NYC Health

Thursday, May 13, 2021

New York City Health Care Coalition Annual Conference

Welcome!

NYC™
Health

North HELP
COALITION

NYC Pediatric Disaster Coalition

NYPDC

GREATER NEW YORK HOSPITAL ASSOCIATION

GNYHA

Greater New York
Health Care Facilities
Association

CHCANYS DEFINING NEW DIRECTIONS

COMMUNITY HEALTH CARE ASSOCIATION OF NEW YORK STATE

SOUTHERN NEW YORK
ASSOCIATION, INC.

Southern New York Association, Inc.
SNYA

Agenda - AM

9:00 - 9:15 ***Opening Remarks and Welcome***

- **David Miller Jr.,** Executive Director, Bureau of Healthcare and Community Readiness, OEPR, NYC DOHMH

- **Dave A. Chokshi**, MD, MSc, Commissioner of Health, NYC DOHMH

9:15 - 10:00 ***Keynote Address***

Past, Present, and Future of Healthcare Preparedness

- **Dr. Eric Toner**, Senior Scholar, Senior Scientist, Johns Hopkins Center for Health Security

Agenda - AM

10:00 - 10: 45 ***Panel Discussion***

Sustaining our Gains: How can the NYC Healthcare System build on advances achieved during the pandemic response?

Moderator: **Dr. Eric Toner**

- Panelist 1: **Louise Cohen**

Primary Care - CEO, Primary Care Development Corporation

- Panelist 2: **Dr. Irwin Redlener**

Pediatrics -Special Advisor to NYC Mayor, Director of the National Center for Disaster Preparedness at The Earth Institute

- Panelist 3: **Anna Bennett**

Dialysis/End Stage Renal Disease - Quality Improvement Coordinator, Emergency Manager, IRPO-ESRD Network Region II

- Panelist 4: **Dr. Laura Iavicoli**

Acute Care and Long-Term Care, Senior Assistant Vice President for Emergency Management, NYC Health + Hospitals

Agenda – AM

10:45 - 11:00 ***Panel Discussion Q&A***

11:00 - 11:30 ***Special Topic***

Cybersecurity and Covid-19

- **Eric Cardamone**, Director of Emergency Management, Wyckoff Heights Medical Center
- **Jebashini Jesurasa**, Vice President of Information Technology, Wyckoff Heights Medical Center

11:30 - 12:00

- **Richard S. Richard Jr**., Cybersecurity Advisor, Region II (NY, NJ, PR, USVI), Cybersecurity and Infrastructure Security Agency

12:00 ***Conclusion of AM Session***

Agenda – PM Breakout Sessions

1:00 - 4:00 ***Sector Breakout Sessions***

- Long Term Care

Long Term Care – COVID 19 Recovery Tabletop Exercise

- Pediatrics

Pediatric Disaster Mental Health Model training for Providers Caring for Children

- Federally Qualified Health Centers (FQHCs)/Primary Care

FQHCs: Applying Lessons Learned to Improve Future Response

- Dialysis/End Stage Renal Disease (ESRD)

Perspectives on Personal Protective Equipment (PPE) Crisis
Talking About Transportation

4:00 ***Conference Adjourn***

Past, Present, and Future of Healthcare Preparedness

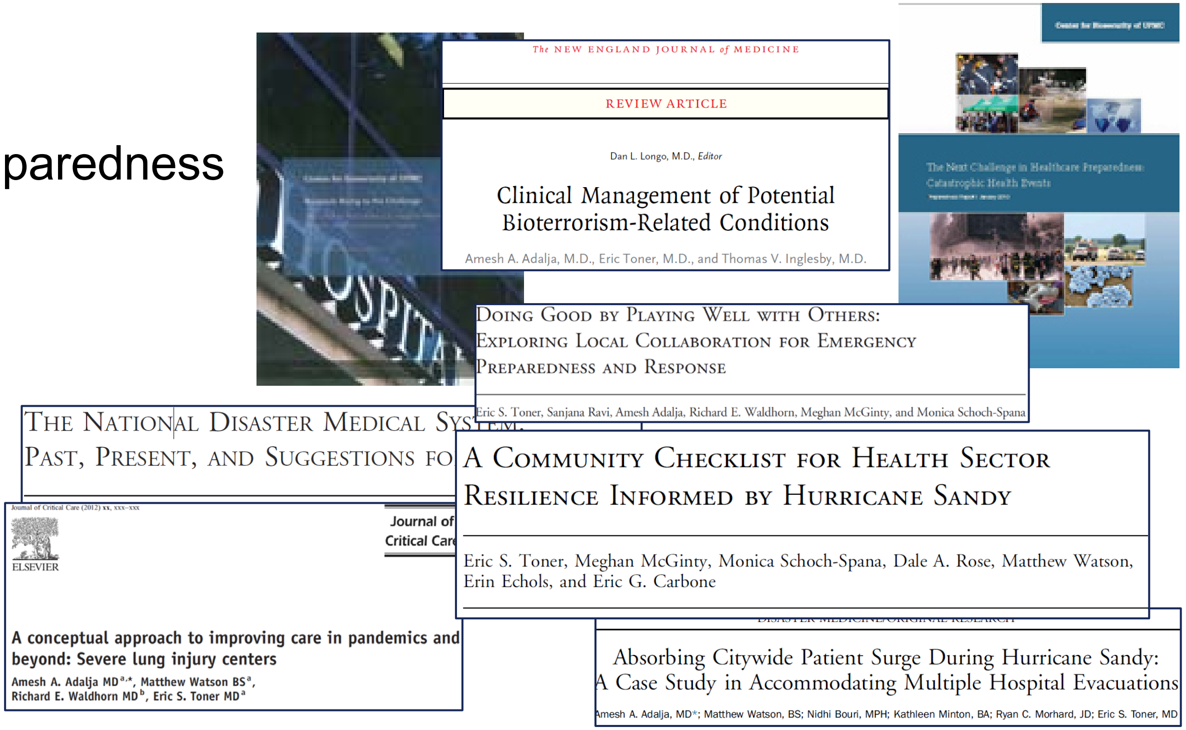
5/13/20

Eric Toner, MD

Johns Hopkins Bloomberg School of Public Health | Center for Health Security

Background: 20 Years of Studying the US Disaster Healthcare System

- Bioterrorism
- SARS
- Pandemic hospital preparedness
- Federal programs
- Hurricane Katrina
- Nuclear terrorism
- Healthcare Coalitions
- Hurricane Sandy
- Ebola
- COVID-19



The NEW ENGLAND JOURNAL *of* MEDICINE

REVIEW ARTICLE

Dan L. Longo, M.D., *Editor*

Clinical Management of Potential Bioterrorism-Related Conditions

Amesh A. Adalja, M.D., Eric Toner, M.D., and Thomas V. Inglesby, M.D.

