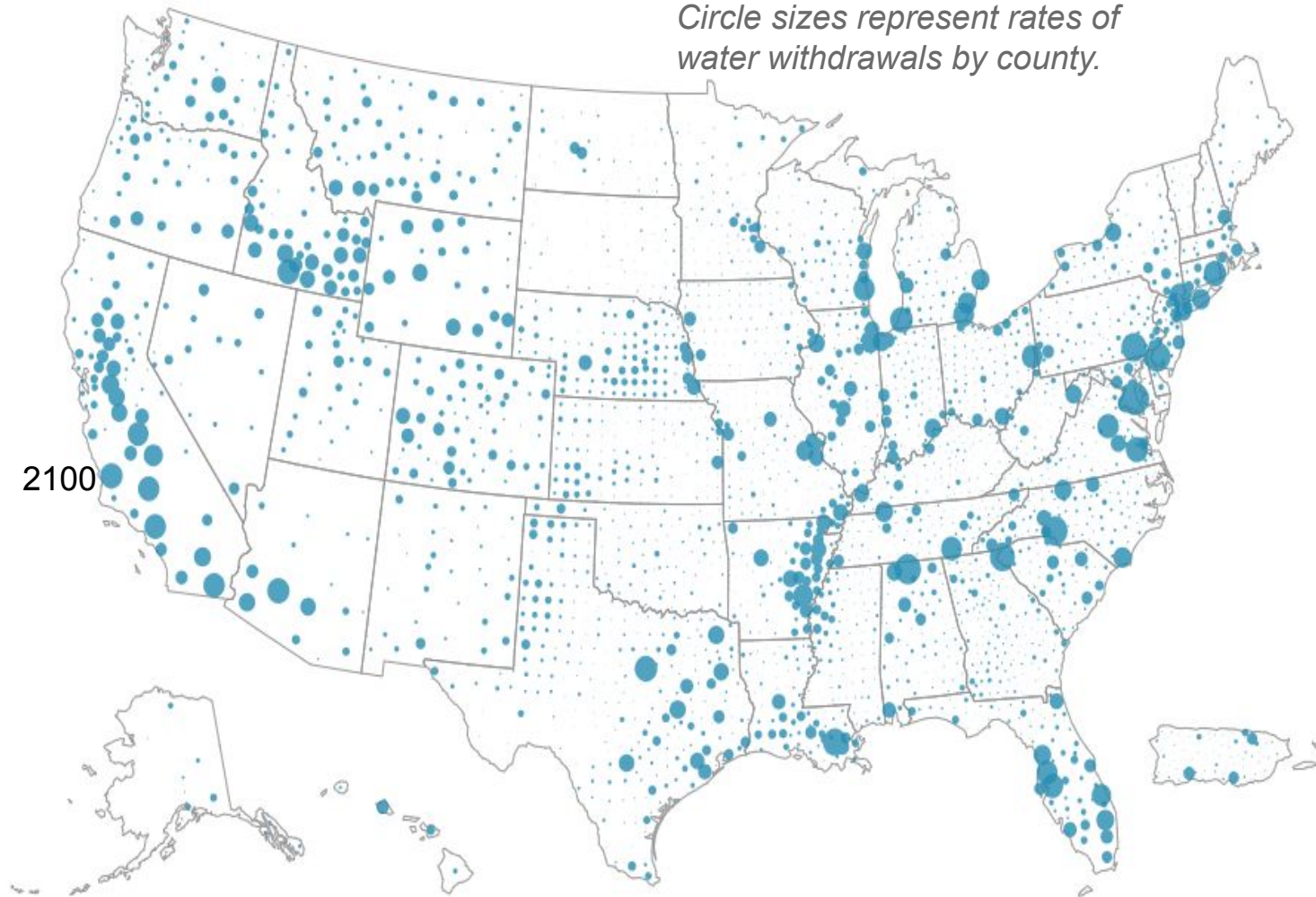
Irrigation

Public Supply

Industrial

*Circle sizes represent rates of water