MORE THAN A CSIRT:

Lessons Learned From Supporting A National Response To Covid-19

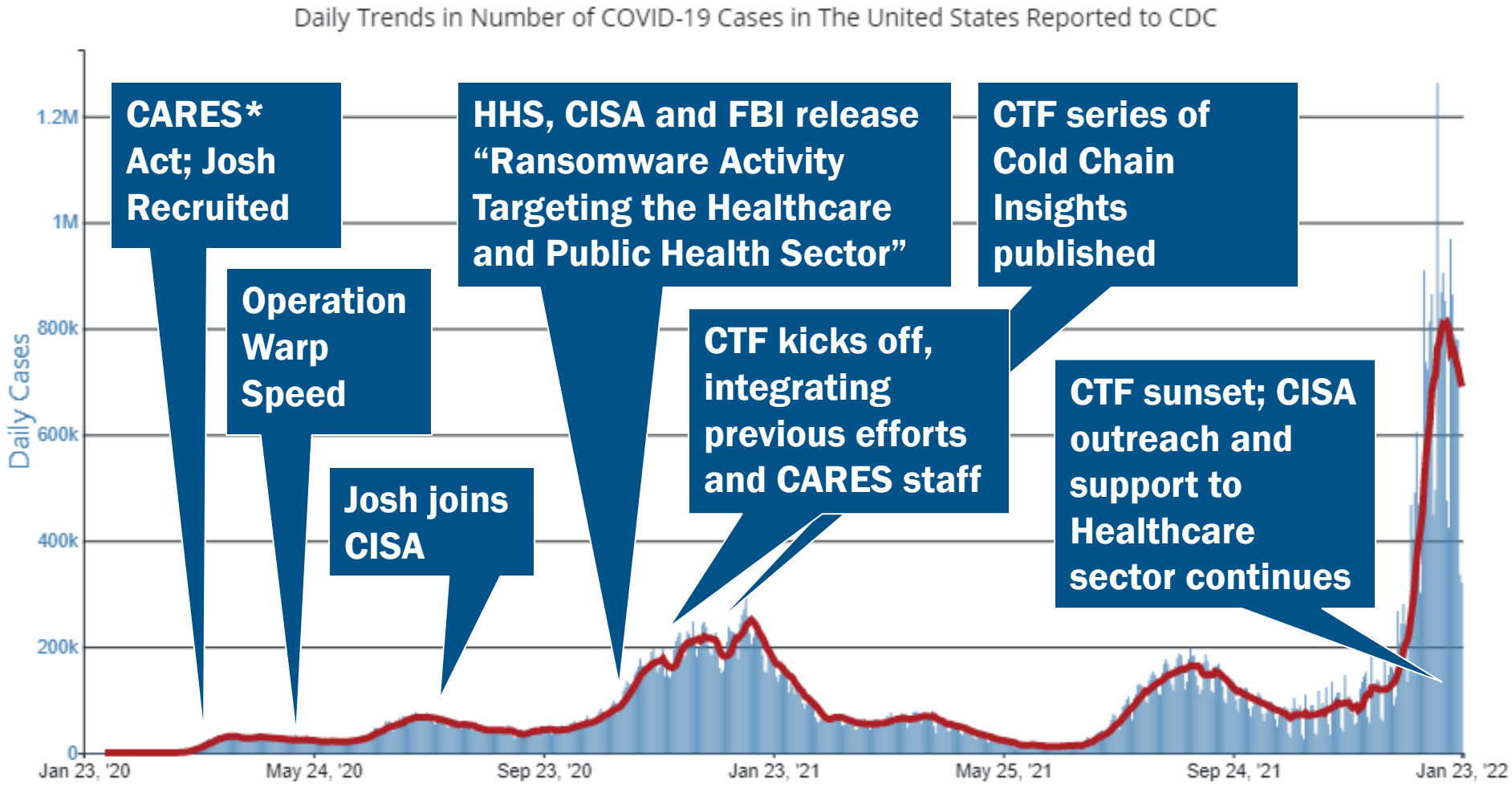
Tom Millar @CISAgov
Josh Corman @joshcorman

CISA: What It Is

"The Nation's Risk Advisor (and Reducer)"

