Louisiana Healthcare Cyber Tabletop Exercise

Well-Ahead Louisiana

May 23, 2023

Cybersecurity and Infrastructure Security Agency

Table of Contents

Handling Instructions (TLP:CLEAR)

The title of this document is Louisiana Healthcare Cyber Tabletop Exercise Situation Manual (SitMan). This document is unclassified and designated as *"Traffic Light Protocol (TLP):CLEAR"*: Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. **Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction.**

This document may be disseminated publicly pursuant to TLP:CLEAR and Well-Ahead Louisiana guidelines.

For questions about this event or recommendations for improvement contact: Nicole Coarsey, Healthcare Access Division Manager of Well-Ahead Louisiana at 225-342-1583 or Nicole.coarsey@la.gov.

Exercise Overview

Exercise Name	Louisiana Healthcare Cyber Tabletop Exercise	
Exercise Date, Time, and Location	May 23, 2023 1:00 p.m. – 4:00 p.m. Central Daylight Time (CDT) Virtual via Zoom	
Exercise Schedule	**Time**	**Activity**
	1:00 p.m. – 1:05 p.m.	Welcome and Opening Remarks
	1:05 p.m. – 1:20 p.m.	Threat Briefing
	1:20 p.m. – 1:25 p.m.	Exercise Overview
	1:25 p.m. – 2:05 p.m.	Module 1
	2:05 p.m. – 2:10 p.m.	Break
	2:10 p.m. – 2:55 p.m.	Module 2
	2:55 p.m. – 3:05 p.m.	Break
	3:05 p.m. – 3:50 p.m.	Module 3
	3:50 p.m. – 4:00 p.m.	Hotwash and Closing Comments
Scope	3-hour facilitated, discussion-based tabletop exercise	
Purpose	Examine the coordination, collaboration, information sharing, and response capabilities of rural healthcare facilities in response to a cyber incident.	
NIST	Identify, Protect, Detect, Respond and Recover	
Objectives	1. Examine the ability of rural healthcare facilities to respond to 2. and recover from a significant cyber incident. 3. Discuss the impacts of a cyber incident on patient care and operations. 4. Assess rural healthcare facilities' cybersecurity training program. 5. Explore rural healthcare facilities' processes for information sharing, communications, and business continuity during a cyber incident. 6. Analyze rural healthcare facilities' third-party vendor and patch management programs.	
Threat or Hazard	Cyber	
Scenario	A threat actor targets rural healthcare facilities' employees through phishing emails. Imaging equipment, patient records, and other hospital equipment begin malfunctioning/displaying incorrect data. Rural healthcare facilities operations are reduced, PHI data is exfiltrated, and ransomware compromises computer systems and equipment, followed by social media backlash and media inquiries.	

Exercise Name	Louisiana Healthcare Cyber Tabletop Exercise	
Sponsor	Well-Ahead Louisiana	
Participating Organizations	Louisiana Department of Health (Well-Ahead Louisiana), Rural Health Clinics, Federally Qualified Health Centers, Nursing Homes, Critical Access Hospitals, U.S. Department of Health and Human Services (HHS), Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center	
Points of Contact	**Well-Ahead Louisiana** Nicole Coarsey Nicole.Coarsey@la.gov Amanda Triche Amanda.triche@la.gov	**National Cyber Exercise Program (NCEP)** CEP@hq.dhs.gov

General Information

Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

Players have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
Observers do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
Facilitators provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members may also assist with facilitation as subject matter experts (SMEs) during the exercise.
Note-takers are assigned to observe and document exercise activities. Their primary role is to document player discussions, including how and if those discussions conform to plans, policies, and procedures.

Exercise Structure

This exercise will be a multimedia, facilitated exercise. Players will participate in the following:

- Cyber threat briefing
- Scenario modules:
    - Module 1: A cybersecurity alert for healthcare organizations, a suspicious 401(k) email, unusual network traffic, and an unannounced visit by a vendor.
    - Module 2: 401(k)-management vendor was compromised by a cyberattack, imaging equipment is malfunctioning, patient records are displaying incorrect data, infusion pumps are faulty, and patient families critique the hospital online.
    - Module 3: A ransomware message locks organization equipment, patients are solicited with their stolen data, local news stations ask for comment, patients request transfers to other hospitals along with their records.
- Hotwash

Exercise Guidelines

- This exercise will be held in an open, no-fault environment. Varying viewpoints are expected.
- Respond to the scenario using your knowledge of existing plans and capabilities, and insights derived from your training and experience.
- Decisions are not precedent setting and may not reflect your organization's final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions and/or suggested actions to resolve or mitigate a problem.
- There is no hidden agenda, and there are no trick questions. The resources and written materials provided are the basis for discussion.