withdrawals by county.*

2100

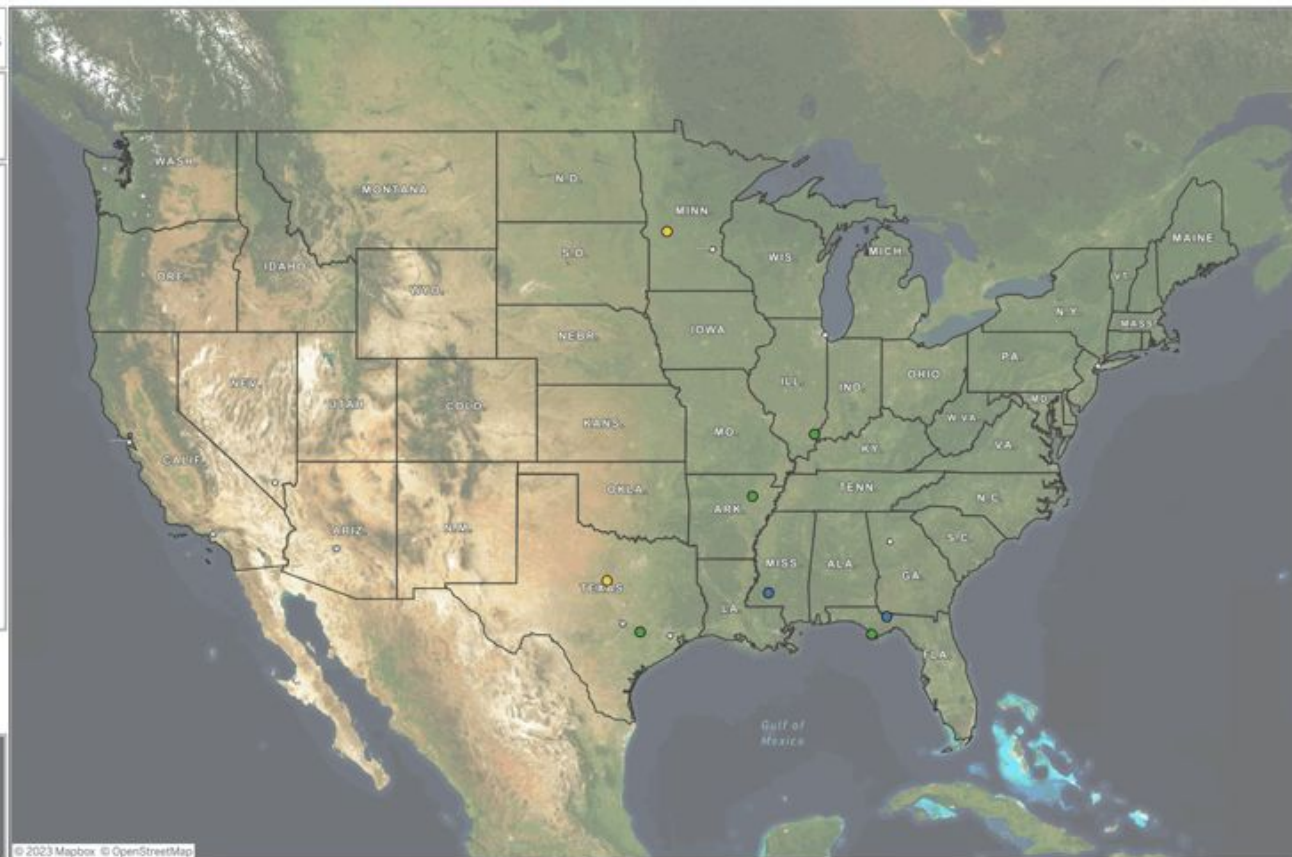
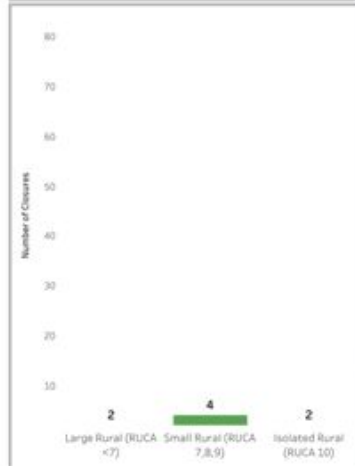