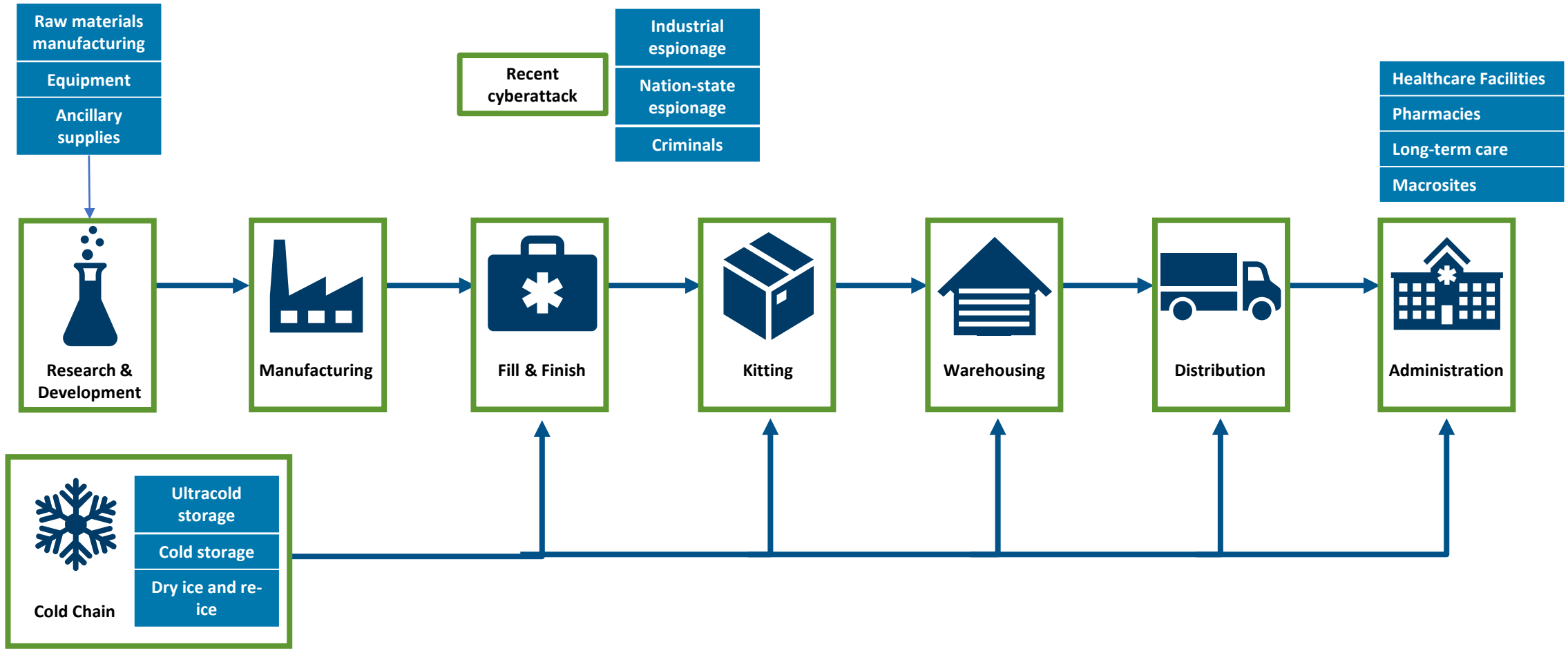
- Composed of divisions devoted to:
  - Cybersecurity
  - Infrastructure Security
  - Emergency Communications
  - National Risk Management
  - Stakeholder Engagement
  - Integrated Operations
- Serves as the "GovCERT" and National CSIRT for the US

CISA COVID-19 Task Force (CTF) Timeline



*Coronavirus Aid, Relief, and Economic Security

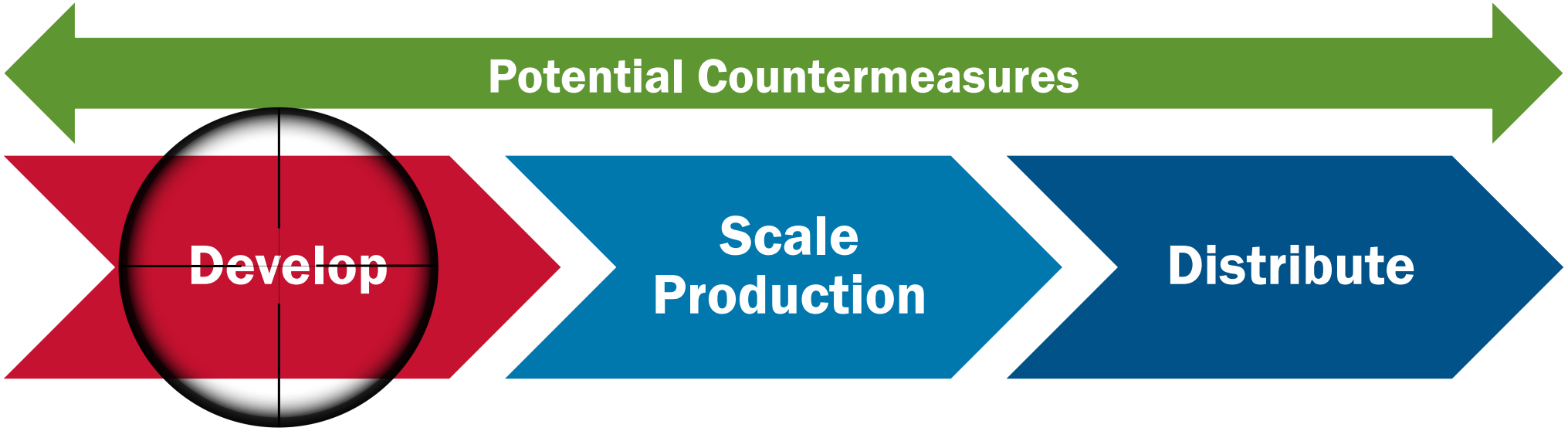
Threats to Pandemic Response



Analyzing the Mission Space ("Ball Bearings")