- The scenario has been developed in collaboration with subject matter experts and exercise planners from your organization.
- In any exercise, assumptions and artificialities are necessary to complete play in the time allotted, to achieve training objectives, and/or account for logistical limitations. Please do not allow these considerations to negatively impact your participation in the exercise.

Exercise Hotwash and Evaluation

The facilitator will lead a hotwash with participants at the end of the exercise to address any ideas or issues that emerge from the exercise discussions.

Module 1

Day 1

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS) release a joint alert regarding a rise in cyberattacks targeting healthcare organizations. The alert describes the tactics, techniques, and procedures used by cyber criminals, including phishing emails, ransomware, remote hacking, distributed denial of service attacks (DDoS), and data exfiltration from healthcare organizations.

Day 9

Many employees receive an email from your company's 401(k) manager advising them of pending account changes and instructing recipients to click the link for more details. Employees that click on the link are taken to the website and are required to enter their credentials for access.

Some employees contact Human Resources (HR)/Benefits asking why the changes have been made. HR/Benefits are unaware of any changes to the 401(k) and requests a copy of the email.

Day 10

During a routine review, the Information Technology (IT) Department discovers the network logs show an abnormally high volume of traffic during non-business hours. It is determined most of this traffic is outbound and being sent to unknown Internet Protocol (IP) addresses.

Day 21

A third-party electronic medical record (EMR) vendor shows up unannounced at your facility to update equipment. The vendor needs to patch a recently discovered vulnerability in software used on several devices, including workstations, imaging and radiology equipment, bedside monitors, and other clinical devices.

Discussion Questions

1. What is the greatest cybersecurity risk to your facility?
2. What cyber threat information do you receive?
    a. How do you collect and share this information?
    b. Who is responsible for collecting and disseminating this information?
    c. What information is most actionable?
3. What cybersecurity training does your facility provide your staff?
    a. How often must they complete this training?
    b. What happens if the training is not completed?
    c. Who is required to complete this training?
4. What essential functions depend on information technology, and what are the effects throughout the facility if they are disrupted?
5. How do employees report suspicious emails?
6. Describe your patch management and cybersecurity protocols for third-party technology vendors.
    a. How do vendors notify you that maintenance and updates are required?
    b. How do you communicate your cybersecurity concerns to your vendors?

   c. What cybersecurity language is included within your vendor contracts?
7. How regularly are users required to change their passwords?
   a. What is your account lockout policy if users don't change their passwords in a timely fashion?
   b. What are the facility's requirements for password length and level of complexity?

Module 2

Day 35

Your 401(k)-management vendor notifies you that they were recently the target of a malware attack that compromised their business email. They confirm the email your employees received came from their system but was not sent by them. They also confirm that the site accessed through the link in the spoofed email was not legitimate.

Day 47 – Morning

Technicians begin reporting the imaging equipment is not performing properly. They report blurred images, incorrectly formatted images, and images containing incorrect patient data.

Day 47 – Mid-Morning

Nurses on the floor report that patient records are displaying incorrect information about medication, diagnoses, and personal information.

Day 47 – Afternoon

Staff discover bedside monitor data is inaccurate and the infusion pumps are not operating properly and are failing to deliver infusions at the correct rate.

Day 49

Several patients' families overhear hospital staff talking about the problems with medical records and infusion pumps and demand to know if the issues are affecting their family members. They begin posting on social media about the issues the hospital is experiencing and wondering just how safe it is to be there.

Discussion Questions

1. How would you rate the severity of these events?
    a. What are your priorities? What do you do first?
2. Describe the decision-making process for responding to a cyber incident.
    a. What options are available?
    b. What options are documented in plans?
    c. Do you have a response team you can activate?
        i. How are they activated?
3. What processes are used to contact critical personnel at any time, especially outside of business hours?
    a. How does the facility proceed if critical personnel are unreachable or unavailable?
4. How are your EMR, EHR, and business data backed up?
5. What alternative systems or manual processes are available to continue operations if a critical system is unavailable for a significant period?
    a. Who can authorize use of alternate systems or procedures?
    b. At what point would they be initiated?