The Next Challenge in Healthcare Preparedness: Catastrophic Health Events

Doing Good by Playing Well with Others: Exploring Local Collaboration for Emergency Preparedness and Response

Eric S. Toner, Sanjana Ravi, Amesh Adalja, Richard E. Waldhorn, Meghan McGinty, and Monica Schoch-Spana

The National Disaster Medical System: Past, Present, and Suggestions fo

Journal of Critical Care (2012) xx, xxx–xxx

ELSEVIER

Journal of Critical Care

A conceptual approach to improving care in pandemics and beyond: Severe lung injury centers

Amesh A. Adalja MD[a,*], Matthew Watson BS[a], Richard E. Waldhorn MD[b], Eric S. Toner MD[a]

A Community Checklist for Health Sector Resilience Informed by Hurricane Sandy

Eric S. Toner, Meghan McGinty, Monica Schoch-Spana, Dale A. Rose, Matthew Watson, Erin Echols, and Eric G. Carbone

Absorbing Citywide Patient Surge During Hurricane Sandy: A Case Study in Accommodating Multiple Hospital Evacuations

Amesh A. Adalja, MD*; Matthew Watson, BS; Nidhi Bouri, MPH; Kathleen Minton, BA; Ryan C. Morhard, JD; Eric S. Toner, MD

The Past

The Distant Past

- Prior to 2001, very limited JCAHCO requirements
- TJC issued the first emergency management standards in early 2001 in response to terrorist attacks in the 1990s

Then Things Got Serious

Year	Event	Progress
2001	9/11; anthrax	
2002		NBHPP; smallpox vax program
2003	SARS; severe H3N2 flu season	
2004	4 Florida hurricanes; Indian ocean tsunami	NIMS created
2005	HPAI H5N1; Hurricane Katrina	
2006		PAHPA (ASPR, BARDA)
2007		Review of HPP → shift to HCC
2009	H1N1 pandemic	Crisis standards reports
2012	Hurricane Sandy	
2014	Ebola	Tiered Ebola hospital system
2017	Las Vegas shooting	
2018		RDHRS with demonstration projects

Real Progress Was Made

- ✓NIMS created and healthcare workers across the country trained in it and HICS.
- ✓Health care emergency management field born
- ✓Hospital EOPs improved, pandemic/bio annexes added
- ✓Hospitals stockpiled respiratory protection devices
- ✓HCC to coordinate local preparedness and response arose across the country
- ✓The concept of crisis standards of care was developed
- ✓CMS preparedness rule

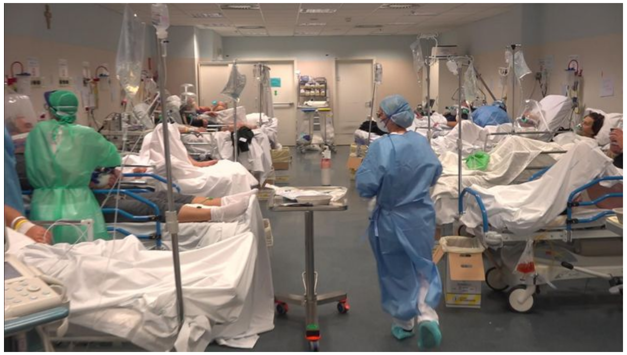
But Chronic Problems Persisted

- Most hospitals devoted minimal effort and money to emergency preparedness
- HPP’s budget cut in half; no longer funds hospital preparedness directly
- Facilities, offices, practices outside of hospitals have not been very engaged in emergency preparedness.
  - Limited success in attracting them to coalitions.

The Present: COVID-19

What Worked Well

- Much more surge capacity than expected
    - Cancellation of surgeries
    - Pop-up ICUs
    - ACS
- Innovation/creativity
    - Supply and equipment work arounds
    - Huddles
    - Homemade J-I-T YouTube ventilator instructions
    - Email, text, Whatsapp groups for clinicians
- Staff commitment/ willingness to work
- Load balancing (in some places)
- Rapid learning re: treatment
    - HFNC, proning, steroids, etc



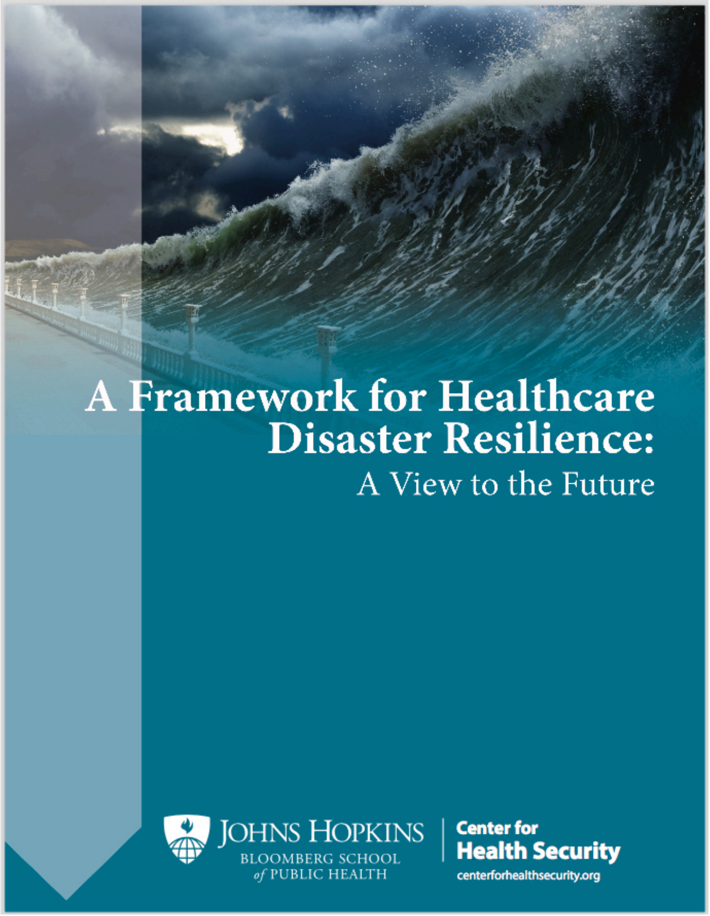
What Did Not Go Well

- Testing
  - Impaired situational awareness
- Bidirectional communications/information flow
  - Neither the USG nor the beside clinicians had the information they needed
- The medical supply chain is long and fragile
  - PPE, vents, meds, supplies
  - USG government had limited insight into it with few tools to adjust it
- Oxygen
  - Shift from vents to HFNC
  - Frozen vaporizers
  - Shortage of cylinders and flow meters