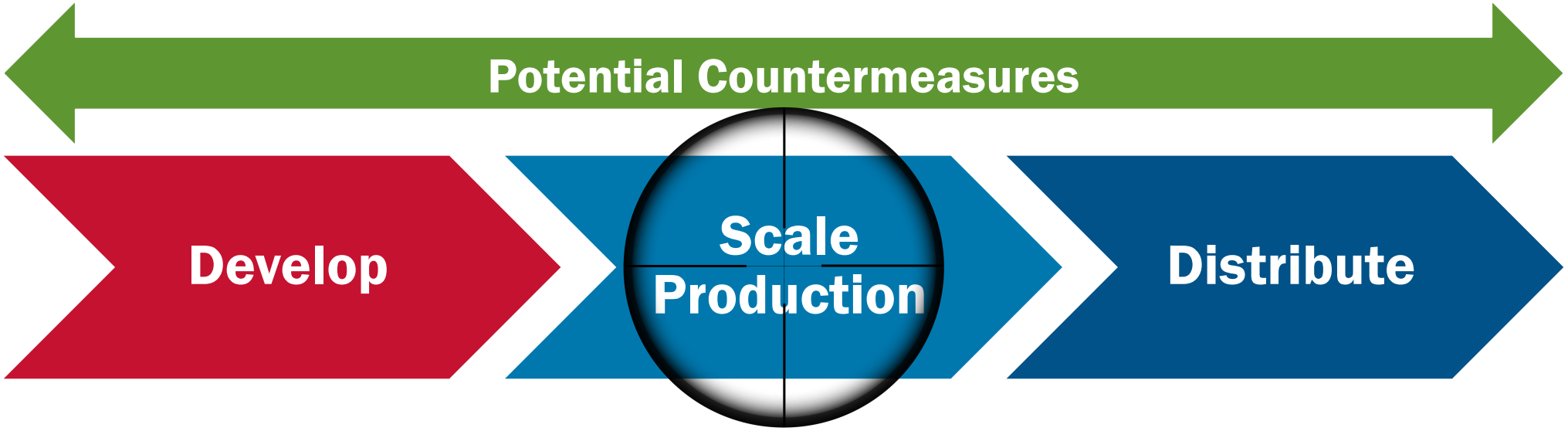
- **Operation Warp Speed / "Tier Zero" (~30 organizations)**
  - **Critical to vaccine R&D and manufacturing**
- **"Tier One" (~100 organizations)**
  - **Critical to healthcare supply chain and logistics**
- **Healthcare Delivery Organizations (HDOs) (~6,000 organizations)**
  - **Hospitals, Clinics, etc.**

“Lead The Target”



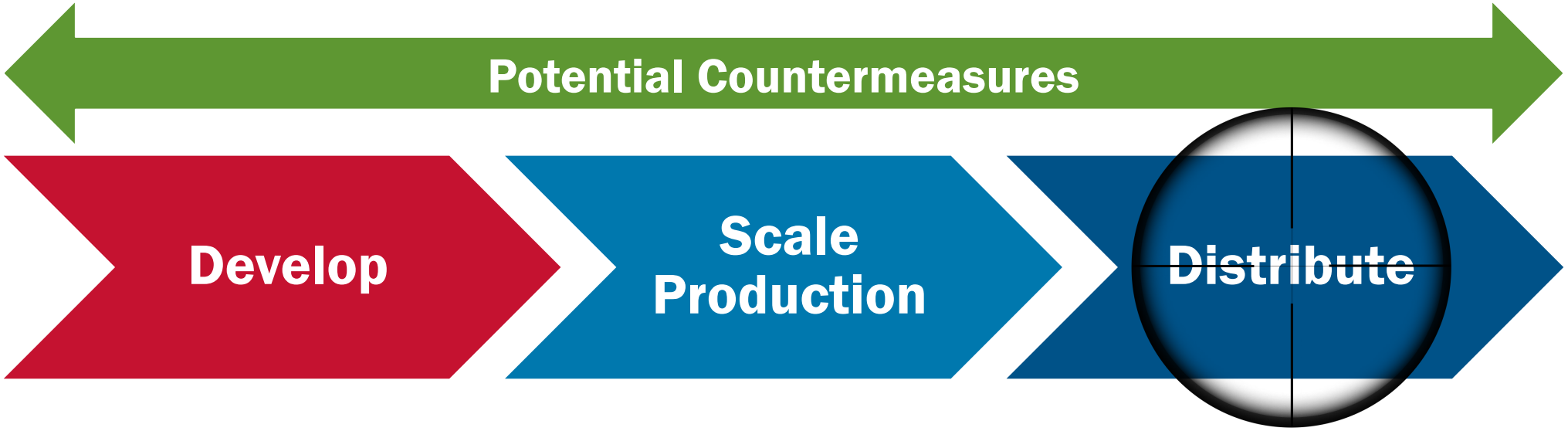
Tom Millar & Josh Corman
June 30, 2022

“Lead The Target”



Tom Millar & Josh Corman
June 30, 2022

“Lead The Target”



Tom Millar & Josh Corman
June 30, 2022

Forming the CTF

- CARES Act Hires: Staff recruited through special, temporary authorities to ensure CISA had the necessary expertise to best support US critical infrastructure through the pandemic
- Career team members: Staff seconded from their career positions within CISA to support the CTF efforts full-time
- The CTF worked across nearly every division and office within CISA
- Reported primarily to CISA's Executive Director

Example CTF Analysis: "Provide Medical Care"

- February 2021 Milestone: 500K + 150K
- October 2021 CISA Insight
- November 2021 Centers for Disease Control Morbidity and Mortality Weekly Report
- January 2022 CTF Hand-off