6. How do you respond to social media posts about these events?
    a. What does your organization do to monitor social media?
    b. What is your social media policy for employees?

Module 3

Day 58

Hospital staff start experiencing issues with their computers freezing, and work devices begin shutting down. When devices restart, employees are locked out of their machines and their screens display a ransomware message that reads:

> "Hello! Your files have been encrypted, but do not fear because for the sum of $250,000 in cryptocurrency, your files will be returned. The decryption key will expire in 72 hours. Please submit payment to the wallet below or you will not be able to recover your files."

Day 60

Current and former patients contact the hospital saying they have been called by people claiming to have access to their medical records and offering to return them for a fee. The patients are given enough information to verify the callers have their records.

Patients say the fees range from a few hundred dollars to more than a thousand and are demanding to know how these individuals could have their records.

Some say they have contacted law enforcement; others have contacted the media. Many are threatening to sue. Others are posting about the incident on social media.

Day 61

Local news stations contact the hospital for comment and some stations arrive at the hospital to begin live broadcasts for the evening news.

Day 63

Patients begin requesting transfers to other local hospitals, as they feel unsafe. They also demand the return of all their medical records, as well as the removal of them from your network. They state that neither they nor their families will be treated in your facilities again.

Discussion Questions

1. What is the decision-making process for responding to ransomware?
    a. What actions would be taken based on your incident response plan?
    b. Do you have a cyber insurance policy? What does it cover?
    c. What are the advantages/disadvantages to agreeing/refusing to pay?
    d. What are the potential legal and reputational ramifications?
2. What concerns would arise with the discovery of protected health information (PHI) of patients being available to unauthorized personnel?
    a. Does the loss of PHI affect your decision to pay the ransom?
3. At what point do you contact law enforcement during a cyber incident?
4. Where does your facility store backups of vital records? Are your backups stored in a location that is separated from your primary working copies of your files?
    a. How long do you keep copies of archived files backed up?

   b. How long of a downtime would exist between loss of your primary files and the restoration of files via your backup?
5. Who is responsible for public information dissemination related to the incident? What training or preparation have they received?
   a. Who would the public relations team contact in the event of an incident?
   b. How are these contacts prioritized?
6. What are your concerns with regards to these events impacting your facility's reputation in the community?

Appendix A: Acronyms

Acronym	Definition
CISA	Cybersecurity and Infrastructure Security Agency
DDOS	Distributed Denial of Service Attack
DHS	U.S. Department of Homeland Security
EHR	Electronic Health Record
EMR	Electronic Medical Record
FBI	Federal Bureau of Investigation
HHS	U.S. Department of Health and Human Services
HR	Human Resources
IT	Information Technology
PHI	Protected Health Information
SITMAN	Situation Manual
TLP	Traffic Light Protocol
TTX	Tabletop Exercise

Appendix B: Case Studies

Ransomware

University of Vermont Medical Center Ransomware

On October 28, 2020, the University of Vermont (UVM) Medical Center information technology (IT) desk received dozens of calls from staff complaining of computer access problems. When staff began investigating for malicious software, they found a file with instructions to contact the alleged perpetrators of the cyberattack. To prevent further damage, the UVM Center locked down email, internet access, and major chunks of the organization's computer network.

As a result of the shutdown, UVM Medical Center employees couldn't use electronic health records, payroll programs, and other vital digital tools nearly a month. For days, staff didn't even know which patients were scheduled for appointments. Urgent surgeries were rescheduled, and cancer patients had to go elsewhere for radiation treatment.

The Center did not pay the ransom, but the attack still cost an estimated $50 million, mostly from lost revenue, says UVM Health Network Chief Medical Information Officer Doug Gentile, MD. It took IT staff three weeks of working 24/7 to scrub network systems and restore capability to the thousands of affected computers.[1]

Universal Health Services Ransomware

Universal Health Services (UHS) operates 400 hospitals and behavioral health facilities in the United States and United Kingdom and, in September 2020, a cyberattack wiped out all its IT systems.