What Did Not Go Well

- Operational planning for CSC never completed
  - confusion and inappropriate application.
- HCW wellness
  - Illness (acute and chronic)
  - Anxiety
  - Depression
  - PTSD
  - Burnout

The Future: A Rational System



A Framework for Healthcare Disaster Resilience: A View to the Future

Johns Hopkins Bloomberg School of Public Health

Center for Health Security

centerforhealthsecurity.org

2018

Think about Four Distinct Disasters

- Hurricane Sandy
- Boston Bombing
- COVID-19 pandemic
- Massive Wildfires

- What’s similar and what's different in terms of healthcare needs/response?
- How well prepared are we for each?

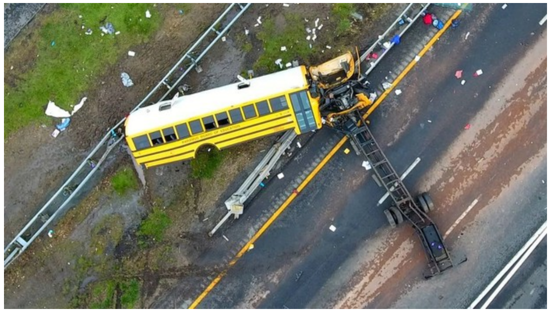
4 Types of Disasters
Health Events

- **SMALL:** Relatively small mass injury/illness events (e.g., bus crash, tornado, multiple shootings, and local epidemics/small disease outbreaks).
- **BIG:** Large-scale natural disasters (e.g., Hurricanes Sandy and Katrina, moderate earthquake, large-scale flooding, wildfires)
- **COMPLEX:** Complex mass casualty events (e.g., large scale shootings or bombing; mass casualty burn events; chem, rad, limited-scale bioterrorism; limited outbreaks of high –consequence infectious diseases e.g., Ebola or SARS)
- **CATASTROPHIC:** Catastrophic heath events (e.g., nuclear, large-scale bioterrorism, major earthquake, severe pandemic)

Differ with respect to characteristics and response requirements

How Should We Prepare for Different Disaster Health Events?

Small Mass Injury/Illness (e.g., bus crash, small epidemic, tornado)



Characteristics:

- Infrastructure mostly intact
- Healthcare system mostly intact
- Most needed response resources exist in the local area

Response Requirements:

- Healthcare coalitions (HCCs) and their constituent members provide the structure and function required for small scale events. Tested many time in recent years

Large Scale Natural Disasters

(e.g., Hurricanes, moderate earthquake, and large-scale flooding)

Brandon Clement/ LSM

Characteristics:

- Infrastructure often damaged across a wide area
- Healthcare facilities degraded for long periods
- Vulnerable populations are at greatest risk
- Much of the population is displaced from normal sources of health care
- Most individuals seeking health care are patients displaced from normal sources of healthcare
- Hospitals become refuge sites

Response Requirements :

- Greater resilience of all aspects of the health sector as well as many other parts of civil society (transportation, utilities, and communication) is needed to prevent overwhelming hospitals

Complex Mass Casualty

(e.g., large scale shootings/bombing; mass casualty burn, chemical; radiological, limited-scale bioterrorism; limited outbreaks of Ebola or SARS)

Characteristics:

- Infrastructure/healthcare system are mostly intact
- Specialty care is needed for large numbers of complex victims

Response Requirements :

- HCCs, trauma networks, and EMS together have enabled an impressive response to many recent events at the low end of the scale
- Highly specialized care mostly found in large medical centers.
  - Most community hospitals can not achieve or maintain the level of expertise and preparedness needed
- Need a network of disaster specialty centers connected to local HCCs.

A Network of Specialized Disaster Resource Hospitals

- **A network of geographically distributed disaster specialty centers** (Disaster Resource Hospitals) in large academic medical centers.
  - Each closely connected to the local HCCs, MRCs and NDMS units
- Provide:
  - **Specialized care** for complicated patients
  - **Surge capacity and capabilities**
  - **Education and training** to their local partners and coordinate exercises
  - **Research test bed** for best practices and innovation
  - **A brain trust of expertise** for each other and state and national governments.
  - **Advanced practice innovation** including exploring ways for the formal healthcare system to interact more closely with civil society and community-based organizations

Catastrophic Heath Event

(e.g., nuclear detonation, large-scale bioterrorism, severe pandemic, or major earthquake)

Characteristics:

- Infrastructure may be damaged
- Healthcare system degraded or overwhelmed
- Many people displaced from normal sources of care
- Many complex casualties
- Large geographic area

Response Requirements :

- All of the previous requirements (building community resilience, HCCs, disaster hospitals)

What Is Lacking for a Catastrophic Health Event

- A detailed national strategy
  - concept of how the many pieces would work together
  - how to enlist all national resources, public and private to work together
- True situational awareness (bedside→ boardroom → bureaucracy)
- A well-developed system for crisis standards of care

Elements of a Rational System

- A truly integrated system
- Able to adapt to events of all sizes and types
- Regular preparedness education, training, and exercises across facilities, systems, and jurisdictions
- Effective directional communication
- Coordination across a region and across healthcare systems
- Automated, standardized data collection and reporting to HICS, state and federal authorities

Specific Recommendations

1. Concurrent increase in preparedness requirements and funding
2. Continue to support and foster of HCCs with increased funding through HPP
3. Fund individual hospital prep through CMS with strengthened prep rule
   - Emphasis on surge capacity
4. Revamp federal role in medical supply chains
5. Designate a program at ASPR/NSC exclusively dedicated to catastrophic preparedness and response
   - Launch an initiative to promote disaster resilience among CBOs
   - Create a new set of healthcare-specific national planning scenarios
6. Expand the RDHRS from 3 to at least 10 through a separate HPP funding line
   - Begin to create a national network of regional disaster resource hospitals

Acknowledgments

- Rich Waldhorn, MD
- Tom Inglesby, MD
- Monica Schoch-Spana, PhD
- Matthew Shearer, MPH
- Hanna Collins

Robert Wood Johnson Foundation

Questions?

