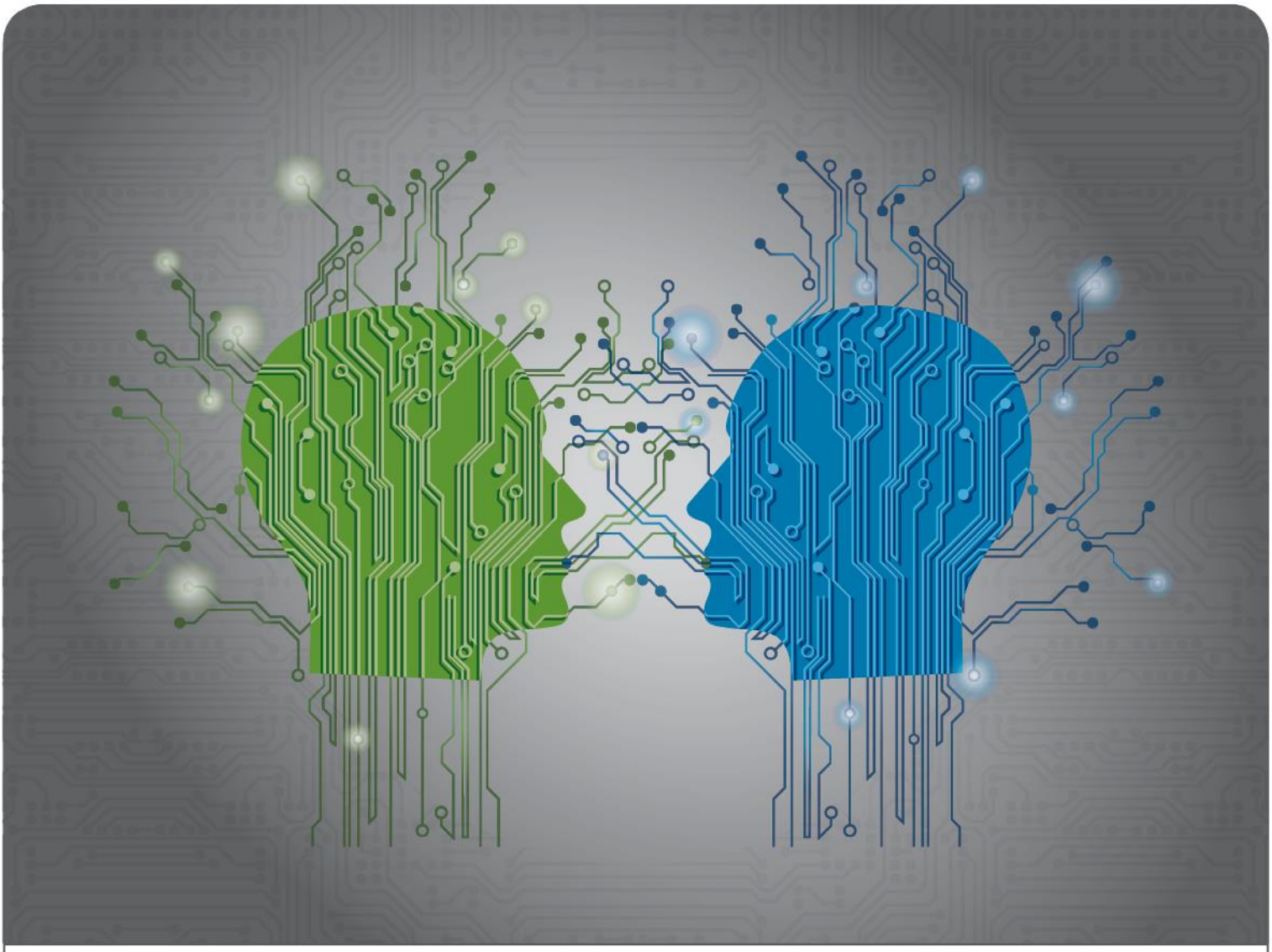

NYS Healthcare Cybersecurity Exercise
Hosted by:
Greater New York Hospital Association and Healthcare Association of New York State
After Action Report

May 5, 2017

Exercise Sensitive

HANDLING INSTRUCTIONS

This document is Exercise Sensitive. It may be disseminated on a need-to-know basis to applicable partners and stakeholders.

Control information derived from this exercise based on the sensitivity of the information as determined by the Greater New York Hospital Association (GNYHA), Healthcare Association of New York State (HANYS) (collectively the Associations), and applicable law.