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

September 2021

CRITICAL INFRASTRUCTURE DECISION SUPPORT

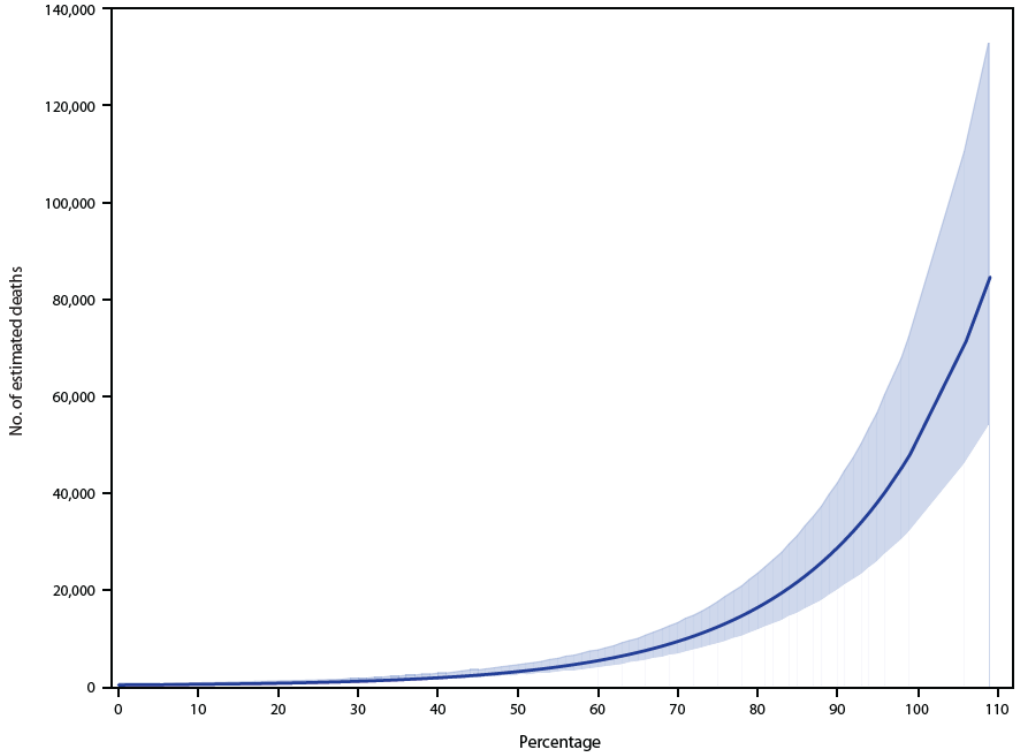
As the COVID-19 pandemic reaches another phase, with increased and protracted strains on the nation's critical infrastructure and related National Critical Functions such as *Provide Medical Care,* CISA is undertaking a renewed push for cyber preparedness and resilience, as well as decision support for 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:

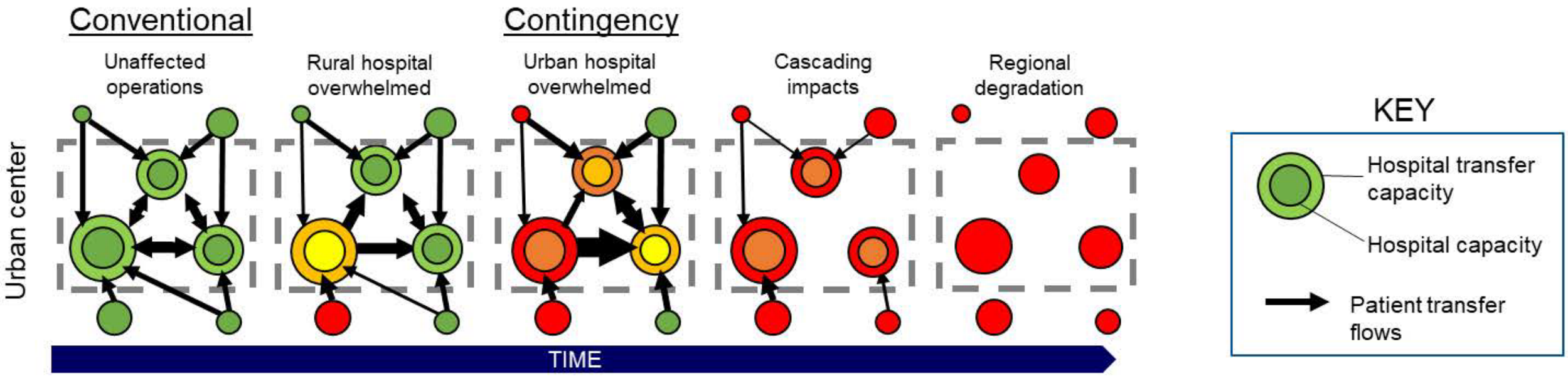
- Analysis and insights into strains on the nation's critical infrastructure, specifically through impacts to the National Critical Function *Provide Medical Care,*
- The compounding risks and harms that apply to all critical infrastructure sectors and the 55 National Critical

