A picture containing chart

Description automatically generated

**A picture containing icon

Description automatically generated**

**SGNL SOLUTIONS**

**www.sgnl.solutions**

**DHS Cybersecurity and Infrastructure Security Agency**

**and Healthcare and Public Health Sector**

**Stakeholder Discussion Guide**

Table of Contents

[Terms of Use 3](#_Toc130464774)

[About SGNL Solutions 3](#_Toc130464775)

[Overview 4](#_Toc130464776)

[Purpose 4](#_Toc130464777)

[Format 4](#_Toc130464778)

[Discussion Planning 5](#_Toc130464779)

[Leadership Support 5](#_Toc130464780)

[Planning Team 5](#_Toc130464781)

[Draft Objectives 5](#_Toc130464782)

[Meeting Logistics 6](#_Toc130464783)

[Participant Invitation 4](#_Toc130464784)

[Facilitator Guide 5](#_Toc130464785)

[Facilitation Tips 5](#_Toc130464786)

[Scenario 6](#_Toc130464787)

[Discussion Questions 7](#_Toc130464788)

[General Questions 7](#_Toc130464789)

[Sub-Sector Specific Questions 7](#_Toc130464790)

[Inject 1: 8](#_Toc130464791)

[General Questions 8](#_Toc130464792)

[Sub-Sector Specific Questions 9](#_Toc130464793)

[Inject 2: 9](#_Toc130464794)

[General Questions 10](#_Toc130464795)

[Sub-Sector Specific Questions 10](#_Toc130464796)

[Inject 3: 11](#_Toc130464797)

[General Questions 11](#_Toc130464798)

[Sub-Sector Specific Questions 12](#_Toc130464799)

[Inject 4: 12](#_Toc130464800)

[General Questions 12](#_Toc130464801)

[Sub-Sector Specific Questions 13](#_Toc130464802)

[Hot Wash 14](#_Toc130464803)

[Next Steps 14](#_Toc130464804)

# Terms of Use

This guide is designed to help a stakeholders engage in an initial conversation about how it can foster improved understanding between DHS CISA and the HPH Sector. Permission is granted to tribal, territorial, state, county and local health departments and healtcare orgnaizations to reproduce and adapt (“Adapted Materials) for noncommercial purposes. The DHS Cybersecurity and Infrastructure Security Agency (CISA) was not involved in the production of this product.

SGNL Solutions does not necessarily adopt or endorse any of the Adapted Materials posted by any other users or organizations and make no representations or warranties about the suitability of such information for any purpose, and the Adapted Materials may not state or imply adoption or endorsement by SGNL Solutions. Individuals or organizations that use all or part of this guide or the Adapted Materials are solely responsible for any discussions or events that may use them as a reference. SGNL Solutions expressly disclaims responsibility and shall have no liability for any damages, loss, injury, or liability whatsoever suffered because of any user’s use of or reliance on this guide.

Copyright Notice: Copyright 2023 SGNL Solutions. Some Rights Reserved. Permission is granted to reproduce by U.S. tribal, territorial, state, county and local health departments and healthcare organizations for noncommercial purposes without written permission. For all other uses, written permission from SGNL Solutions is required.

# About SGNL Solutions

SGNL Solutions (SGNL), a service-disabled veteran-owned small business corporation, connects across research, policy, and practice communities to identify, understand, and solve complex health security challenges. We undertake collaborative projects involving stakeholder engagement, process facilitation, data collection, analysis, evaluation, scientific writing, and product development. Our team of experienced consultants provides cross disciplinary expertise and perspectives, which fosters better understanding and integrated solutions to address our nation’s most pressing issues. We become issue experts and get excited about what matters to our clients. We sift through noisy data and distractions to get at the core of persistent problems to find the signal – the real information and approaches needed to finally address problems. We work across disciplines, think creatively, and break apart silos that oftentimes prevent progress. We then work with clients to make these important issues approachable and actionable.