The title of this document is *New York State Healthcare Cybersecurity Exercise After Action Report.*

For questions about the event or recommendations for improvement, contact:

GNYHA	HANYS
Laura M. Alfredo Senior Vice President Legal, Regulatory and Professional Affairs and Deputy General Counsel **phone:** 212-258-5391 **e-mail:** lalfredo@gnyha.org	**Susan Van Meter** Senior Vice President Federal Relations Healthcare Association of NY State **phone:** 202-488-1272 **e-mail:** Svanmete@hanys.org

EXERCISE OVERVIEW

Exercise Name	New York State Healthcare Cybersecurity Exercise
Exercise Date, Time, and Location	GNYHA and HANYS April 4, 2017, 10:00 a.m. – 2:00 p.m. 555 W. 57th Street, 15th Floor, New York, NY
Scope	This four-hour exercise explored the response and oversight activities of local, state, and federal agencies to a cybersecurity incident affecting one or more New York hospitals through facilitated discussions between hospital cybersecurity teams and regulating agencies.
Mission Area(s)	Response and Mitigation
Core Capabilities	Planning, Information Sharing, Operational Coordination, Public Messaging
Objectives	1. Level-set for agency representatives about the nature of cybersecurity threats and risk affecting the hospital sector 2. Generate discussion among the agency representatives about their respective roles and jurisdiction 3. Attempt to streamline agency response to ease administrative burden on affected hospital(s) 4. Provide a basis for future guidance for the hospital sector and relevant agencies on response activities
Threat or Hazard	Cyber
Scenario	Cyber-attacks of increasing complexity resulting in integrity issues with patient record data, a significant malware incident affecting medical devices nationally, and ransomware.
Sponsor	Greater New York Hospital Association Healthcare Association of New York State

Participating Organizations

- Private Sector:
  - Interfaith Medical Center
  - Mount Sinai Hospital
  - New York Presbyterian Hospital
  - New York University Langone Medical Center
  - Northwell Health
  - Noyes Memorial Hospital
  - Richmond University Medical Center
  - University of Rochester Medical Center
  - Greater New York Hospital Association (GNYHA)
  - Healthcare Association of New York State (HANYS)
- Federal:
  - Department of Health and Human Services Assistant Secretary for Preparedness and Response
  - Federal Bureau of Investigation (NY Joint Cyber Task Force)
  - Department of Homeland Security National Cyber Exercise Planning Program
- State:
  - Governor's Office, Assistant Secretary for Cyber Response
  - New York State Division of Homeland Security and Emergency Services - Office of Emergency Management (NYSDHSES/ OEM)
  - New York State Department of Health (DOH)
  - New York State Police Cyber Analysis Unit
  - New York State Office of Mental Health (OMH)
  - New York State Office of Alcoholism and Substance Abuse Services (OASAS)
  - New York State Office for People with Developmental Disabilities (OPWDD)
- City:
  - New York City Department of Health and Mental Hygiene (NYCDOHMH)
  - New York City Police Department

Exercise Evaluation and Improvement Planning

This report consists of observations based on exercise objectives. Observations and related recommendations in this after action report (AAR) are based on an analysis of exercise discussions, participants' key observations, and feedback forms completed by the participants.

Appendix A contains an "Improvement Plan" listing observations, associated recommendations for improvement, with space to identify corrective actions, responsible organizations/offices, points of contact (POCs), and target start and completion dates for each item. The appendix is a suggested method for tracking areas for improvement to completion and provides a basis for a lessons learned, best practices database. How you use the information in this report is entirely at your discretion.

Summary of Key Observations

Participants met exercise objectives and identified several observations:

- Agency guidelines should address the potential effects of cyber incidents on patient care and the healthcare system, identify the State's cyber response capabilities, the regulatory relief available to association members during a cyber response, or the type of information members should provide to agencies during and after an incident..
- Association members may benefit from a severity schema that provides a standardized process for assessing the impact of a cyber incident on institutions and the sector.
- It was unclear how and under what circumstances association members share cybersecurity threat information within the sector.
- The Associations should consider developing best practices guidelines for procuring and managing software and equipment being connected to IT networks.
- A cyber-induced incident at a healthcare facility can generate significant public attention. Coordinating public information between healthcare organizations and government agencies may be required to maintain public trust.

ANALYSIS OF OBSERVATIONS

Observation 1:

Agency guidelines do not address the potential effects of cyber incidents on patient care and the healthcare system, identify the State's cyber response capabilities, the regulatory relief available to association members during a cyber response, or the type of information members should provide to agencies during and after an incident.