Eric Toner, MD

etoner1@jhu.edu

http://www.centerforhealthsecurity.org/our-work/publications/a-framework-for-healthcare-disaster-resilience-a-view-to-the-future

Cybersecurity Services For Building Cyber Resilience

aka *Don’t Divide and Conquer – Partner and Prevail*

R. S. Richard Jr., CISM, CCISO
Cybersecurity Advisor, Region II (NY, NJ, PR, VI)
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency

NYC Health Care Coalition Annual Conference
13 May 2021

CISA
CYBER+INFRASTRUCTURE

Cybersecurity Advisor Program

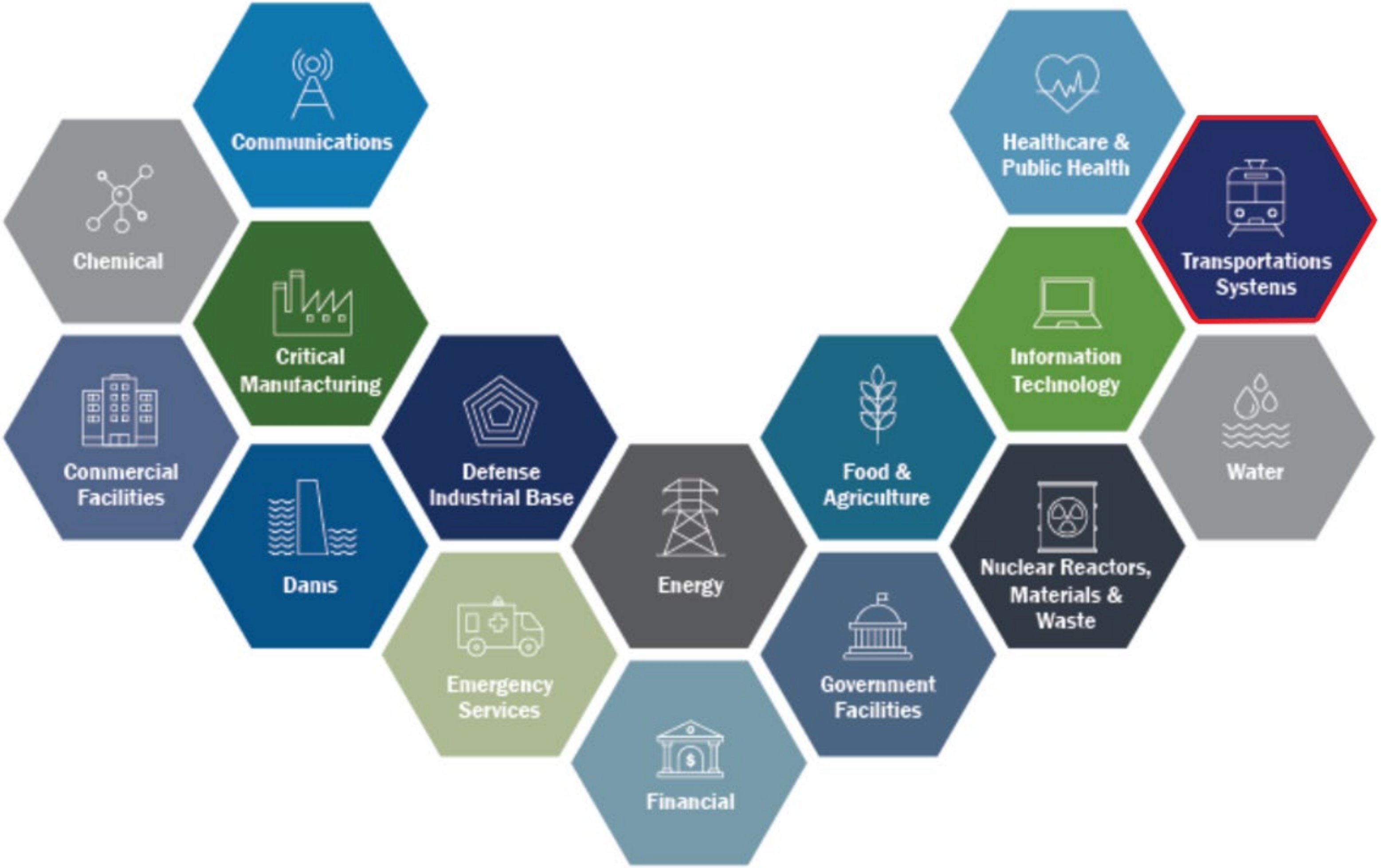
CISA mission: Lead the collaborative national effort to strengthen the security and resilience of America’s critical infrastructure

In support of that mission: Cybersecurity Advisors (CSAs):

- **Assess**: Evaluate critical infrastructure cyber risk.
- **Promote**: Encourage best practices and risk mitigation strategies.
- **Build**: Initiate, develop capacity, and support cyber communities-of-interest and working groups.
- **Educate**: Inform and raise awareness.
- **Listen**: Collect stakeholder requirements.
- **Coordinate**: Bring together incident support and lessons learned.

Critical Infrastructure Sectors

CISA assists the public and private sectors secure its networks and focuses on organizations in the following 16 critical infrastructure sectors.



Sampling of Cybersecurity Offerings

- **CISA Integrated Operations Coordinating Center (CIOCC)**
  - National CERT
    - Remote / On-Site Assistance
    - Malware Analysis
- **Cyber Security Advisors**
- **Protective Security Advisors**
- **Cyber Exercise Program**
- **User Awareness Training**

- **CISA Assessments & Evaluations**
  - Vulnerability Scanning
  - Web Application Scanning
  - Risk & Vulnerability Assessment (RVA)
  - Remote Penetration Testing (RPT)
  - Phishing Campaign Assessment (PCA)
  - Cyber Security Evaluation Tool (CSET)
- **CSA Facilitated Cyber Security Evaluations**
  - Cyber Resilience Review (CRR)
  - Cyber Infrastructure Survey (CIS)
  - External Dependencies Management (EDM) Assessment