Direct any questions regarding this product to:

Justin Snair, MPA

Managing Partner and Principal Consultant

SGNL Solutions

[jsnair@sgnl.solutions](mailto:jsnair@sgnl.solutions)

# Overview

## Purpose

The purpose of this discussion guide is to help participants engage with Healthcare and Public Health Sector (HPH) sector stakeholders to discuss critical infrastructure dependencies and capabilities Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) may better engage as the Federal lead for critical infrastructure risk assessment and preparedness. The discussion guide is designed to encourage a conversation between CISA regional office staff and HPH sector stakeholders in a way that highlights the interconnectedness of the sector with others, especially when responding to complex incidents with far-reaching implications. It is intended to serve as a catalyst for developing risk management strategies and information sharing practices by identifying existing gaps and vulnerabilities.

## Format

This discussion guide is designed for large or small participant groups to have a facilitated discussion around the HPH sector organizations with a role in critical infrastructure protection or as critical infrastructure assets. This guide is intended to structure the planning efforts for a discussion and provide all of the resources needed to facilitate. The facilitation guide contained in this document includes a plausible scenario with 4 additional injects and 120 discussion questions, intended for customized use. The discussion questions are further organized into two tiers. The first tier of questions may be posed to representatives from any HPH subsector. The second tier of questions are subsector-specific questions.

# 

# Discussion Planning

## 

## Leadership Support

The mission of CISA is to lead the National effort to understand and manage cyber and physical risk to our critical infrastructure. As one of the 16 critical infrastructure sectors, it is imperative that CISA gain an understanding of the form and function of the HPH sector. Holding facilitated discussions with sector stakeholders is a great first step toward enhanced communication and coordination.

Leadership should be briefed early and often about the value of engagement efforts to the HPH sector. With backing from leadership, it is much easier to allocate resources to conduct the discussion, recruit participants, and produce actionable outcomes. It is recommended that the following points be leveraged to encourage leadership buy-in on facilitated discussion engagement with HPH sector stakeholders:

* Demonstrate value to the CISA mission
* Link outreach efforts to CISA strategic priorities, business goals and National strategic objectives
* Contextualize with real-world threats and case examples
* Highlight past successes of HPH sector assets being leveraged to reduce National risk and mitigate incidents.

## Planning Team

The planning team is formed to support discussion development and conduct. The planning team also establishes the discussion objectives. Team members also help with building and distributing discussion read-ahead materials. At a minimum, the planning team should consist of individuals filling the following roles:

|  |  |
| --- | --- |
| Role | Responsibility |
| Facilitator | Guides the discussion toward the objectives using the questions contained in the facilitation guide as reference. |
| CISA Lead | Lead CISA participant with in-depth understanding of the participating organizations, cybersecurity, critical infrastructure and responsible for engaging directly with HPH sector stakeholders. |
| SME Presenter | Provides any relevant special sector specific topic briefings to the planning team. Can provide subject matter expertise as requested during the discussion. |
| Host | Coordinates meeting logistics, including inviting participants, finding a meeting space, securing supplies, and communicating about the meeting effectively. |
| Note Taker | Documents the major themes, decisions and outputs from the discussion. |

## Draft Objectives

Defining the objectives of a discussion helps to scope the conversation and unite all participant groups toward a common goal. The planning team should establish the discussion objectives, with input from the participants, before conduct and use them to shape the facilitation strategy.

Generally speaking, one should always strive to establish SMART objectives:

* Specific – The objective is clearly defined.
* Measurable – The objective can be measured and the measurement source is identified.
* Achievable – The objective or expectation of what will be accomplished must be realistic.
* Relevant – The objective directly supports the strategic priorities of the participating organizations.
* Time-framed – The objective is framed to fit into the timeframe allocated for the discussion.

## Meeting Logistics

The discussion facilitated by this guide is designed to be conducted over 3-4 hours with an estimated preparation time of four to six weeks. Once the planning team determines the duration of the discussion, they must select a date, time, and venue. If the discussion is slated to run longer than four hours, the planning team may consider including breaks in the agenda that are long enough for participants to leave to obtain food. The planning team should secure a meeting space that can accommodate the intended number of participants. The room should be large enough to comfortably fit the group and be ADA compliant to accommodate all needs of participants. For in-person meetings it is recommended that tables be arranged in a way that allows participants are encouraged to engage in face-to-face interaction.