The healthcare sector is embracing and expanding its reliance on cyber-based record systems, medical devices, and diagnostic equipment; rendering it vulnerable to a range of cyber disruptions. The consequences of a cyber incident on a single system, network, or device could have affects far outside the affected system. The time needed to identify, respond to, mitigate, and recover from a cyber incident may require providers to employ alternative care and records management protocols beyond "normal" recovery times, possibly affecting patient care.

Additionally, cyber incidents may generate multiple calls to oversight agencies concerning patient care or hospital operations. Agencies investigate each report as an individual incident. If a cyber incident was the root cause of the reports, this methodology could lead to unwarranted disciplinary actions. Guidelines for assessing the severity of a cyber incident and its effect on patient and healthcare operations could improve incident management activities for state agencies and association members.

A listing of cyber and non-cyber resources available help association members respond to an incident and defined procedures for requesting assistance or regulatory relief would be helpful.

Recommendation 1:

The Associations, state, and local agencies should collaborate to develop criteria to assess and manage cyber incidents affecting the healthcare sector, and identify the cyber and non-cyber resources available to members during a cyber response.

Observation 2:

Association members may benefit from a severity schema that provides a standardized process for assessing the impact of a cyber incident on institutions and the sector.

An impact-based cyber incident severity schema is included in the National Cyber Incident Response Plan. The schema identifies conditions, at the national level, that warrant a higher level of scrutiny, reporting, and response. The State of New York Emergency Management Agency has modified that schema to address state cyber incidents.

Recommendation 2:

Develop severity schemas tailored to assess the impacts of cyber incidents on member organizations.

Additionally, the Associations should consider linking the schemas to the state's cyber severity schema. This would allow state emergency managers to use standardized impact assessments to prioritize state assistance.

Observation 3:

It was unclear how, and under what circumstances, association members share cybersecurity threat information within the sector.

In the scenario presented, multiple healthcare providers were attacked using similar tactics, techniques and procedures. Though specifically avoided during the exercise, this scenario could indicate a coordinated, sector-wide attack. All participants stated they would notify law enforcement agencies when appropriate; however, participants appeared reluctant to share information with other healthcare providers in the state. Federal and state agency policies favor responding to widespread incidents as the best use of limited resources. Keeping the information in-house masks the extent of sector attacks and could delay or limit federal, state, and law enforcement response to a serious cyber incident.

Recommendation 3:

The Associations should explore ways to encourage their members to share cybersecurity information with other association members while an incident is occurring. Whether through automated information sharing programs or "alerts" issued by the Associations in coordination with the affected institution, sharing known tactics, techniques, and procedures (TTP) while an incident is in progress reduces everyone's risks.

Observation 4:

The Associations should consider developing best practices guidelines for procuring and managing software and equipment being connected to IT networks.

The variety of IT based systems and equipment used to coordinate and manage patient care creates significant cybersecurity risks if not effectively managed. Coordinating purchases through IT departments ensures software and equipment added to the network is compatible with the network, and that the vendor's update policies meet network standards.

Recommendation 4:

The Associations should consider creating IT best practices folios that members can tailor to their individual needs.

Observation 5:

A cyber-induced incident at a healthcare facility can generate significant public attention; requiring a coordinated communications strategy to maintain public trust.

Adverse information on social media, regardless of accuracy, can affect the public's confidence in the organization, and in some cases, put the organization's future at risk. Accurate, verifiable, and timely information from official sources can correct the record, but only if all involved agencies provide the same information.

Although this may not be an issued for a single organization dealing with an isolated incident, a cyber incident affecting multiple organizations simultaneously increases the risk of public information offices releasing conflicting information to the media. This could create a situation that erodes public confidence in the affected organizations, supporting government agencies, and the sector as a whole.

Recommendation 5:

The Associations should discuss the concept of coordinating the release of information to the public with affected healthcare facilities member associations, and government agencies with their members.

CONCLUSION

This tabletop exercise allowed private sector healthcare organizations to discuss cyber-incident response and recovery issues with the public sector agencies providing oversight and support.

Objective 1: Level-set for agency representatives about the nature of cybersecurity threats and risk affecting the hospital sector.

Healthcare providers discussed the range of cyber threats, their potential to interfere with patient care or compromise patient privacy, and their policies for responding to cyber incidents. The potential scale of cyber-induced patient care degradation presented in the exercise provided public sector participants a filter to re-evaluate their planning assumptions. All participants agreed the current regulatory guidance fails to address adequately the unique characteristics of cyber incidents.