# Rural Hospital Closures Maps, 2005 – Present



Closure Year  
 2005  2005

Rurality  
 Large Rural (RUCA <7)  
 Small Rural (RUCA 7,8,9)  
 Isolated Rural (RUCA 10)

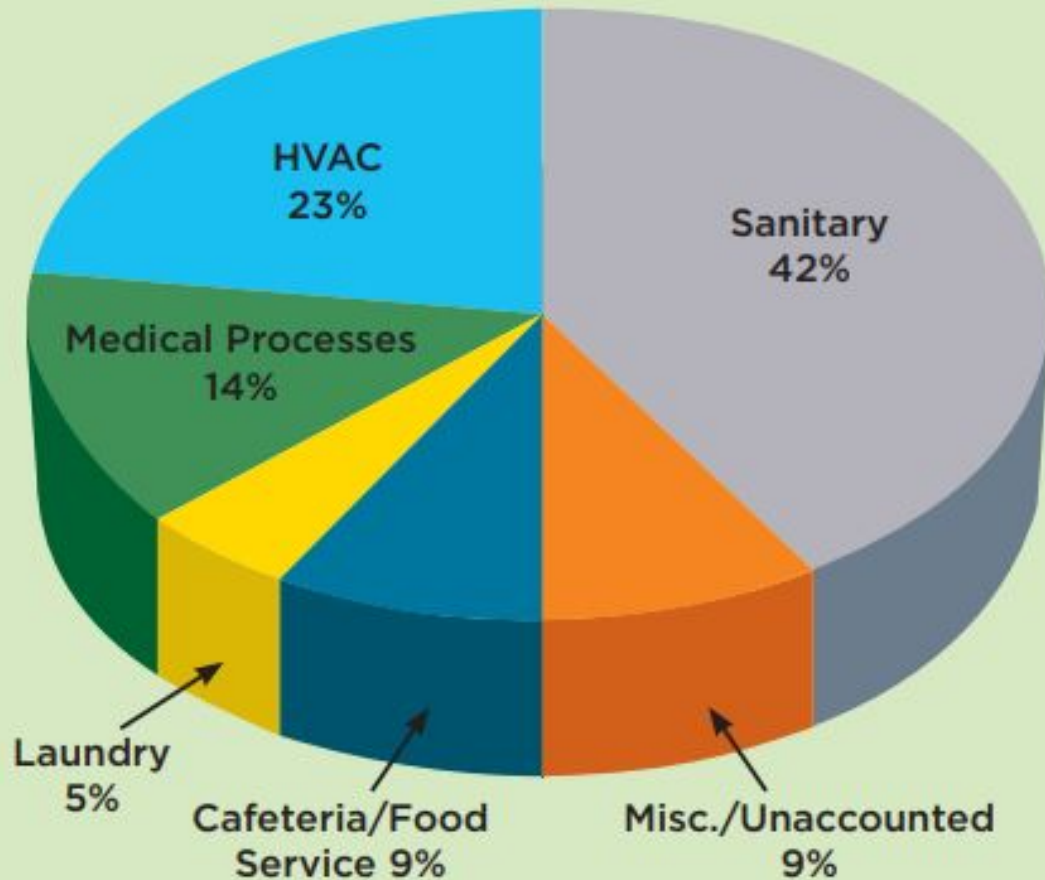