Phone systems were no longer functioning and, without access to computers and electronic health records, employees had to resort to pen and paper to record patient information. Initially, the health system was forced to divert ambulances to alternative facilities and some elective procedures were either postponed or transferred elsewhere. Patients also reported delays receiving test results while UHS recovered from the attack.

While UHS worked quickly to restore its information technology infrastructure, the recovery process still took nearly three weeks. Naturally, this disruption also entailed a major financial impact: the UHS quarterly earnings report for Q4 2020 showed approximately $42.1 million in losses. Restoring the IT infrastructure resulted in a significant increase in labor costs, both internally and externally, and UHS reported total pre-tax losses of an estimated $67 million due to the ransomware attack.[2]

---

[1] Weiner, Stacy (2021, July 20). *The growing threat of ransomware attacks on hospitals.* Retrieved from the Association of American Medical Colleges (AAMC): The growing threat of ransomware attacks on hospitals | AAMC

[2] Alder, Steve (2021, March 1). *Universal Health Services Ransomware Attack Cost $67 Million in 2020.* Retrieved from HIPAA Journal: Universal Health Services Ransomware Attack Cost $67 Million in 2020 (hipaajournal.com)

Springhill Medical Center Ransomware Death

In July 2019, the Springhill Medical Center suffered a ransomware attack and was forced to operate without the full function of its computer systems for nearly eight days. Patient records were inaccessible and medical staff were unable to use equipment to monitor fetal heartbeats.

While these systems were down, a baby was born at the hospital with her umbilical cord wrapped around her neck. The child suffered severe brain damage as a result of the delivery, and she died nine months later due to related complications. Katelyn Parnell, MD, attending OB-GYN at the hospital, texted the nurse manager that she would have delivered the baby by cesarean had she seen the monitor readout.[3] The fetal heartbeat monitor would have indicated the distress caused by the umbilical cord, and provided information so emergency intervention could be performed. Now, the mother is suing the hospital and, if the lawsuit is successful, this will be the first case of a death due to a ransomware attack in the United States.[4]

Malware and Data Theft

Florida Orthopedic Institute Data Breach

The Florida Orthopedic Institute's servers were infiltrated by malicious actors who then encrypted patients' files, blocking access to them by the facility's staff members on April 9, 2020. According to the HHS Office for Civil Rights breach portal, the attackers gained access to the PHI of approximately 640,000 individuals.[5] The Florida Orthopedic Institute's own investigation also uncovered reasons to suspect that some of the patients' complete identities had been stolen before the encryption, which would include data points such as names, birthdates, Social Security numbers, and more.

While the Florida Orthopedic Institute has not found evidence that those identities have been used, the Institute is facing a class-action lawsuit due to the data breach. Current and former patients are seeking at least $99 million, citing a "failure to properly secure and safeguard protected health information," according to the complaint filed June 30, 2020.[6]

Twelve Oaks Recovery Malware and Data Breach

On December 13, 2020, Twelve Oaks Recovery, a Florida-based addiction and mental health treatment center, detected unusual network activity. Upon further investigation, they discovered that an unauthorized individual had gained access to its network, installed malware, and stole documents from its systems. A forensic investigation confirmed that malware had been deployed on December 13, 2020 and data exfiltration was confirmed the following day.

---

[3] U.S. Department of Health and Human Services (2022, March 03). *Heath Sector Cybersecurity: 2021 Retrospective and 2022 Look Ahead*. Retrieved from: Department of Health and Human Services

[4] Mitchell, Hannah (2021, September 30). Cyberattack on Alabama hospital linked to 1st alleged ransomware death. Retrieved from: Cyberattack on Alabama hospital linked to 1st alleged ransomware death (beckershospitalreview.com)

[5] U.S. Department of Health and Human Services Office for Civil Rights. *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*. Retrieved from: U.S. Department of Health & Human Services - Office for Civil Rights (hhs.gov)

[6] Calaway, Jackie (2020, July 2*). One of Florida's largest orthopedic providers faces class-action lawsuit after data breach.* Retrieved from ABC News: Fla. orthopedic provider faces class-action lawsuit after data breach (abcactionnews.com)

The attacker obtained documents that contained the PHI of 9,023 patients, including names, addresses, dates of birth, medical record numbers, and Social Security numbers.[7]

Phishing

Utah Pathology Services

One June 30, 2020, Utah Pathology Services discovered that hackers had gained access to their systems via an employee's compromised email account. Using the compromised account, the hackers tried to redirect funds from the organization but were ultimately unsuccessful.