Objective 2: Generate discussion among the agency representatives about their respective roles and jurisdiction.

Detailed discussions ensued on the various agencies' responsibilities during a cyber incident affecting patient care. A key result is that participants agreed the agency should de-emphasize its customary role of compliance assessment during a significant cyber incident and focus on coordinating state assistance, as needed.

Objective 3: Attempt to streamline agency response to ease administrative burden on affected hospital(s).

All participants agreed that existing guidance for reporting and supporting cybersecurity incidents is inadequate. Agencies agreed to work with the Associations to develop cyber-specific guidance aimed at reducing administrative burdens. Additionally, they will provide information on how organizations can request available government resources.

Objective 4: Provide a basis for future guidance for the hospital sector and relevant agencies on response activities.

The exercise allowed participants to explore issues, voice concerns, and propose ways to address future challenges in a collaborative environment. The Associations and agencies agreed to prioritize the issues and begin a series of meetings and working groups to develop mutually beneficial policies and guidelines for cybersecurity incidents within the sector.

APPENDIX A: IMPROVEMENT PLAN

The Improvement Plan is a tool to help participating agencies track the implementation of recommendations and corrective actions for each area for improvement identified in the exercise. Its use is voluntary. If used, stakeholders should collaborate to identify corrective actions, responsible components, points of contact (POCs), and target start and completion dates for each item.

OBSERVATION: Agency guidelines do not address the potential effects of cyber incidents on patient care and the healthcare system, identify the State's cyber response capabilities, the regulatory relief available to association members during a cyber response, or the type of information members should provide to agencies during and after an incident.					
Recommendation	**Corrective Action**	**Primary Responsible Component**	**POC**	**Start Date**	**Completion Date**
1. The Associations, state and local agencies develop criteria to:					
a. Assess and manage cyber incidents.					
b. Determine a "needs based" policy for providing state assistance.					
c. Identify the cyber and non-cyber resources available to members during a cyber response.					

OBSERVATION: The Associations, state, and local agencies should collaborate to develop criteria to assess and manage cyber incidents affecting the healthcare sector, and identify the cyber and non-cyber resources available to members during a cyber response.					
Recommendation	**Corrective Action**	**Primary Responsible Component**	**POC**	**Start Date**	**Completion Date**
1. Develop severity schemas tailored to assess the impacts of cyber incidents on member organizations.					

OBSERVATION: It was unclear how and under what circumstances association members share cybersecurity threat information within the sector.					
Recommendation	**Corrective Action**	**Primary Responsible Component**	**POC**	**Start Date**	**Completion Date**
1. Explore ways to encourage information sharing among association members.					
2. Identify platforms smaller organizations can use to obtain current threat information at low, or no cost.					
3. Evaluate the value of using Association resources to share attacker tactics, techniques and procedures with association members during and incident.					

OBSERVATION: Association's should consider developing best practices guidelines for procuring and managing software and equipment being connected to IT networks.					
Recommendation	**Corrective Action**	**Primary Responsible Component**	**POC**	**Start Date**	**Completion Date**
1. The Associations should consider creating IT best practices folios that members can tailor to their individual needs.					

OBSERVATION: A cyber-induced incident at a healthcare facility can generate significant public attention; requiring a coordinated communications strategy to maintain public trust.					
Recommendation	**Corrective Action**	**Primary Responsible Component**	**POC**	**Start Date**	**Completion Date**
1. The Associations should discuss the concept of coordinating the release of information to the public with affected healthcare facilities member associations, and government agencies with their members.					

APPENDIX B: PARTICIPATING ORGANIZATIONS

Organization
Private Sector:
Interfaith Medical Center
Mount Sinai Hospital
New York Presbyterian Hospital
New York University Langone Medical Center
Northwell Health
Noyes Memorial Hospital
Richmond University Medical Center
University of Rochester Medical Center
Greater New York Hospital Association (GNYHA)
Healthcare Association of New York State (HANYS)
Federal:
Department of Health and Human Services Assistant Secretary for Preparedness and Response
Federal Bureau of Investigation (NY Joint Cyber Task Force)
Department of Homeland Security National Cyber Exercise Planning Program
State:
Governor's Office, Assistant Secretary for Cyber Response
New York State Division of Homeland Security and Emergency Services- Office of Emergency Management (NYSDHSES/ OEM)
New York State Department of Health (DOH)
New York State Police Cyber Analysis Unit
New York State Office of Mental Health (OMH)
New York State Office of Alcoholism and Substance Abuse Services (OASAS)
New York State Office for People with Developmental Disabilities (OPWDD)
City:
New York City Department of Health and Mental Hygiene (NYCDOHMH)
New York City Police Department

APPENDIX C: FEEDBACK FORM ANALYSIS

Nine participants provided written feedback on the exercise. The tables below are consolidated listings of their observations and recommendations. Where appropriate, their comments are incorporated in the observations listed above.