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

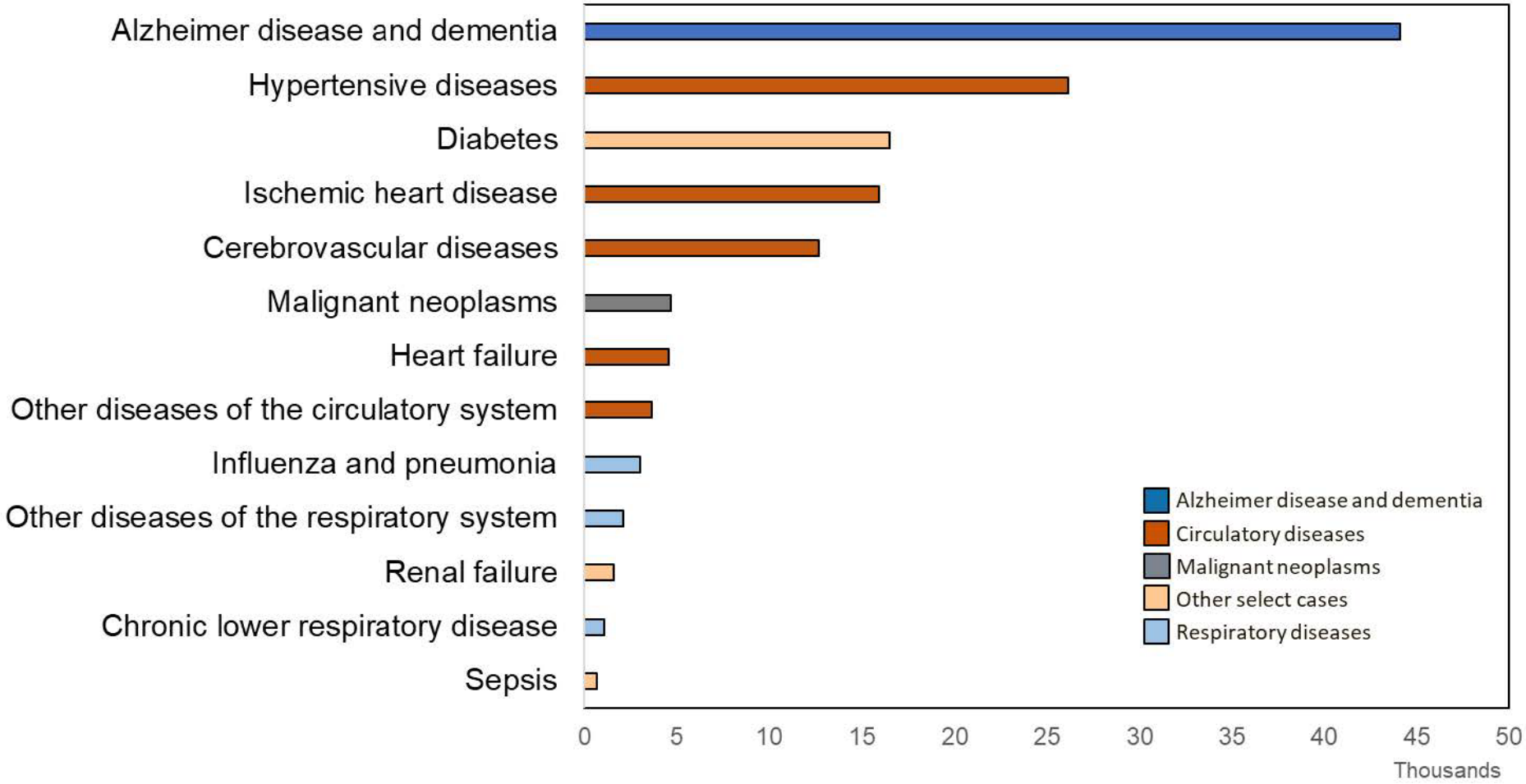


* Upper and lower boundaries of shaded area indicate 95% CIs.