There are a few written materials the planning team will need to draft for participants ahead of execution. The facilitation guide should be available for the facilitator to use during the discussion. An agenda should be finalized detailing every stage of the discussion with its associated time frame. A participant list of confirmed attendees should be provided to participants. This allows them to understand the represented organizations in the room. If possible, it is beneficial to provide a seating charge for the facilitator to reference. Name tags and table tents put names to faces which can help facilitate cross discussion with sector stakeholder who have not met before. If there is a presentation being shared during the discussion, hard copies of the slides should be provided to the participants.

Discussion Materials Checklist

Participants

* Agenda
* Participant List
* Name tag or Table tent
* Presentation slides (if applicable)

Facilitator

* Facilitation guide
* Agenda
* Seating chart
* Name tag or Table tent

Copies of handouts should be made available for all participants. Prior to the meeting or upon arrival, each participant should receive a packet of information and materials that might be useful to them during the meeting, as outlined in the checklist above. The planning team should also consider including a SME presentation at the beginning of the meeting agenda to showcase in-depth information relevant to the discussion. The presenter should be knowledgeable about the topics they are presenting and viewed as an authority by participants.

## 

## Participant Invitation

This discussion is intended to encourage a better understanding of the structure, authorities and stakeholders of the HPH sector. The planning team must seek out participants that can enhance CISA knowledge of each subsector of the HPH sector in their Region.

Participant selection is an important aspect of planning the discussion. Participants will need to be knowledgeable enough to speak to the entirety of the organization they are representing. Ideally the role of the individual participating should have something to do with critical infrastructure protection.

Invitations to prospective participants should be sent via email no later than four weeks ahead of conduct. The message body should detail the following:

* Intended execution date
* Objectives of the discussion
* Organizations invited
* Length of discussion
* Location of discussion
* Instructions for arrival
* Point of contact

Additionally, the planning team may consider attaching the agenda to the invitation for reference.

# Facilitator Guide

Discussion-based exercises typically work best when facilitated or moderated by a non-participant party. Facilitated discussions occur in a plenary session or in breakout groups that are typically organized by discipline or agency/organization. Moderated discussions generally follow breakout group discussions where a representative from each group provides participants with a summary of their facilitated discussion.

Whether the exercise is facilitated or moderated, or both, the facilitator is responsible for keeping discussion relevant to the discussion objectives. The facilitator is also responsible for ensuring all objectives and issues are addressed to the greatest extent possible by asking relevant discussion questions to gather information for desired outcomes. The facilitator must be well-read into the participant organizations in the discussion in order to effectively target the objectives with their questions.

## Facilitation Tips

* Conduct an audio check before the discussion begins to ensure all participants can hear or understand the speaker. Accommodations may need to be made ahead of execution for the aurally impaired.
* Ensure any visual components are visible and legible to all participants. In larger rooms, providing hard copies or digital versions can help mitigate this.
* Establish basic ground rules to include “sharing the airtime”, use of ‘I” statements, one speaker at a time, all ideas are valid, ask questions before you try to persuade, choose to be present, treat the scenario as plausible and be brief. Ask participants if there are other ground rules that they would like to establish.
* When leading a discussion, ask one question at a time and wait at least ten seconds for responses. Be prepared to rephrase the question in order to illicit a response.
* Use open-ended questions rather than yes or no questions. Ask who, what, when, where, why, and how questions.
* When documenting information on visual aids such as a (whiteboard, screen or flipboard) write in large, clear, thick print and alternate marker color to help participants separate statements.
* Use contrasting colors to distinguish different discussion threads, ideas or questions.
* During any small-group activities, circulate among the tables to answer questions and keep the participants engaged.