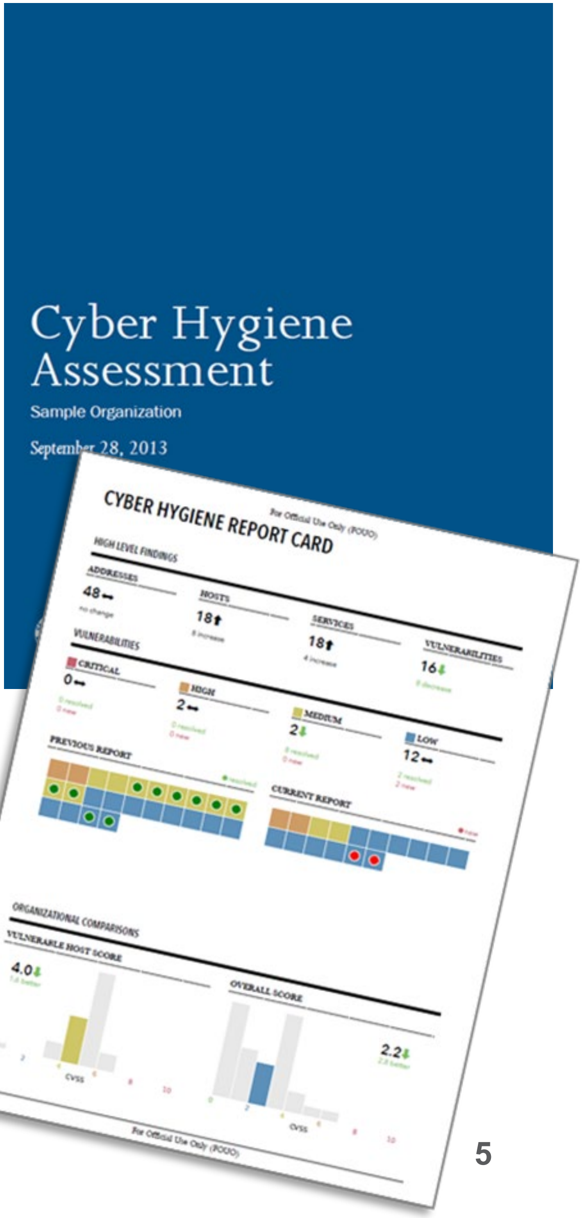
Vulnerability Scanning Service (CyHy)

Assess Internet accessible systems for known vulnerabilities and configuration errors

Work with organization to proactively mitigate threats and risks to systems

Activities include:

- Network Mapping
  - ➢ Identify public IP address space
  - ➢ Identify hosts that are active on IP address space
  - ➢ Determine the O/S and Services running
  - ➢ Re-run scans to determine any changes
  - ➢ Graphically represent address space on a map
- Network Vulnerability & Configuration Scanning
  - ➢ Identify network vulnerabilities and weakness



Cyber Hygiene Assessment

Sample Organization

September 28, 2013

CYBER HYGIENE REPORT CARD

For Official Use Only (FOUO)

HIGH LEVEL FINDINGS

ADDRESSES 48 → no change

HOSTS 18 ↑ 8 increase

SERVICES 18 ↑ 4 increase

VULNERABILITIES 16 ↓ 8 decrease

VULNERABILITIES

CRITICAL 0 → 0 resolved 0 new

HIGH 2 → 0 resolved 0 new

MEDIUM 2 ↓ 8 resolved 0 new

LOW 12 → 2 resolved 2 new

PREVIOUS REPORT

CURRENT REPORT

ORGANIZATIONAL COMPARISONS

VULNERABLE HOST SCORE 4.0 ↓ 1.6 better

OVERALL SCORE 2.2 ↓ 2.8 better

For Official Use Only (FOUO)

Web Application Scanning (WAS)

An Internet based scanning service to assess the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations.

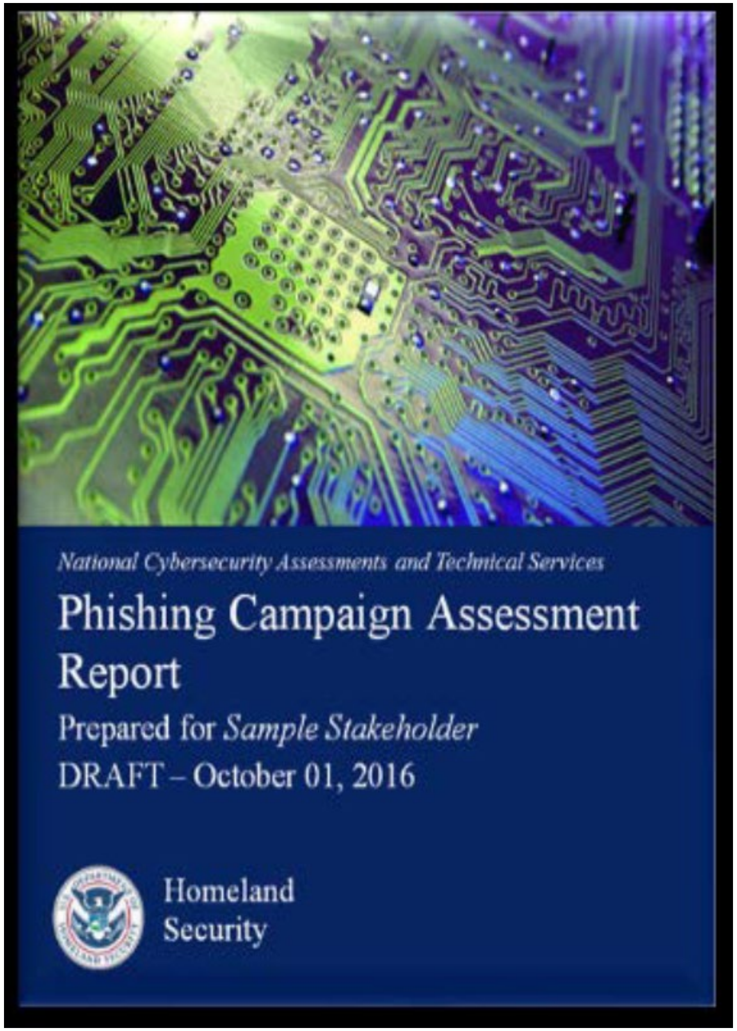
SCANNING OBJECTIVES

- Maintain enterprise awareness of your publicly accessible web-based assets
- Provide insight into how systems and infrastructure appear to potential attackers
- Drive proactive mitigation of vulnerabilities to help reduce overall risk

SCANNING PHASES

- Discovery Scanning: Identify active, internet-facing web applications
- Vulnerability Scanning: Initiate non-intrusive checks to identify potential vulnerabilities and configuration weaknesses

Phishing Campaign Assessment (PCA)