The hack prompted an investigation, which revealed that multiple employees were the victims of an email phishing scheme. Further, approximately 148,594 individuals may have had their PHI exposed. The PHI involved included names, dates of birth, gender, telephone numbers, addresses, health insurance information, clinical and diagnostic information, and Social Security numbers.[8]

[7] Alder, Steve (2021, March 2). *Roundup of Recent Healthcare Phishing and Malware Incidents.* Retrieved from HIPAA Journal: Roundup of Recent Healthcare Phishing and Malware Incidents (hipaajournal.com)

[8] U.S. Department of Health and Human Services Office for Civil Rights. *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*. Retrieved from: U.S. Department of Health & Human Services - Office for Civil Rights (hhs.gov)

Appendix C: Attacks and Facts

Distributed Denial of Service

Distributed Denial of Service (DDoS) attacks overload bandwidth and connection limits of hosts or networking equipment, specifically through a network of devices (e.g., computers, cellphones, Internet of Things, etc.) making excessive connection requests. DDoS attacks unfold in stages. First, a malicious actor infects a computer with malware that spreads across a network. This infected computer is known as the "master" because it controls any subsequent devices that become infected. The other infected devices, known as "bots" or "zombies" carry out the actual attack and create what is known as a "botnet". The "bots" receive a command from the "master" which includes the address of the target. Extremely high volumes (floods) of data are sent to the target which slows down web server performance and prevents acceptance of legitimate network traffic. The cost of a DDoS attack can be severe loss of revenue or reputation to the victim.

More information on DDoS attack possibilities within each layer of the Open Systems Interconnection (OSI) Model, as well as traffic types and mitigation strategies, can be found in the resource list below.

Additional Resources

- CISA Understanding and Responding to Distributed Denial-of-Service Attacks (https://www.cisa.gov/news-events/news/understanding-denial-service-attacks)
- CISA DDoS Quick Guide (https://www.cisa.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf)
- MITRE ATT&CK® Network Denial of Service, Technique T1498 – Enterprise (https://attack.mitre.org/techniques/T1498/)
- NIST SP 800-189, Resilient Interdomain Traffic Exchange (https://csrc.nist.gov/publications/detail/sp/800-189/final)

Social Engineering and Phishing

One of the most prominent tactics attackers use to exploit network and system vulnerabilities is social engineering–the manipulation of users through human interaction and the formation of trust and confidence to compromise proprietary information. Techniques for uncovering this information largely involve the use of phishing, i.e., email or malicious websites that solicit personal information by posing as a trustworthy source. Social engineering is effective for breaching networks, evading intrusion detection systems without leaving a log trail, and is completely dependent on the operating system platform. While technical exploits aim to bypass security software, social engineering exploits are more difficult to guard against due to the human factor. Organizations should take steps towards strengthening employee cybersecurity awareness training, to include training personnel to be cautious of suspicious emails, providing instruction on where to forward them, and keeping software and systems up to date.

Additional Resources

- Avoiding Social Engineering and Phishing Attacks (https://www.cisa.gov/uscert/ncas/tips/ST04-014)
- Phishing (https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing)

Ransomware

Ransomware is a type of malware that denies access to victims' data or systems through encryption with a key only known by the malicious actor who deployed the malware. Once encrypted, the ransomware directs the victim to pay the attacker, typically in the form of cryptocurrency, so the victim can receive a decryption key. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website. Recovery can be an arduous process and there is no guarantee the victim will receive access to their data or systems if the ransom is paid. For more information on best practices to protect users from the threat of ransomware, as well as recent Alerts on specific ransomware threats, see the resource list below.