## Scenario

A global pandemic of the pathogenic variant of the yeast strain Candida has taken root over the past two months. This variant, named Candida quiesces, is spreading rapidly through direct contact with infected people, surfaces and aerosolized droplets in high concentration from perspiration or respiration. Symptoms are similar to those of a bacterial infection; severe fever, chill, body aches and pain. C. quiesces can cause bloodstream infections and even death, particularly in the elderly, immunocompromised and those with preexisting severe medical conditions. More than 1 in 3 patients with invasive C. quiesces infection (for example, an infection that affects the blood, heart, or brain) die. It is suspected that C. quiesces is disproportionately affecting low-income communities and frontline workers through use of public transportation and working in high traffic environments. The fungus is not easily identifiable without advanced laboratory equipment and is resistant to current antifungal drugs. Patients have been found to be asymptomatic up to 3-5 days after beginning to shed the fungal spores. Most individuals remain infectious for 10 – 15 days total with severe symptoms manifesting between days 8 – 12. Several major pharmaceutical companies have filed for emergency use authorizations on medical therapies employing novel inhaled antifungal medication and corticosteroids.

Public information campaigns around personal hygiene, infection indicators and personal protective equipment have been undermined by fringe internet-based groups launching targeted disinformation campaigns. Propelled by media coverage and political rhetoric, civil distrust in public health advisories is leading to clashes in public places though they are seldom violent. The apparent intent of the disinformation online is to detract from political opponents domestically but there are suspicions in the intelligence community that an adversarial nation-state may be fostering these efforts as well. Many major metropolitan governments have issued stay at home orders forcing business closures and dramatically increased telework. Unemployment claims have skyrocketed, however, Federal aid is not forthcoming. As the country enters summer it is expected that many will break isolation orders, gathering restrictions and intra-state travel bans. Additionally, due to the suspected origin of the pathogen, hate groups have escalated displayed of racial prejudice; particularly against African Americans. Violence perpetrated by hate groups have resulted in the deaths of 9 people to date stirring civil rights activists to peacefully demonstrate in state capitols and major cities. Hate groups and domestic terrorist organizations have begun to counter-protest these events threatening to impart continued violence.

Since the onset of the pandemic, cyber-attacks intended to extract proprietary information from healthcare and clinical research facilities. Though few have been successful, a lone wolf hacker has successfully penetrated the electronic health record system of the region’s largest healthcare provider network. Preliminary indicators point to an old privileged account tied to a since-retired administrator at an associated teaching hospital as the point of compromise. The adversary had remote access to the networks patient filing systems for weeks before their activity was noticed by IT staff. The network has hired cyber support specialists to find the adversary but progress is slow. The story of a suspected cyber-attack against the region’s top healthcare provider network, during a pandemic, was picked up in the media. The adversary, now aware of the cyber support specialists conducting a hunt, extracts 3.2 million patient records and delivers a malware payload locking all active accounts out of the system. There has been no ransom communication. With no system back-ups to use the healthcare provider network is forced to try and decrypt access to their platform. Meanwhile clinical workers have devolved to using paper intake forms and charts.

## Discussion Questions

Included in this section are 120 questions centered around the scenario presented on the previous page and 4 injects.

There are two tiers of questions. The first tier of questions may be posed to representatives from any HPH subsector. The second tier of questions are subsector-specific questions. The facilitator should only select tier two questions relevant to the subsectors represented at the discussion. The questions included in this guide are meant to explore communication pathways, coordination mechanisms and capabilities. It is recommended that the facilitator follow the line of questioning presented in this guide.

### General Questions

1. What events in this scenario present challenges for your organization?
   1. What is your role with regard to the scenario events presented?
2. What operational changes would need to be implemented to continue your organization's function in the sector?
   1. Could you define the key services to the HPH sector that your organization provides?
3. At this time, what are the informational and data is needs for your organization?
   1. From what organizations do you typically receive this type of information?
   2. What are the time constraints for this data to be actionable?
4. What other organizations would you be working with at this point?
   1. Do you have existing agreements or documentation of understanding with them?
   2. How were these connections developed?
5. How would a disruption or degradation of your capabilities affect the community?
   1. Describe any individuals or groups that may be reliant on your services.
6. Who in your organization would be involved in mitigating the events of the presented scenario?
   1. What does the incident response structure for your organization look like?
   2. Are these individuals full time emergency management specialists?
   3. How does your organization manage emergency operations funding and staffing?