National Cybersecurity Assessments and Technical Services

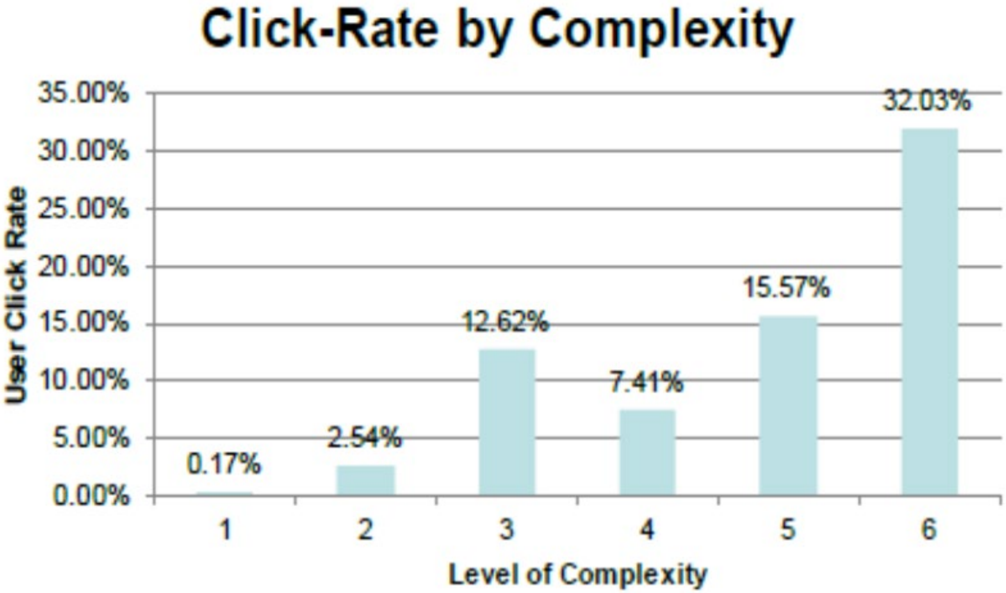
Phishing Campaign Assessment Report

Prepared for *Sample Stakeholder*

DRAFT – October 01, 2016

Homeland Security

Week	Campaign	Date Sent	Complexity Level	User Click Rate	# Emails Sent
1	Please Help!	3/18/16	1	0.17%	401
2	Reveal Your Past	3/31/16	2	2.54%	402
3	Password Expire Alert	4/6/16	3	12.62%	401
4	Severe Weather Checklist	4/15/16	4	7.41%	402
5	Federal Employee Survey	4/20/16	5	15.57%	401
6	Salary Guidelines	4/27/16	6	32.03%	402



Risk and Vulnerability Assessment (RVA)

A penetration test, or the short form pen-test, is an attack on a computer system with the intention of finding security weaknesses, potentially gaining access to it, its functionality and data.

- Involves identifying the target systems and the goal, then reviewing the information available and undertaking available means to attain the goal
- A penetration test target may be a white box (where all background and system information is provided) or black box (where only basic or no information is provided except the company name)
- A penetration test will advise if a system is vulnerable to attack, if the defenses were sufficient and which defenses (if any) were defeated in the penetration test

Remote Penetration Test (RPT)

Utilizes a dedicated remote team to assess and identify vulnerabilities and work with customers to eliminate exploitable pathways.

- Focuses on externally accessible systems

SCENARIOS:

- **External Penetration Test**: Verifying if the stakeholder network is accessible from the public domain by an unauthorized user by assessing open ports, protocols, and services.
- **External Web Application Test**: Evaluating web applications for potential exploitable vulnerabilities; the test can include automated scanning, manual testing, or a combination of both methods.
- **Phishing Assessment**: Testing through carefully crafted phishing emails containing a variety of malicious payloads to the trusted point of contact.

Cyber Security Evaluation Tool (CSET)

Purpose: Provides a detailed, effective, and repeatable tool for assessing systems security against established industry standards and guidance.

Facilitated: Self-Administered, undertaken independently

Benefits:

- Immediately available for download upon request
- Understanding of operational technology and information technology network security practices
- Ability to drill down on specific areas and issues
- Helps to integrate cybersecurity into current corporate risk management strategy

Time to Execute / Availability:

- Varies greatly (min 2 Hours) / N/A (self-assessment)

CISA
CYBER+INFRASTRUCTURE

Cyber Resilience Review (CRR)

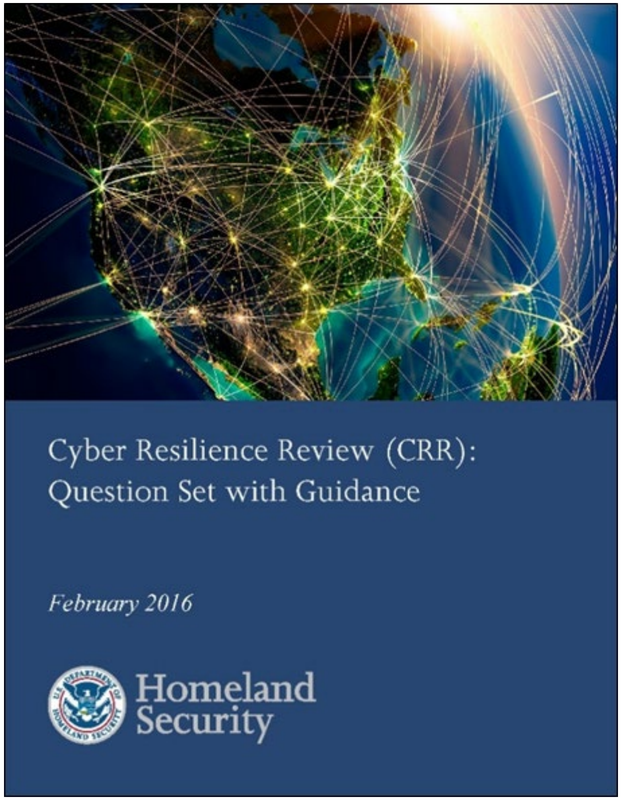
Purpose: The CRR is an assessment intended to evaluate an organization’s operational resilience and cybersecurity practices of its critical services

Delivery: The CRR can be

- Facilitated
- Self-administered

CRR Self-Assessment Package is available on the C-Cubed Voluntary Program website.

- Helps public and private sector partners understand and measure cyber security capabilities as they relate to operational resilience and cyber risk
- Based on the CERT ® Resilience Management Model (CERT® RMM)



Cyber Resilience Review (CRR):
Question Set with Guidance

February 2016

Homeland
Security

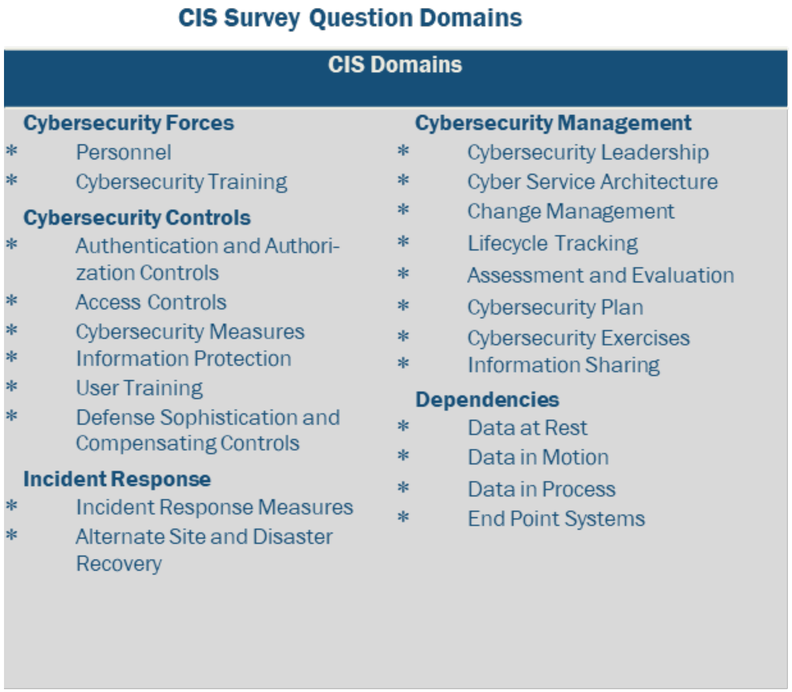
Cybersecurity Infrastructure Survey (CIS)

Structured, interview based assessment (2 ½ to 4 hours) of essential cybersecurity practices in-place for critical services within your organization

Identifies interdependencies, capabilities, and the emerging effects related to current cybersecurity posture

Focuses on protective measures, threat scenarios, and a service based view of cybersecurity in context of the surveyed topics

Broadly aligns to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)



CIS Survey Question Domains

CIS Domains

Cybersecurity Forces

* Personnel
* Cybersecurity Training

Cybersecurity Controls

* Authentication and Authorization Controls
* Access Controls
* Cybersecurity Measures
* Information Protection
* User Training
* Defense Sophistication and Compensating Controls

Incident Response

* Incident Response Measures
* Alternate Site and Disaster Recovery

Cybersecurity Management

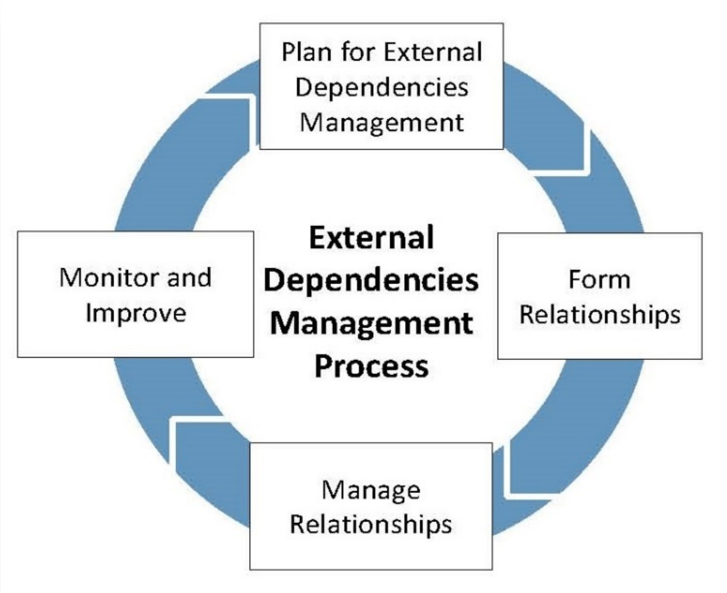
* Cybersecurity Leadership
* Cyber Service Architecture
* Change Management
* Lifecycle Tracking
* Assessment and Evaluation
* Cybersecurity Plan
* Cybersecurity Exercises
* Information Sharing

Dependencies

* Data at Rest
* Data in Motion
* Data in Process
* End Point Systems

External Dependencies Management Assessment

- **Purpose:** Evaluate an entity's management of their dependencies on third-party entities
- **Delivery:** CSA-facilitated
- **Benefits**:
    - Better understanding of the entity's cyber posture relating to external dependencies
    - Identification of improvement areas for managing third parties that support the organization

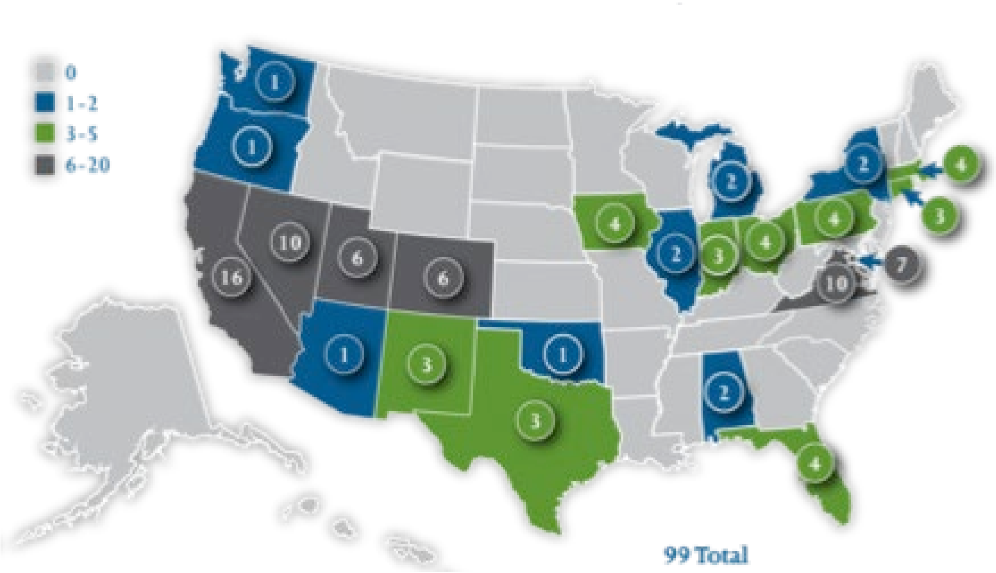

Plan for External Dependencies Management
External Dependencies Management Process
Form Relationships
Manage Relationships
Monitor and Improve

EDM process outlined per the External Dependencies Management Resource Guide

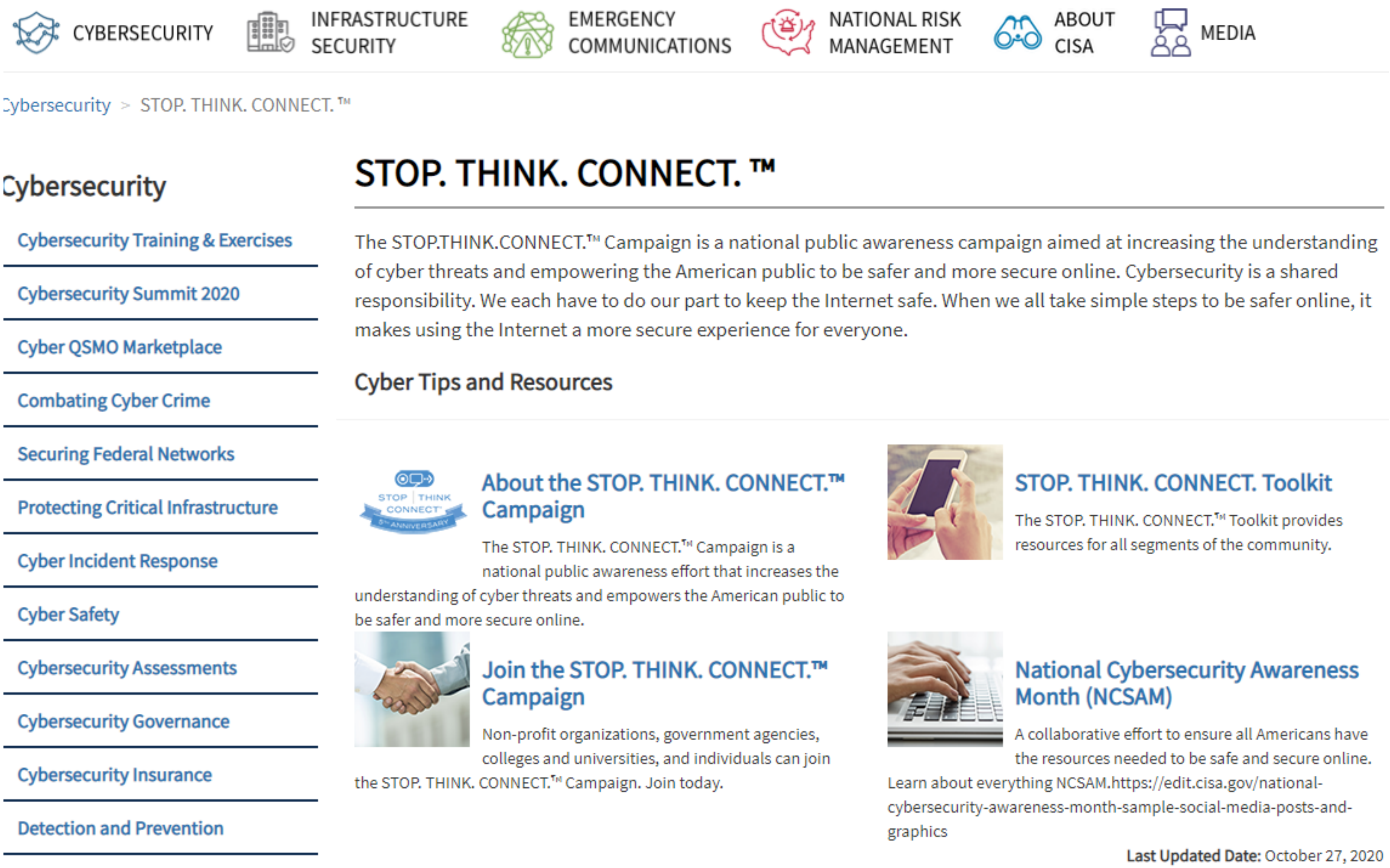
Cyber Exercises and Planning

CISA's National Cyber Exercise and Planning Program develops, conducts, and evaluates cyber exercises and planning activities for state, local, tribal and territorial governments and public and private sector critical infrastructure organizations.

- Cyber Storm Exercise – DHS's flagship national-level biennial exercise
- Exercise Planning and Conduct
- Cyber Exercise Consulting and Subject Expertise Support
- Cyber Planning Support
- Off-the-Shelf Resources



STOP. THINK. CONNECT.



Cybersecurity

- Cybersecurity Training & Exercises
- Cybersecurity Summit 2020
- Cyber QSMO Marketplace
- Combating Cyber Crime
- Securing Federal Networks
- Protecting Critical Infrastructure
- Cyber Incident Response
- Cyber Safety
- Cybersecurity Assessments
- Cybersecurity Governance
- Cybersecurity Insurance
- Detection and Prevention

STOP. THINK. CONNECT. ™

The STOP.THINK.CONNECT.™ Campaign is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. Cybersecurity is a shared responsibility. We each have to do our part to keep the Internet safe. When we all take simple steps to be safer online, it makes using the Internet a more secure experience for everyone.

Cyber Tips and Resources

About the STOP. THINK. CONNECT.™ Campaign

The STOP. THINK. CONNECT.™ Campaign is a national public awareness effort that increases the understanding of cyber threats and empowers the American public to be safer and more secure online.

STOP. THINK. CONNECT. Toolkit

The STOP. THINK. CONNECT.™ Toolkit provides resources for all segments of the community.

Join the STOP. THINK. CONNECT.™ Campaign

Non-profit organizations, government agencies, colleges and universities, and individuals can join the STOP. THINK. CONNECT.™ Campaign. Join today.

National Cybersecurity Awareness Month (NCSAM)

A collaborative effort to ensure all Americans have the resources needed to be safe and secure online. Learn about everything NCSAM.https://edit.cisa.gov/national-cybersecurity-awareness-month-sample-social-media-posts-and-graphics

Last Updated Date: October 27, 2020

https://www.cisa.gov/stopthinkconnect

Contact / Questions

Questions?

Contact:
R. S. Richard Jr.
Cybersecurity Advisor, Region II
Cybersecurity & Infrastructure Security Agency
Email: richard.richard@hq.dhs.gov
Phone: 631-241-3662