Additional Resources

- CISA Stop Ransomware Website (https://www.cisa.gov/stopransomware)
- Protecting Against Ransomware (https://www.cisa.gov/uscert/ncas/tips/ST19-001)

Appendix D: Doctrine and Resources

Laws

- National Cybersecurity Protection Act of 2014 (Dec 2014) (https://www.congress.gov/bill/113th-congress/senate-bill/2519)
- Federal Information Security Modernization Act of 2014 (Dec 2014) (https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act)
- Office of Management and Budget (OMB) Memorandum: M-15-01, Fiscal Year 2014-2015: Guidance on Improving Federal Information Security and Privacy Management Practices (Oct 2014) (https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2015/m-15-01.pdf)

Presidential Directives

- Executive Order 14028: Improving the Nation's Cybersecurity (May 2021) (https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/)
- Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 2017) (https://trumpwhitehouse.archives.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/)
- Presidential Policy Directive 41: United States Cyber Incident Coordination (Jul 2016) (https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident)
- Annex to Presidential Policy Directive 41: Annex to the Directive on United States Cyber Incident Coordination (Jul 2016) (https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/annex-presidential-policy-directive-united-states-cyber-incident)
- Presidential Policy Directive 8: National Preparedness (Mar 2011, Updated Sep 2015) (https://www.dhs.gov/presidential-policy-directive-8-national-preparedness)
- Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (Feb 2013) (https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil)
- Executive Order 13636: Improving Critical Infrastructure Cybersecurity (Feb 2013) (https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity)

Strategies and Frameworks

- CISA's Stop Ransomware Website (2021) (https://stopransomware.gov)
- New Federal Government Cybersecurity Incident and Vulnerability Response Playbooks (Nov 2021) (https://www.cisa.gov/uscert/ncas/current-activity/2021/11/16/new-federal-government-cybersecurity-incident-and-vulnerability)

- Department of Justice Cybersecurity Unit White Papers and Other Documents (2021) (https://www.justice.gov/criminal-ccips/cybersecurity-unit)
- National Response Framework (2019) (https://www.fema.gov/emergency-managers/national-preparedness/frameworks/response)
- National Cybersecurity Strategy of the United States of America (March 2023) (https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf)
- U.S. Department of Homeland Security Cybersecurity Strategy (May 2018) (https://www.dhs.gov/publication/dhs-cybersecurity-strategy)
- Framework for Improving Critical Infrastructure Cybersecurity (Apr 2018) (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf)
- National Cyber Incident Response Plan (NCIRP) (Dec 2016) (https://www.cisa.gov/resources-tools/resources/national-cyber-incident-response-plan-ncirp)
- National Protection Framework, Second Edition (Jun 2016) (https://www.fema.gov/sites/default/files/2020-04/National_Protection_Framework2nd-june2016.pdf)
- OMB Memorandum: M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government (Oct 2015) (https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf)
- National Infrastructure Protection Plan (NIPP) (2013) (https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/national-infrastructure-protection-plan-and-resources)
- National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide, Rev. 2 (2012) (https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final)
- CISA National Cyber Incident Scoring System (NCISS) (https://www.cisa.gov/news-events/news/cisa-national-cyber-incident-scoring-system-nciss)
- NIST Supply Chain Risk Management Practices for Federal Information Systems and Organizations (2015) (https://www.nist.gov/publications/supply-chain-risk-management-practices-federal-information-systems-and-organizations)

Federal Government Resources

- CISA (contact: central@cisa.dhs.gov)
- United States Secret Service (USSS) Field Offices and Electronic Crimes Task Forces (ECTFs) (contact http://www.secretservice.gov/contact/field-offices, https://www.secretservice.gov/investigation/cyber)

- Federal Bureau of Investigation (FBI)
  - Field Office Cyber Task Forces (contact: https://www.fbi.gov/contact-us/field-offices)
  - Internet Crime Complain Center (IC3) (contact: http://www.ic3.gov)
  - National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center (contact: cywatch@ic.fbi.gov; 855-292-3937)

State Level Resources

- Multi-State Information Sharing and Analysis Center (MS-ISAC) (contact: info@msisac.org; 518-266-3460)
- National Governors Association (NGA) (https://www.nga.org/)
  - NGA Center for Best Practices (https://www.nga.org/bestpractices/divisions/hsps/)
- DHS Cybersecurity Fusion Centers (https://www.dhs.gov/state-and-major-urban-area-fusion-centers)
- National Association of State Chief Information Officers (NASCIO) (https://www.nascio.org/)

Private Sector/Business Resources

- InfraGard (https://www.infragard.org/)
- Internet Security Alliance (https://isalliance.org/)
- Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) (https://www.isao.org/information-sharing-groups/)
  - International Association of Certified ISAOs (http://www.certifiedisao.org; contact: operations@certifiedisao.org)
  - National Council of ISACs (https://www.nationalisacs.org)