### Sub-Sector Specific Questions

|  |  |
| --- | --- |
| Direct Patient Healthcare | * How quickly are pandemic response protocols for clinical settings established? * How are clinical staff read in to threat briefings on imminent threats such as zoonotic disease in order to more effectively treat cases? * Does your facility employ cybersecurity specialists? |
| Public Health Agency | * What are the mechanisms by which your organization receives health data for the community it serves? * Does your organization handle PHI on any of its IT systems? |
| Healthcare Educational Facility | * How does your organization monitor and manage the health and safety of students and faculty? * How is network systems data for your organization secured and validated in a remote learning environment? |
| Health Supporting Facility | * What are the communication means used by direct patient care providers to request additional materials or resources from your organization during a health emergency? * What measures has your organization taken to prevent unlawful proprietary data extraction? * How often are your organizations staff provided cybersecurity training? |
| Fatality/Mortuary Facility | * What is the capacity of your facility to intake and process bodies? * Is autopsy data shared with any organizations outside of your own? |
| Regulatory, Oversight, or Industry Organization | * Does your organization have any Federal reporting requirements for public health or cybersecurity incidents? * What means of incident document does your organization use and where is it hosted? |

## Inject 1:

Large gatherings for the Fourth of July led to a doubling of C. quiesces infection cases in the region. There is still no viable treatment available for patients with severe illness.

Protests have largely shut down many of the means of ingress to the major medical campuses in the city forcing those seeking care to flood smaller facilities in outlying areas. With their patient health record systems down, care facilities are reporting increased patient intake times and dwindling available beds.

### General Questions

1. What emergency response plans does your facility have to mitigate major health crises, such as the described pandemic?
2. How can your organization help to reduce the burden of a pathogen case surge for the region’s major medical centers?
   1. What facilities do you have available?
   2. What resources can you share?
   3. Will this affect your organization’s mission effectiveness?
   4. Is there cost associated with your assistance?
3. How would reduced access to city facilities affect your organizations capabilities?
4. How does your organization ensure the safety of its workers?
   1. What occupational hazards are your workers prepared for?
5. To what degree does your organization have the ability to shift materials and resources to other sector entities?
   1. Can your organization physically move those resources?
6. Would you describe your organizations capacity to conduct internal cybersecurity risk assessments?
   1. How often are network scans and system backups conducted?
   2. Are communications conducted with end-to-end encryption?
7. How do state or national emergency declarations affect your organizations operations?
   1. What relevant authorities is your organization subject to?

### Sub-Sector Specific Questions

|  |  |
| --- | --- |
| Direct Patient Healthcare | * How often does your facility conduct preparedness exercises and for which hazards? * Do the facilities of your organization have continuity of operations plans? |
| Public Health Agency | * What are your organizations primary means of influence and intervention when mitigating pathogenic disease? * Does your organization’s incident response plans account for alternative sites to conduct patient treatment? |
| Healthcare Educational Facility | * Does your facility serve as an alternative site for care to increase direct patient surge capacity? |
| Health Supporting Facility | * Do you have high-demand resources stockpiled to meet increased demand? * How is inventory data securely shared with sector partners? |
| Fatality/Mortuary Facility | * Can death paperwork be filed with the loss of electronic recording systems? * What is the rate limiting step in an emergency for your facility to process a body? |
| Regulatory, Oversight, or Industry Organization | * What are the national reporting thresholds for your organization to report an outbreak or mass fatality incident? * What resources can be made available to support frontline health workers? * Where is epidemiological data used by your organization and who has access to it? |

## 

## Inject 2:

Several months have passed and a couple major pharmaceutical companies have received emergency authorization for their nasally administered antifungal treatment; though production will take an estimated two weeks to spin up. Cases of C. quiesces have slowly declined but in the past week the governor caved to political pressure, removing all public health restrictions on social gatherings and travel.