Exercise Design

Participants rated exercise design according to specific assessment factors identified in the charts below. The aggregated and averaged results (shown in the "Mean" column) of each factor are below.

Assessment Factor	Strongly Disagree				Strongly Agree	Mean
	1	2	3	4	5	
Pre-exercise briefings were informative and provided the necessary information for my role in the exercise	0	0	1	3	4	*4.375
The exercise scenario was plausible and realistic	0	0	0	1	7	4.5
Exercise participants included the right people in terms of level and mix of disciplines	0	0	1	2	5	4.5
Exercise participation was appropriate for someone in my field with my level of experience/training	0	0	0	2	6	4.75
Exercise Objectives						
Level-set for agency representatives about the nature of cybersecurity threats and risk affecting the hospital sector	0	0	0	7	2	4.0
Generate discussion among the agency representatives about their respective roles and jurisdiction	0	0	0	3	6	4.66
Attempt to streamline agency response to ease administrative burden on affected hospital(s)	0	1	2	3	3	4.0
Provide a basis for future guidance for the hospital sector and relevant agencies on response activities	0	0	0	7	2	4.0

Previous Exercise Experience				
Number of Exercises	0	1-5	5-10	15+
Number of Participants	2	7	1	0
Exercise Role**				
Role	Player	Facilitator/Controller	Observer	Evaluator
Number of Participants	5	0	6	0

*Only eight participants provided feedback for this section
**Some participants reported multiple roles

Participant Feedback

Participants' comments on the exercise's strengths, areas for improvement, quality of exercise materials, and suggestions for future exercises are listed below. Similar comments were consolidated into a single bullet point

1. **Areas Identified as Strengths by Participants:**
    - Running through realistic scenarios generated valuable discussions between the private and public sectors.
    - Hearing how other organizations respond to cyber incidents and the role of government agencies during a cyber incident was helpful.
    - The discussions raised very important issues to bring back to my agency for review.
    - Participants were a good mix of experts in their fields.
    - The exercise increased my knowledge of healthcare sector customers and their expectations and limitations.
    - The discussion questions encouraged active engagement.
    - Scenarios covered a wide array of the threats hospitals faced.
2. **Areas Identified for Improvement:**
    - More discussions about threat intelligence sharing, resource sharing, and standards for deploying medical equipment would be helpful.
    - The topic areas needed more development.
    - Some redirection when people go way off target would be helpful.
    - NYC is tough to get to for many participants. Suggest Westchester County area next time.
    - Include a discussion on cybersecurity threat vectors, best practices for protecting key areas, and mitigating an attack.
    - Re-evaluate inclusion of regulators. This may discourage hospitals from actively participating.
3. **Most Useful Exercise Materials:**
    - All materials were equally useful.
4. **Recommendations for Improvement or Enhancement of this or Future Exercises:**
    - Have more exercises of this type, maybe tailored for junior employees.
    - Have high-level discussion on best practices and communications models healthcare should follow.
    - Establish a forum with my particular hospital on a similar tabletop discussion on cybersecurity.
    - Identify some best practices on communication among the various sectors and agencies.
    - Play out the severity schema and National Cyber Incident Response Plan more. Who or what determines severity level. What is the state/federal response?

APPENDIX D: ADDITIONAL RESOURCES AND CYBERSECURITY DOCTRINE

Principal Doctrine

Presidential Policy Directive – United States Cyber Incident Coordination (PPD-41)
https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

Comprehensive National Cybersecurity Initiative (CNCI)
https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative

Cybersecurity: Authoritative Reports and Resources (Congressional Research Service)
http://www.fas.org/sgp/crs/misc/R42507.pdf

Cyberspace Policy Review
https://obamawhitehouse.archives.gov/cyberreview/documents/

National Cyber Incident Response Plan (NCIRP) (2016)
https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

Executive Order: Improving Critical Infrastructure Cybersecurity (2013)
https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Framework for Improving Critical Infrastructure Cybersecurity (2014)
http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Homeland Security Presidential Directive (HSPD 7)
https://www.dhs.gov/homeland-security-presidential-directive-7