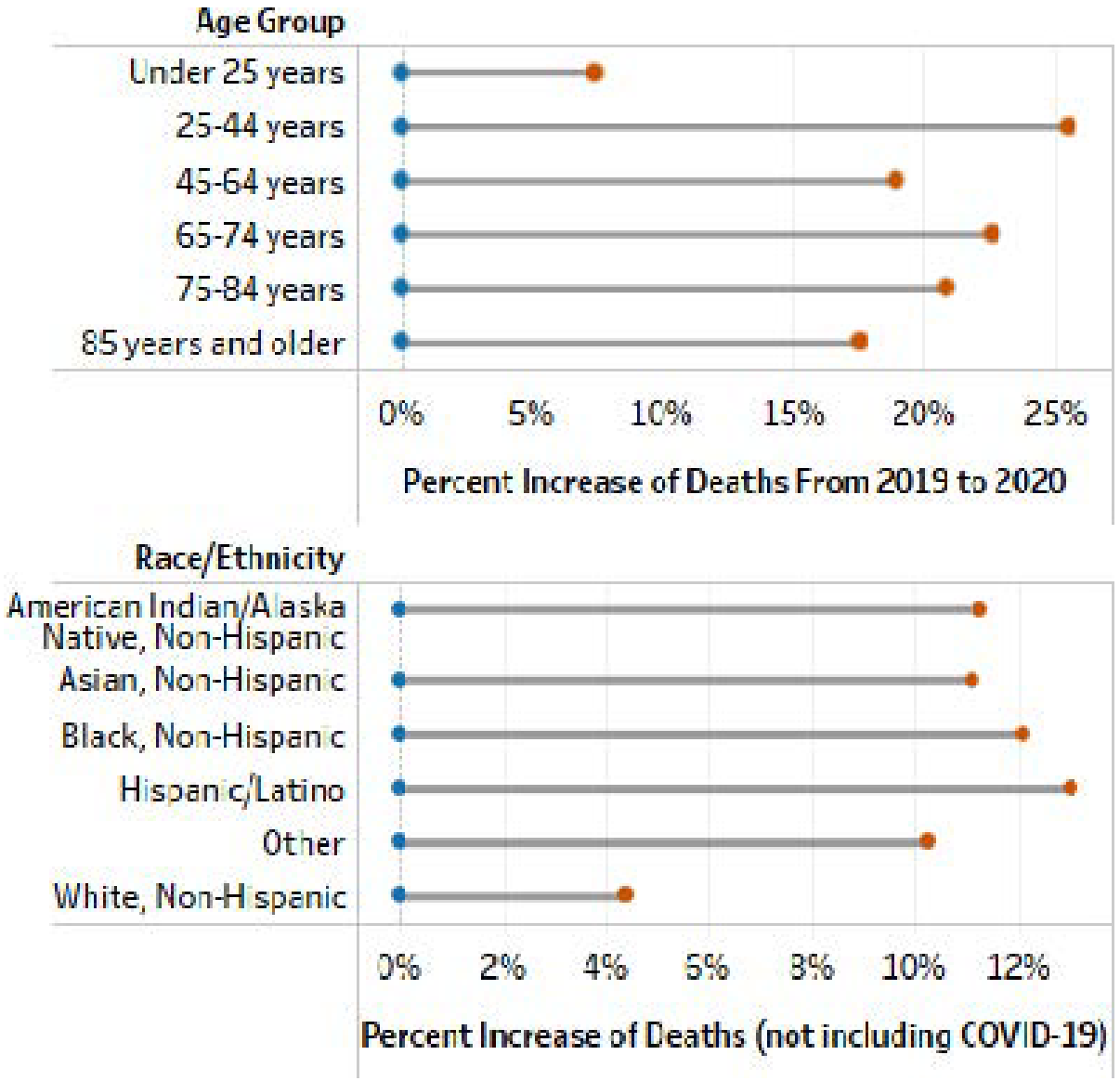
Conceptual Model of Cascading Impacts



2020 US Deaths Above Average, Excluding COVID-19



COVID-19 Deaths 2019-2020 Demographic Comparison



Hospital Services and Departments Disrupted by Cyber Attack

Emergency Services

- Loss of communication with other hospitals
- Diversion of ambulances

Outpatient Services

- Delay or cancellation of elective surgeries

Patient Portal

- Inability to view records, test results, or upcoming appointments

Radiology

- Inability to requisition scans or imaging

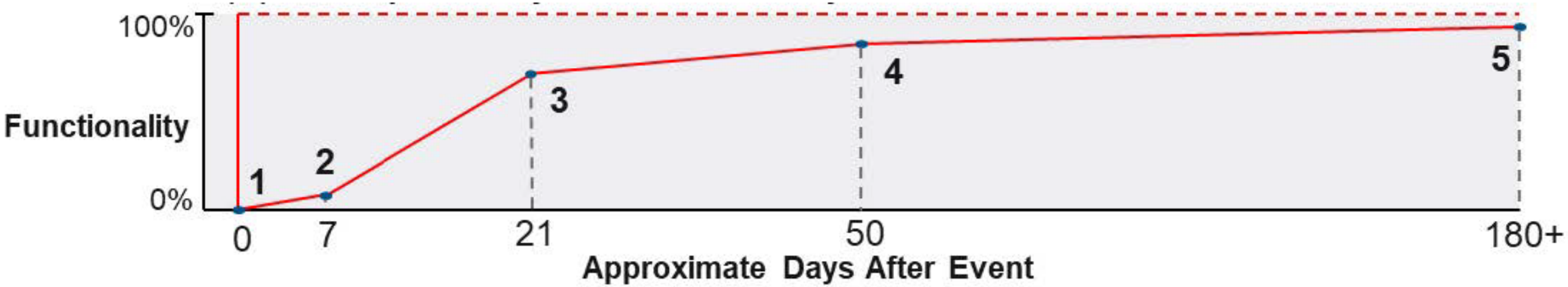
Laboratory

- Closure of COVID-19 testing sites
- Delay of processing and communicating test results

Electronic Health Records

- Inaccessible patient record systems
- Staff required to manually record patient progress and treatment