Today, a major international of plastics, particularly polypropylene-based goods lost 2 major production plants and their adjoining warehouses full of inventory when a massive amount of ammonium nitrate from a nearby fertilizer factory was accidentally ignited. PPE manufacturers in the U.S. and abroad are scrambling to source new raw materials.

IT professionals working for a hospital in the healthcare provider network received a message demanding $5M in cryptocurrency to regain access to their patient records. They have since shifted to a new platform but over 25 million PHI files remain held hostage by the cyber adversary. This event spurs concerns from your organization’s executives around the safety and security of the sensitive data your organization handles.

### General Questions

1. What kind of support does your organization offer to medical countermeasure efforts?
   1. Do you have the bandwidth to conduct outreach in support of common HPH sector goals?
2. How does your organization interface with the public to prevent resurgent disease?
3. Could you describe the resource supply chains your organization uses to remain operational?
   1. What materials are essential to keeping your organization on mission?
   2. Do you have multiple suppliers?
4. What reporting requirements does your organization have to communicate suspected cyber incidents?
   1. Do you have a connection to US-CERT?
   2. What percentage of your workforce has active security clearances?
5. How does your organization invest in cybersecurity hygiene?
   1. How often do employees of your organization undergo cyber training?
6. How would you describe the cybersecurity sophistication of your organizations staff?
   1. Have you run internal cyber exercises in the past?

### Sub-Sector Specific Questions

|  |  |
| --- | --- |
| Direct Patient Healthcare | * How are new treatment techniques socialized with clinical staff? * Does your procurement office stockpile medical countermeasures or order as needed? * Has your organizations IT department identified viable backups for in-use patient data systems? |
| Public Health Agency | * How do you target health information messaging to vulnerable populations? |
| Healthcare Educational Facility | * Are students permitted to support patient care facilities to relieve staff? |
| Health Supporting Facility | * What is the standard operating procedure for your organization when confronted with a denial of service or ransomware attack? * Does your organization diversify its raw materials and manufactured goods suppliers? * How does your organization forecast and respond to international events with domestic supply chain consequences? |
| Fatality/Mortuary Facility | * Does your organization preposition supplies in expectation of increased instances of death? If so, how far in advance? * How do death statistics from your organization affect public policy? |
| Regulatory, Oversight, or Industry Organization | * Are there watchdog authorities that may be levied against political figures when there is overwhelming evidence of inherent risk to public health? * How is HPH sector data conveyed to decisionmakers by your organization? |

## Inject 3:

Two weeks later the healthcare provider network elects not to pay the ransom for their data and are continuing to use an alternate system to handle EHRs. HHS inspectors have launched an investigation into possible HIPAA Security Rule violations.

Reports of an outbreak of C. quiesces infections at a local retirement complex are beginning to circulate as 10 residents within 3 days pass away from characteristic symptoms. Facility caregivers are suggesting that a member of the staff may be intentionally infecting residents in light of the precautions in place.

Shipments of clinical-certified PPE are being shifted for distribution only to regional hospitals as manufacturer production slows to a standstill. The first 10,000 doses of the antifungal drug used to treat C. quiesces have arrived in the region.

### General Questions

1. To what standards does your organization align its cybersecurity plans, policies and procedures?
   1. Has your organization incorporated NIST security control guidance?
2. Could you describe the partnerships your organization to maintain cyber regulation compliance and to help mitigate cyber incidents?
   1. What connections has your organization formed with Federal cybersecurity organizations relevant to the sector?
   2. What types of cyber guidance has your organization found most helpful?
3. Describe the connections and outreach your oganization has to vulnerable populations in the region.
   1. What demographic data sources do you utilize to conduct this outreach?
4. How does your organization support health investigatory efforts?
5. To what extent is your organization dependent on consistent PPE delivery in order to continue its mission?