© 2023 Mapbox © OpenStreetMap



# Hospital Water Usage—Example Study

Source: Massachusetts Water Resources Authority

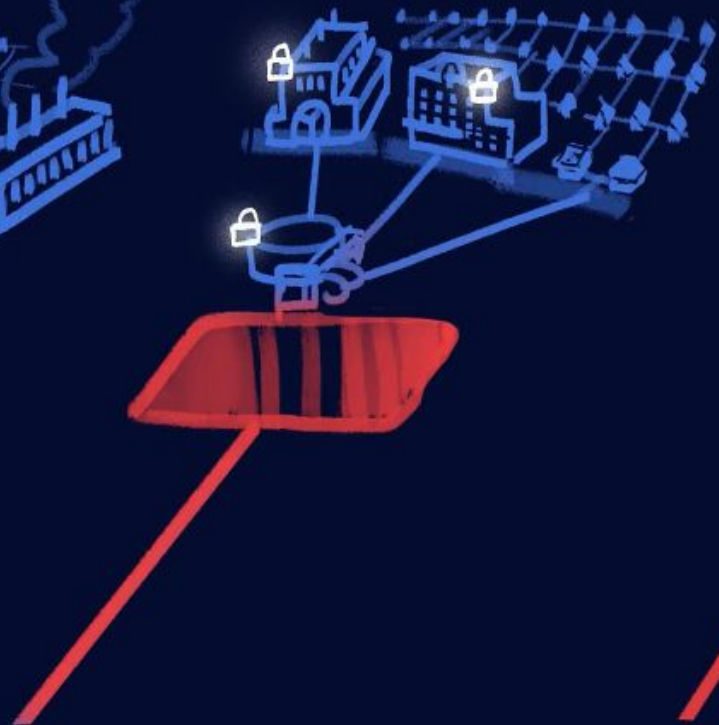
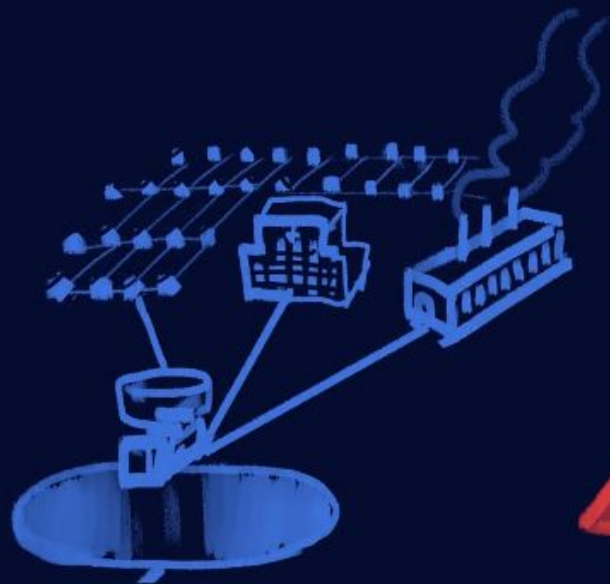


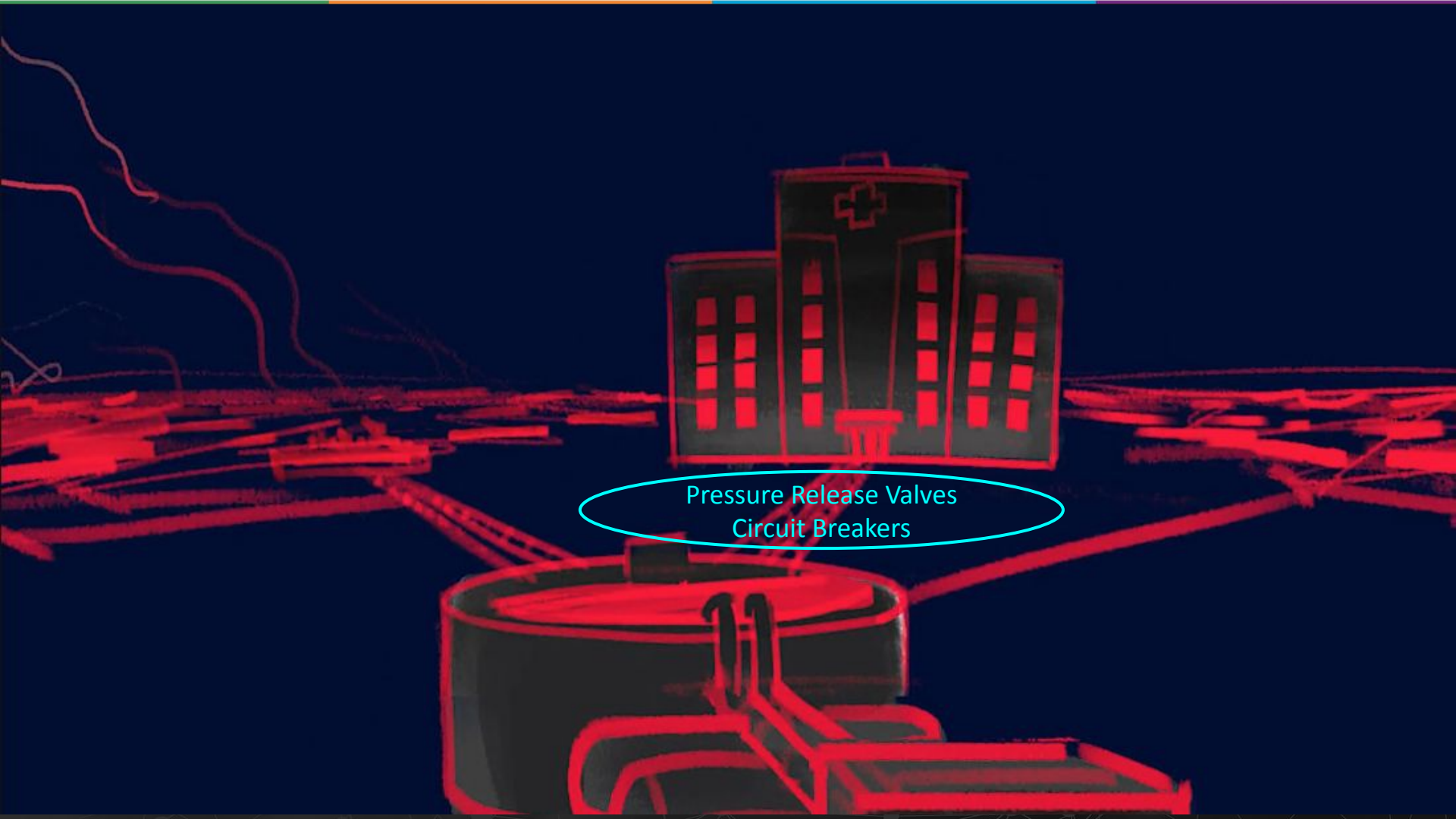
# Storyboard: UnDisruptable27.org



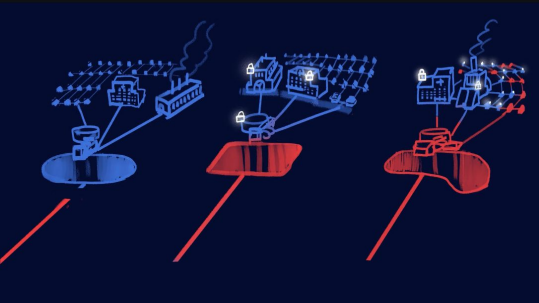








Pressure Release Valves  
Circuit Breakers



## U.S. Water Withdrawals (million gallons per day)

Total	321,672.0
Thermoelectric	
Irrigation	
Public Supply	
Industrial	

Mutual Assistance?  
Everything? Everywhere?  
All at Once?  
Focus on Trauma  
Centers?

Circle sizes represent rates of water withdrawals by county.







THE

I Am The Cavalry is a grassroots organization focused on the intersection of digital security, public safety, and human life.

Safer. Sooner. Together.

[iamthecavalry.org](https://iamthecavalry.org)



# THANK YOU!

@joshcorman

@iamthecavalry

I AM THE  
Cavalry

[www.iamthecavalry.org](http://www.iamthecavalry.org)





NASEM HPH CIP Workshop

**Thank You**

*Monday, December 9, 2024*

*Joshua Corman - @joshcorman*

*IST - The Institute for Security and Technology  
Undisruptable27.org*