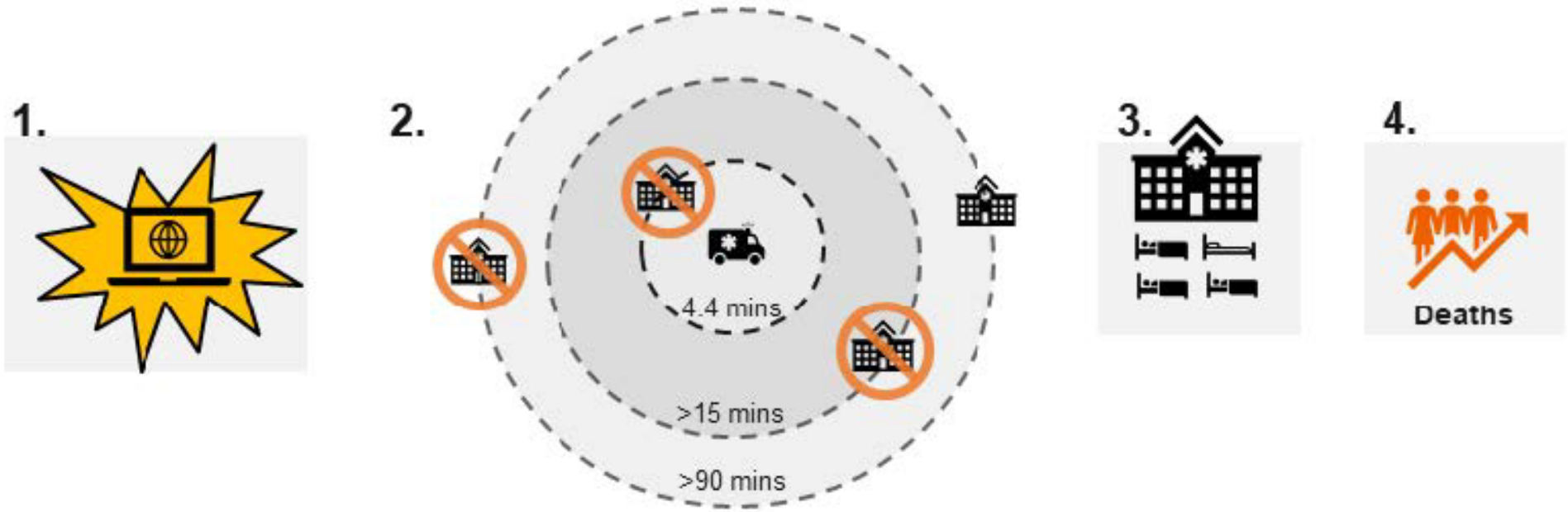
Conceptual IT System Functionality after Ransomware Event



1. Immediately after the event, the entire IT network is down, no access to online systems.
2. Available offline back-ups of the system are accessible, restoring access to some.
3. Experts begin returning network functionality to systems after clearing hardware.
4. Majority of hardware has restored access. However, some tools remain offline for cleaning/repair.
5. All hardware has access restored. Some tools may remain out of service or require more cleaning.

Conceptual Model of Impact of Cyber Attack on Patient Outcomes

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**.



Target Rich; Cyber Poor

Bad Practices

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)[1] should implement an effective cybersecurity program to

Stuff Off Search

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

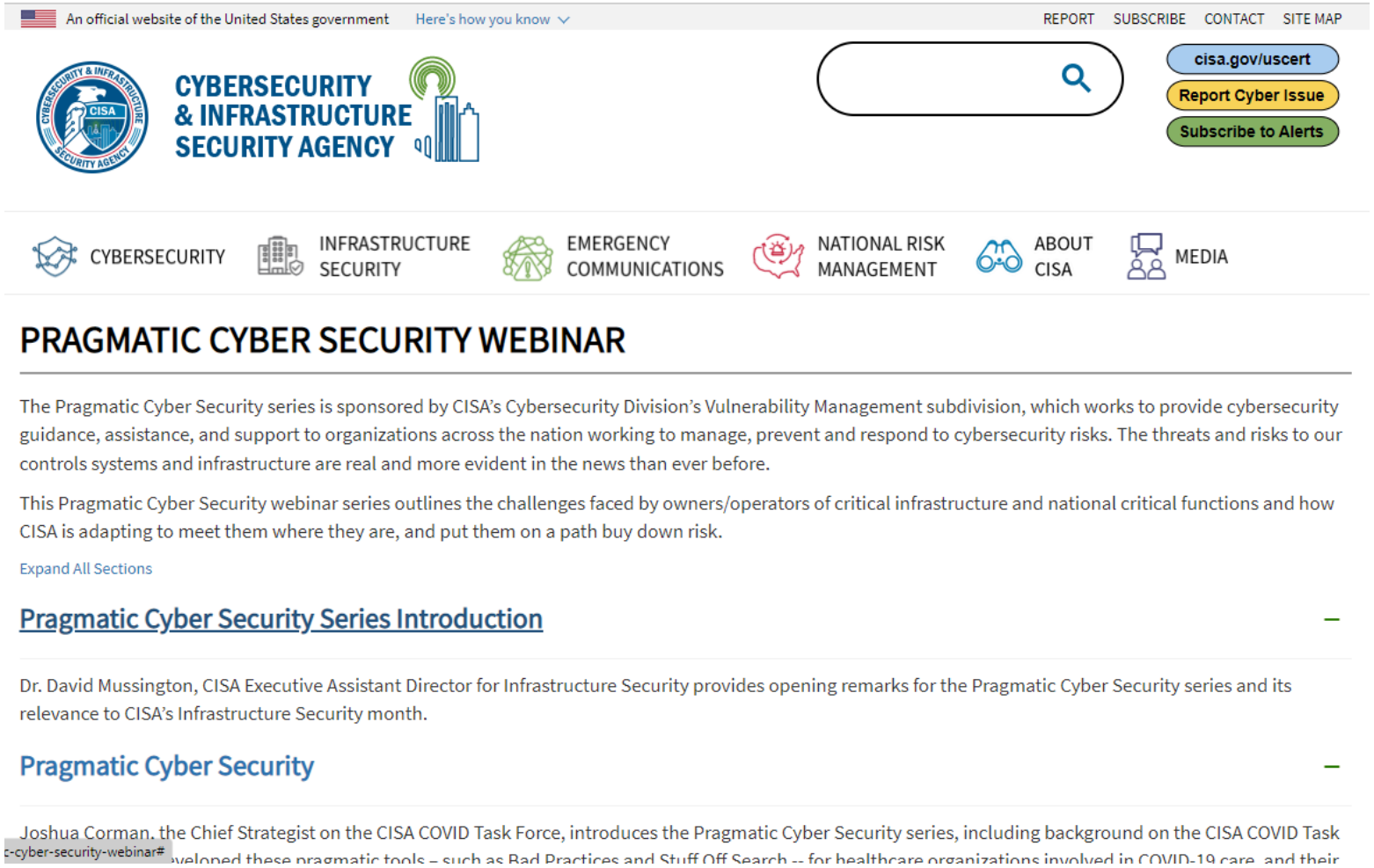
You have probably done a lot to secure your facilities. However, without visibility into your assets that are accessible across the Internet, you may not fully understand your potential for being attacked. While many people use search engines to find cat pictures, cyber attackers commonly use similar 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 default and maintenance passwords are in-use, the adversaries' job is easy as they just flip a switch to exploit.