### Sub-Sector Specific Questions

|  |  |
| --- | --- |
| Direct Patient Healthcare | * What is the protocol and timeline for response to a cyber-attack affecting your networks? * Does your organization have connections to public or private cyber incident resolution teams? |
| Public Health Agency | * What are some best practices your organization has identified for managing expectations during the gradual resolution of a long-term health incident? * What demographics in your community are most vulnerable and why? |
| Healthcare Educational Facility | * Are cybersecurity regulations and guidance part of the curriculum taught at your organization? |
| Health Supporting Facility | * How does your facility assist in forensic investigations of malicious spread of pathogenic disease? * Under what authority can resources be redistributed from their original purchaser? |
| Fatality/Mortuary Facility | * Does your organization have access to federal strategic stockpiles? |
| Regulatory, Oversight, or Industry Organization | * How does your organization process and prioritize incoming requests for assistance? * How does your organization conduct oversight or investigatory actions of private organizations suspected to have violated PHI security rules? |

## Inject 4:

In spite of the challenges of the past six months, strategically distributed treatments for C. quiesces infections have dramatically lowered the mortality of illness caused by the pathogen. The outbreak at the local retirement complex is growing and the county morgue is running out of space to store the bodies.

The healthcare provider network was found to be in violation of HIPAA and was fined a substantial amount of money. The board has promised to implement new cybersecurity standards and training for all personnel with access to PHI.

Later this week, deviations in prevailing winds are predicted to bring tens of inches of rain to the region. Severe flooding is imminent. Regional residents living in flood plains have been advised to evacuate their homes immediately.

### General Questions

1. How does is your organization get involved with long-term disease or hazard mitigation efforts?
   1. What does recovery and return to normal operations look like for your organization?
2. How does your organization plan to mitigate potential fiscal and legacy consequences from a cybersecurity incident?
3. Can you describe past cyber incidents that affected d your organization or its partners?
4. Can you describe the process by which your organization becomes aware of sector threats and vulnerabilities (more specifically, as they relate to cyber)?
5. Can you describe any hazardous weather emergency preparedness activities your organization has participated in?
6. How would your organization prepare for a disaster such as widespread severe flooding?
7. What utilities are essential to your organization’s operation?
   1. Are you familiar with the HPH sector lifelines defined in the affected Sector Specific Plan?

### Sub-Sector Specific Questions

|  |  |
| --- | --- |
| Direct Patient Healthcare | * How has the physical infrastructure of your organization’s facilities been hardened against the effects of extreme weather. * What is the process for cybersecurity improvement at your organization? |
| Public Health Agency | * Can you describe the climate preparedness portfolio of activities for your organization? * What are some of the climate-borne health concerns you are seeing start to grow in your region? |
| Healthcare Educational Facility | * To what level are interdisciplinary topics such as climate resiliency, the national response framework, and the incident command structure covered in your organization’s curriculum? |
| Health Supporting Facility | * How are requests for emergency supplies, research data, or other services received and fulfilled when a region is experiencing a widespread, severe natural disaster? * How does your organization track the movement of temporary aid sites and field hospitals during a disaster? |
| Fatality/Mortuary Facility | * Has your organization developed overflow mitigation strategies? * Are there any existing regulations for body storage that your organization must abide by? |
| Regulatory, Oversight, or Industry Organization | * How does your organization ensure changes to cybersecurity regulations for the sector are socialized? |

## Hot Wash

Once the discussion is concluded, it might be beneficial to conduct a brief Hot Wash. The Hot Wash provides an opportunity to summarize the discussion strengths and areas for improvement immediately following the conduct. The facilitator leads the Hot Wash and ensures the discussion remains constructive using information captured during the discussion. Participant are encouraged to shared items that stuck out to them and any logic next steps they see for their organization. The Note Taker should capture all information discussed during the Hot Wash. Once the Hot Wash is complete the participants are allowed to leave.

## Next Steps

Once the discussion is concluded, the planning team can be tasked with drafting a report of the conversation and any relevant findings. This report could be shared with all participants following the discussion or remain an internal document. At a minimum this report should include:

* A summary of the group discussion.
* Challenges posed to sector critical infrastructure
* Identified partnerships, formal agreements or instances of past cooperation between sector stakeholders
* Information sharing channels and escalation pathways
* Key players at participating organizations
* Relevant CISA resources and services
* Priorities for future engagements

Given the sensitive information that could be included in such a report, the planning team may consider applying security markings to the document.