National Institute of Standards and Technology Computer Security Incident Handling Guide
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

National Strategy for Trusted Identities in Cyberspace (2011)
https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

National Preparedness Goal (2016)
https://www.fema.gov/national-preparedness-goal

National Strategy to Secure Cyberspace (2003)
https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (2013)
https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

Department of Homeland Security

Cyber Capabilities/Entities

National Cybersecurity and Communications Integration Center (NCCIC) (contact: NCCIC@hq.dhs.gov)
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (contact: ics-cert@hq.dhs.gov; 877-776-7585)
- National Coordinating Center for Communications (NCC) (contact: NCC@hq.dhs.gov; 703-235-5080)
- United States Computer Emergency Readiness Team (US-CERT) (contact: info@us-cert.gov; 888-282-0870)

National Infrastructure Coordinating Center (contact: NICC@hq.dhs.gov)

Resources/Documents

Cyber Storm V Final Report
https://www.dhs.gov/sites/default/files/publications/CyberStormV_AfterActionReport_2016vFinal-%20508%20Compliant%20v2.pdf

DHS Blueprint for a Secure Cyber Future
http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf

DHS Memorandum of Agreement with Department of Defense
http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf

DHS Quadrennial Homeland Security Review
https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf

DHS Strategic Plan Fiscal Years 2014-2018
https://www.dhs.gov/sites/default/files/publications/FY14-18%20Strategic%20Plan.PDF

Enabling Distributed Security in Cyberspace
http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf

ICS-CERT Incident Response Summary Report 2009-2011
http://ics-cert.us-cert.gov/sites/default/files/documents/ICS-CERT%20Incident%20Response%20Summary%20Report%20%282009-2011%29.pdf

National Infrastructure Protection Plan (NIPP) 2013
http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

National Response Framework (NRF) 2016
http://www.fema.gov/national-response-framework

Protected Critical Infrastructure Information (PCII) Program Fact Sheet
https://www.dhs.gov/publication/pcii-fact-sheet

Testimony of National Cybersecurity and Communications Integration Center Director Seán P. McGurk, National Protection and Programs Directorate, before the U.S. House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, "The DHS Cybersecurity Mission: Promoting Innovation and Securing Critical Infrastructure"
http://www.dhs.gov/ynews/testimony/testimony_1302814781943.shtm

Written testimony of Department of Homeland Security Secretary Janet Napolitano for a Senate Committee on the Judiciary hearing titled "The Oversight of the Department of Homeland Security"
http://www.dhs.gov/ynews/testimony/20120425-s1-dhs-oversight-sjc.shtmn

State Government

Cyber Capabilities/Entities

Multi-State Information Sharing & Analysis Center (MS-ISAC) https://msisac.cisecurity.org/ contact: info@msisac.org; 518-266-3460

Resources/Documents

National Association of State Chief Information Officers (NASCIO) http://www.nascio.org/

MS-ISAC Charter https://msisac.cisecurity.org/documents/Charter.pdf

MS-ISAC Cybersecurity Guides https://msisac.cisecurity.org/guidelines/

Robert T. Stafford Disaster Relief and Emergency Assistance Act http://www.fema.gov/media-library-data/1383153669955-21f970b19e8eaa67087b7da9f4af706e/stafford_act_booklet_042213_508e.pdf

Private Sector/Business

Cyber Capabilities/Entities

Business Executives for National Security http://www.bens.org/

Critical Infrastructure Sector Partnerships https://www.dhs.gov/critical-infrastructure-sector-partnerships

Electronic Privacy Information Center http://epic.org/

Information Sharing and Analysis Centers (ISACs) https://www.it-isac.org/

Internet Security Alliance http://www.isalliance.org/

National Council of ISACs https://www.nationalisacs.org/

National Health – Information Sharing and Analysis Center https://nhisac.org

Resources/Documents

Commonsense Guide to Cyber Security for Small Businesses (U.S. Chamber of Commerce) http://www.ready.gov/sites/default/files/documents/files/security_for_small_business%5B1%5D.pdf

The Financial Management of Cyber Risk (ANSI and Internet Security Alliance) http://publicaa.ansi.org/sites/apdl/khdoc/Financial+Management+of+Cyber+Risk.pdf

The Role of ISACs in Private/Public Critical Infrastructure Protection http://www.isaccouncil.org/images/ISAC_Role_in_CIP.pdf

Verizon Data Breaches Investigations Report (2016) http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/