#2 EVALUATE AND REDUCE YOUR EXPOSURE

After you know which assets are exposed, decide which need to be open to the Internet. Once you evaluate

Known Exploited Vulnerabilities (KEV)

Pragmatic Cyber Security Webinar



An official website of the United States government Here's how you know

REPORT SUBSCRIBE CONTACT SITE MAP

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

cisa.gov/uscert
Report Cyber Issue
Subscribe to Alerts

CYBERSECURITY | INFRASTRUCTURE SECURITY | EMERGENCY COMMUNICATIONS | NATIONAL RISK MANAGEMENT | ABOUT CISA | MEDIA

PRAGMATIC CYBER SECURITY WEBINAR

The Pragmatic Cyber Security series is sponsored by CISA's Cybersecurity Division's Vulnerability Management subdivision, which works to provide cybersecurity guidance, assistance, and support to organizations across the nation working to manage, prevent and respond to cybersecurity risks. The threats and risks to our controls systems and infrastructure are real and more evident in the news than ever before.

This Pragmatic Cyber Security webinar series outlines the challenges faced by owners/operators of critical infrastructure and national critical functions and how CISA is adapting to meet them where they are, and put them on a path buy down risk.

Expand All Sections

Pragmatic Cyber Security Series Introduction

Dr. David Mussington, CISA Executive Assistant Director for Infrastructure Security provides opening remarks for the Pragmatic Cyber Security series and its relevance to CISA's Infrastructure Security month.

Pragmatic Cyber Security

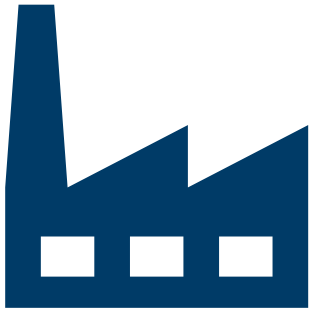
Joshua Corman, the Chief Strategist on the CISA COVID Task Force, introduces the Pragmatic Cyber Security series, including background on the CISA COVID Task

c-cyber-security-webinar#

veloped these pragmatic tools – such as Bad Practices and Stuff Off Search -- for healthcare organizations involved in COVID-19 care, and their

Helping “Tier Zero” (Vaccine R&D + Manufacture)

- Individual outreach to each “Tier Zero” organization to provide tailored services
- Highlights:
  - Full Red Team assessments
  - Cyber Hygiene assessments
  - Enhanced Information Sharing
  - Cyber Sentry / Persistent Threat Hunting



Helping “Tier One” (Vaccine & Healthcare Supply Chain)

- Individual outreach to each “Tier One” organization
- Highlights:
  - Stopransomware.gov
  - Stuff Off Search
  - Bad Practices
  - Cyber Hygiene Services
  - KEV Catalog
  - National Cyber Awareness System
  - Tabletop Exercise Packages
  - Information Sharing

Helping HDOs

- Broad outreach efforts targeting national associations and communities
- Highlights:
  - Stopransomware.gov
  - Stuff Off Search
  - Bad Practices
  - Cyber Hygiene Services
  - KEV Catalog
  - National Cyber Awareness System
  - Tabletop Exercise Packages
- This work is ongoing and continuous (post-CTF)

Cross-Sector Analysis & Risks to Critical Infrastructure

- Cold Chain / Cold Storage Risks for Vaccines
- Hospital functions & effects on services
- Strains on National Critical Functions (55)
- 2nd & 3rd order effects on Critical Infrastructure Sectors (16)
- Supply Chain Disruptions
- Essential Critical Infrastructure Workforce (ECIW) risks

Lessons Learned for Future Task Forces

- What Worked:
  - CARES Act Staff helped increase collaboration throughout CISA
  - A crisis is the perfect time for pilot efforts
  - Task Forces are great for forcing more outreach to different communities (i.e. HDOs)
  - International Sharing
- What Needs Work:
  - Awareness of CISA, our role, and our capabilities
  - Right-sizing the CISA Service Catalog
  - Build more capacity for concurrent incident response and support ("Right of Boom")
  - "Experts" needs to include *administrative* experts, too
  - Silo-busting, trust, and muscle memory for massively multi-disciplinary, cross-sector risks and incidents

Questions?


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY