Sector Resilience Report: Hospitals

December 19, 2014, 1450 EST

SCOPE

The Department of Homeland Security's Office of Cyber and Infrastructure Analysis (DHS/OCIA)[1] produces Sector Resilience Reports to improve partner understanding of the interdependencies and resilience of certain sectors. This report focuses on the Hospitals Segment within the Healthcare and Public Health Sector and Direct Patient Healthcare Subsector. Specifically, this report provides a brief overview of the Hospitals Segment, and analysis of key dependencies and interdependencies. In addition, this product provides an assessment of, and best practices for, improving community, system, and facility resilience. This Sector Resilience Report was produced to complement other sector-specific guidance, analyses, and scholarly papers on infrastructure resilience by applying data obtained from DHS site visits and assessments analyzing the resilience of critical infrastructure assets and systems.

Best practices for improving resiliance are provided for both hospital systems and community risk management organizations (e.g., State or local emergency operations centers, emergency managers, public works, utility managers, and disaster relief organizations). This product was coordinated with the DHS's Office of Infrastructure Protection, the DHS's Office of Health Affairs, and the Department of Health and Human Services (HHS).

KEY FINDINGS

- **Of the 222 hospitals that received DHS assessments, 100 percent are dependent on electric power; of those facilities, all but one have a backup or alternate source of electric power.**
- **All facilities with backup power had an electric generator, which was most often used to maintain core operations. While on generator power, only a portion of hospital functionality is operable, and the backup typically lasts for only a short period (hours to a few days).**
- **OCIA assesses the hospitals in the DHS data set will experience a 67-99 percent degradation to their core operations after 5 minutes without alternate or backup sources for electric power, after 10 minutes without information technology, and after 2 hours without water and wastewater.**

[1] In February 2014, the National Protection and Programs Directorate (NPPD) created the Office of Cyber and Infrastructure Analysis by integrating analytic resources from across NPPD including the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) and the National Infrastructure Simulation and Analysis Center (NISAC).

- **Similar to other hospitals that received DHS assessments, critical access hospitals[2] rely heavily on key utilities (electric power, water, wastewater treatment, communications, natural gas, and information technology); however, the number of critical access hospitals that have utility backups, contingency plans, or priority restoration plans is noticeably lower than other hospitals.**

HOSPITALS OVERVIEW

The Healthcare and Public Health Sector is defined as publicly and privately owned assets that deliver both direct and supporting health-related services to individuals and populations.[3] The Sector has a critical role in preparedness and response for all hazards, and is responsible for mitigating the physical and psychological health impacts associated with incidents. The effectiveness of health-related response support requires Sector assets to both mitigate incident-related physical and psychological health impacts, and to ensure assets can meet Healthcare and Public Health surge demands associated with these events.[4]

Facilities within the Healthcare and Public Health Direct Patient Healthcare Subsector provide direct medical, diagnostic, and treatment services to individuals to diagnose and treat injuries and diseases. This subsector is composed of the following segments: (1) hospitals; (2) ambulatory healthcare facilities; (3) extended care facilities; (4) health practitioner offices and clinics; and (5) home healthcare.[5] The Hospital Segment provides the greatest amount of employment and generates the most revenue (45 percent) for the Direct Patient Healthcare Subsector.[6,7]

The Hospitals Segment is an integral component of the Healthcare and Public Health Sector. Collectively in 2013, hospitals employed about 4.83 million people and generated about $883.2 billion in revenue from 5,723 registered hospitals and 920,829 registered hospital beds.[8,9] The majority of U.S. hospitals, 78 percent, are privately owned and 22 percent of hospitals are owned by the Federal, State, or local, Government.[10]

The most common hospital type, General Hospital, treats an array of medical conditions. Other hospital types (Psychiatric or Substance Abuse; Children's; and other specific specialty types (e.g., trauma, burns, and cancer)) typically provide unique services or treat a specific patient base.[11] Some hospitals are termed critical access hospitals. Receiving funding and operational support from Medicare, critical access hospitals provide essential medical care to rural

---

[2] A critical access hospital is a rural hospital certified under a set of Medicare Conditions of Participation. See page 11 of this report for more detail.

[3] DHS Office of Infrastructure Protection, *Infrastructure Data Taxonomy Version 4*, 2011.

[4] DHS and HHS, *Healthcare and Public Health Sector-Specific Plan*, 2010, www.dhs.gov/xlibrary/assets/nipp-ssp-healthcare-and-public-health-2010.pdf, accessed May 12, 2014.

[5] DHS Office of Infrastructure Protection, *Infrastructure Data Taxonomy Version 4*, 2011.

[6] IBISWorld, "Industry Report 62211: Hospitals in the U.S.," 2014, accessed June 1, 2014, www.ibisworld.com/industry/default.aspx?indid=1587, accessed June 1, 2014.

[7] American Hospital Association (AHA), "Fast Facts on U.S. Hospitals, 2014, www.aha.org/research/rc/stat-studies/fast-facts.shtml/, accessed June 10, 2014.

[8] *Ibid.*

[9] IBISWorld, "Industry Report 62211: Hospitals in the U.S.," 2014, www.ibisworld.com/industry/default.aspx?indid=1587, accessed June 1, 2014.

[10] AHA, "Fast Facts on U.S. Hospitals, 2014, www.aha.org/research/rc/stat-studies/fast-facts.shtml/, accessed June 10, 2014.

[11] DHS Office of Infrastructure Protection, *Infrastructure Data Taxonomy Version 4*, 2011.

communities across the country in 45 States.[12,13] Residents of rural areas often face barriers in accessing health care services, including having to travel long distances to seek care. As a result, critical access hospitals are typically the sole local source of patient care in rural communities.

RESILIENCE

The common themes shared in this report are drawn from data obtained from DHS site visits, including the Enhanced Critical Infrastructure Protection (ECIP) Initiative, analysis produced by the Regional Resiliency Assessment Program (RRAP), and information gleaned from industry reports and academic research.[14,15] This paper summarizes results from numerous infrastructure assessments that examine vulnerabilities, threats, and potential consequences from an all-hazards perspective, leading to the identification of dependencies, interdependencies, cascading effects, and resilience characteristics.[16]

PPD—8, National Preparedness, defines resilience as "the ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies."

PPD—21, Critical Infrastructure Security and Resilience, directed the Federal Government to work with critical infrastructure owners and operators and State, local, tribal, and territorial partners to strengthen the security and resilience of its critical infrastructure.

Since 1996, the critical infrastructure community has evolved from focusing primarily on protective security to a greater emphasis on resilience to disruptive events.[17] National policies, such as Presidential Policy Directives (PPD) 8 and 21, highlight that collaborative engagement and information sharing with Federal agencies, private sector facility owners and operators, law enforcement, emergency response organizations, academic institutions, and other stakeholders are vital to building a more resilient Nation.

THREATS AND HAZARDS

Hospitals face a broad range of potential threats and hazards that could impact the ability to effectively continue patient care operations. Natural hazards, cyber-attacks, physical threats, and public health emergencies could impede hospitals' abilities to carry out their mission.

---

[12] A Critical Access Hospital (CAH) is a hospital certified under a set of Medicare Conditions of Participation (CoP). HHS, *Critical Access Hospital*, www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/downloads/CritAccessHospfctsht.pdf, accessed June 25, 2014.

[13] AHA, "The Fragile State of Critical Access Hospitals—Infographic," 2011, www.aha.org/content/13/infographic-cah.pdf, accessed May 10, 2014.

[14] The RRAP evaluates critical infrastructure on a regional level to examine vulnerabilities, threats, and potential consequences from an all-hazards perspective, identifying dependencies, interdependencies, cascading effects, resilience characteristics, and gaps. RRAP projects are voluntary and non-regulatory, and they rely on engagement and information sharing with Federal agencies, private sector facility owners and operators, law enforcement, emergency response organizations, academic institutions, and other stakeholders. For more information, please email resilience@dhs.gov or visit www.dhs.gov/regional-resiliency-assessment-program.

[15] The ECIP Initiative is a voluntary program where DHS Protective Security Advisors conduct outreach with critical infrastructure facility owners and operators and provide security surveys, training and education, and recommended protective measures. ECIP metrics provide DHS with information on the protective and resilience measures in place at facilities and enable detailed analyses of site and sector vulnerabilities. For more information, please contact PDCDOperations@hq.dhs.gov.

[16] DHS, *Regional Resilience Assessment Program Fact Sheet*, December 2013.

[17] The Federal Government began to examine potential threats to critical infrastructure in the 1990s as a result of incidents of domestic and international terrorism. President Clinton issued Executive Order 13010 in 1996, which identified the Nation's critical infrastructure sectors and established a Presidential Commission on Critical Infrastructure Protection (PCCIP) whose objective was to recommend a comprehensive national infrastructure protection policy and implementation strategy.

NATURAL HAZARDS

Natural hazards, such as hurricanes, tornadoes, and floods, can damage building structures and interrupt critical utility equipment and services required for patient care operations. For example, in 2001 the Texas Medical Center flooded during Tropical Storm Allison, causing water to pool in hospital sublevels resulting in approximately $2 billion of flood damage. Damaged critical electrical equipment throughout the Texas Medical Center resulted in the complete closure of multiple medical facilities for about 1 month.[18] Significant flooding occurred in hospitals in 2005 with Hurricane Katrina and more recently in 2012 with Superstorm Sandy, which also resulted in challenges to patient care delivery and caused patient evacuations due to damaged electric equipment and structural damage.[19] Tornadoes also significantly damage hospitals, as in Joplin, Missouri, in 2011 and Moore, Oklahoma, in 2013. These tornadoes resulted in structurally unsafe hospitals, which necessitated patient relocation and temporary closures.[20,21]

CYBERATTACKS

Cyberattacks can compromise medical technologies and enable unauthorized access to medical record databases, either of which can effectively halt the delivery of patient care, including:

- Infecting and disabling network-connected or network-configured medical devices via malware;[22,23]
- Accessing patient data and monitoring systems on various computing devices via malware;[24,25]
- Accessing user-restricted software and hardware through password manipulation (disabling and/or changing password access) to lock out authorized users;[26]
- Manipulating security software and patches to promote update failures to medical devices and networks;[27] and
- Hacking or exposing security vulnerabilities in off-the-shelf, healthcare-related software.[28, 29]

---

[18] Bankhead, C., "Tropical Storm Sets Back Research in Houston," *Journal of the National Cancer Institute*, 93(2001): 1366–1367, http://jnci.oxfordjournals.org/content/93/18/1366.long, accessed June 26, 2014.

[19] Reuters, "Insight: Sandy Shows Hospitals Unprepared When Disaster Hits Home," November 3, 2012, www.reuters.com/article/2012/11/03/us-storm-sandy-hospitals-idUSBRE8A20AV20121103, accessed June 1, 2014.

[20] The Journal Record, "Demolition Starts on Moore Hospital Hit by Tornado," June 25, 2013, http://journalrecord.com/2013/06/25/demolition-starts-on-moore-hospital-hit-by-tornado-health-care/, accessed June 1, 2014.

[21] Yahoo News, 2014, "Joplin's Extreme Efforts to Tornado-proof New Hospital," May 22, 2011, http://news.yahoo.com/joplins-extreme-efforts-to-tornado-proof-new-hospital-222058695.html, accessed July 11, 2014.

[22] Dark Reading, "VA Security Compromised by Medical Devices," May 25, 2010, www.darkreading.com/risk-management/va-security-compromised-by-medical-devices/d/d-id/1089402, accessed July 11, 2014.

[23] The Register, "Paging Dr Evil: Philips Medical Device Control Kit 'Easily Hacked', January 18, 2013, www.theregister.co.uk/2013/01/18/medical_device_control_kit_security/, accessed July 11, 2014.

[24] Healthcare IT News, "Small-town Hospital Gets Hacked," March 17, 2014, www.healthcareitnews.com/news/small-town-hospital-gets-hacked, accessed July 11, 2014.

[25] FoxNews, "Community Health Systems Hacked, Records of Nearly 4.5 Million Patients Stolen," August 18, 2014, www.foxnews.com/tech/2014/08/18/community-health-systems-hacked-records-nearly-45-million-patients-stolen/, accessed November 4, 2014.

[26] *Ibid.*

[27] HHS Food and Drug Administration (FDA), "FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Networks," June 13, 2013, www.fda.gov/medicaldevices/safety/alertsandnotices/ucm356423.htm, accessed July 11, 2014.

With the lack of effective mitigation measures, cyberattack consequences will continue to grow as hospitals continue to integrate cyber-technologies into patient care. In April 2014, the Federal Bureau of Investigation (FBI) warned that cyber actors will likely increase cyber intrusions against healthcare systems and medical devices, due to the mandatory transition from paper to electronic health records, lax security standards, and a higher financial payout for medical records on the black market.[30] The Health Insurance Portability and Accountability Act (HIPAA) requires medical facility owners to focus on protecting the confidentiality, integrity, and availability of electronic protected health information (ePHI) which is created, received, maintained, or transmitted by any covered entity against reasonably anticipated threats, hazards, and impermissible use and disclosure. This plays into the importance of resilience where prudent backing-up of medical data and its safeguard, whether in transit or at rest, is due-diligence and a regulatory requirement.

PHYSICAL ATTACKS

Hospitals typically are open-access environments with limited visitor management, which create basic physical security vulnerabilities. Hospitals are typically open 24 hours a day, 7 days a week, 365 days a year. This openness could allow anyone to walk into a hospital or park a vehicle near a hospital without encountering access controls. Although it is necessary for the primary function of a hospital, the free and open access as well as the constant movement of people and materials (e.g., luggage, packages, and supplies) in and out of a hospital facility present numerous security challenges. Nonexistent or weak access control procedures could allow persons with malicious intent to circumvent existing physical security measures and threaten patient or staff safety.[31]

Hospitals often have curbside access to accommodate patient needs. This leaves little ability to enforce bomb threat stand-off distances of greater than 320 feet, allowing for risks from vehicle-borne improvised explosive devices (VBIEDs).[32,33] Some urban hospitals may appear to be attractive soft targets as there may be increased potential for mass casualties, psychological consequences, economic consequences, and lasting damage to critical infrastructure.

---

[28] HHS Food and Drug Administration (FDA), "FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Networks," June 13, 2013, www.fda.gov/medicaldevices/safety/alertsandnotices/ucm356423.htm, accessed July 11, 2014.

[29] Forbes, "Hacking Insulin Pumps and Other Medical Devices from Black Hat," August 3, 2013, www.forbes.com/sites/ericbasu/2013/08/03/hacking-insulin-pumps-and-other-medical-devices-reality-not-fiction/, accessed July 11, 2014.

[30] FBI, Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain,´ PIN#140408-009, April 8, 2014, http://www.aha.org/content/14/140408--fbipin-healthsyscyberintrud.pdf, accessed November 11, 2014.

[31] Valague, E., "2014 Texas Emergency Management Conference: Active Shooter Preparedness and Response in Healthcare Settings," 2013, www.preparingtexas.org/Resources/documents/2013%20Conference%20Presentations/Active%20Shooter%20Preparedness%20and%20Response%20in%20Healthcare%20Settings.pdf, accessed July 11, 2014.

[32] The bomb threat stand-off distance of 320 feet is the recommended mandatory evacuation distance for VBIEDs with the explosives capacity of 500 lbs. (227 kg). Mandatory evacuation distances are governed by the ability of typical U.S. commercial construction to resist damage or collapse following a blast. Performances can vary significantly, however, and buildings should be analyzed by qualified parties when possible. For more information, visit the National Counterterrorism Center (NCTC), www.nctc.gov/site/technical/bomb_threat.html.

[33] DHS, *Bomb Threat Stand-Off Chart*, www.llis.dhs.gov/sites/default/files/DHS-BombThreatChart-6-5-09.pdf.

PUBLIC HEALTH EMERGENCIES

Hospitals also face public health emergencies such as emerging infectious diseases and pandemics. Most people have little to no immunity to such emerging infectious diseases, and as infection and illness rates soar, a substantial percentage of the population will require some form of medical care. Pandemic influenza can spread quickly from person-to-person worldwide, and can rapidly overwhelm hospital surge capacities. A pandemic can create a shortage of anti-viral medications, hospital beds, ventilators, and other supplies. Vaccines may not be available, particularly in the early stages of the pandemic. Hospital employees may also be impacted by travel bans, school and business closings, and caring for sick family members, all of which can result in significant employee absenteeism, which in turn impacts the delivery of patient care.[34,35]

Data Collection and Levels of Facility Degradation

The ECIP initiative collects data through the Infrastructure Survey Tool (IST), a secure Web-based tool that provides the ability to collect, process, and analyze survey data in near–real time. Data collected during site visits are consolidated in the IST and compared against established values, weights, and data on similar facilities, which enables DHS to develop metrics; conduct sector-by-sector and cross-sector vulnerability comparisons; identify security gaps and trends across critical infrastructure sectors and subsectors; and establish sector baselines for security and resilience scores.

The term "dependency," as used in the IST and reported here, is defined as the reliance of a facility on an outside/external utility or service to carry out its "core operations."

Degradation addresses how soon a facility will be affected if the source is lost, and to what extent it will be affected. Data on degradation are gathered in the IST exclusively from other related conditions: 0 percent degradation, 1–33 percent degradation, 34–66 percent degradation, 67–99 percent degradation, or 100 percent degradation.

Data are also collected on the existence of backup generation, duration of backup generation without refueling, and recovery time after external infrastructure service is restored.

DEPENDENCIES, INTERDEPENDENCIES, AND POTENTIAL IMPACTS

The resilience of a region or community is a function of the resilience of its subsystems, including its critical infrastructure, economy, civil society, and governance (including emergency services). Resilience can be highly complex due to the dependencies and interdependencies that exist within infrastructure systems, the regions they serve, and the potential for cascading consequences.

The following sections will discuss the dependencies of hospitals on other sectors and subsectors—particularly Electric Power, Natural Gas, Water and Wastewater Systems, Communications, and Information Technology (IT). The term "dependency," as defined when collecting information as part of an Enhanced Critical Infrastructure Protection (ECIP) Security Survey, is the reliance of a facility on an outside/external utility or service to

[34] FLU.gov, "About Pandemics," www.flu.gov/pandemic/about/, accessed July 11, 2014.

[35] USA Today, "H1N1 Flu 'Pushing Hospitals to Their Limit,'" October 27, 2009, http://usatoday30.usatoday.com/news/health/2009-10-26-swine-flu-hospitals_N.htm, accessed July 11, 2014.

carry out its core operations (e.g., produce key services or goods). Core operations are specific to an asset or facility. Some examples include domestic uses (e.g., potable water), security operations (e.g., electric power for closed circuit television (CCTV), scanners, and sensors), providing on-site heat or hot water (e.g., natural gas). The degradation in service (i.e., to one or more of those core operations) data captures how soon and to what extent a facility will be affected if the source is lost. DHS assessment data from the RRAP and the ECIP Initiative, in which DHS partners with State and local agencies and the private sector to conduct voluntary assessments of a large number of critical infrastructure facilities, was analyzed to determine potential dependencies and resilience of hospitals.[36]

HOSPITAL DEPENDENCIES

Since January 2011, 222 hospitals have been surveyed as part of the ECIP program. As shown in Figure 1, of the hospitals surveyed all responded that they require electric power, and most responded that they are also heavily dependent on water, wastewater treatment, communications, and IT. Transportation dependence was minimal, because multiple roads or other transportation mechanisms exist in order to allow staff and patients to safely arrive at the facilities. Approximately half of the facilities responded that they required chemicals (46 percent) or waste removal (43 percent) to maintain their core operations.

The inner circle in Figure 1 depicts the percentage of surveyed hospitals dependent upon external products and services. The outer ring depicts the percentage that hospital core capabilities are degraded and the time to impact without considering backup measures for those dependent facilities.

ELECTRICITY

Hospitals rely on electricity for their core operations, security operations, as well as for on-site heat, air conditioning, air circulation, and hot water. All but one of the surveyed hospitals had a backup or alternate source of electric power (99 percent). All facilities with a backup had an electric generator, which was most often used for core operations (60 percent).[37] The Joint Commission, a healthcare accreditation organization, requires hospitals be able to run on generator backup for 72 hours.[38] However, many hospitals do not have large on-site fuel reserves nor guaranteed fuel contracts, and during prolonged, widespread power outages such as those following a hurricane or severe winter storm, fueling the backup generators may be problematic.

Uninterruptible power supplies can be critical for patient safety, meant to ensure that critical equipment, such as ventilators, stays operational following an electric power outage.[39] Uninterruptible power supply runtime is typically only a few minutes, but allows time to start up backup power or properly shut-down equipment. 50 percent of the facilities surveyed indicate

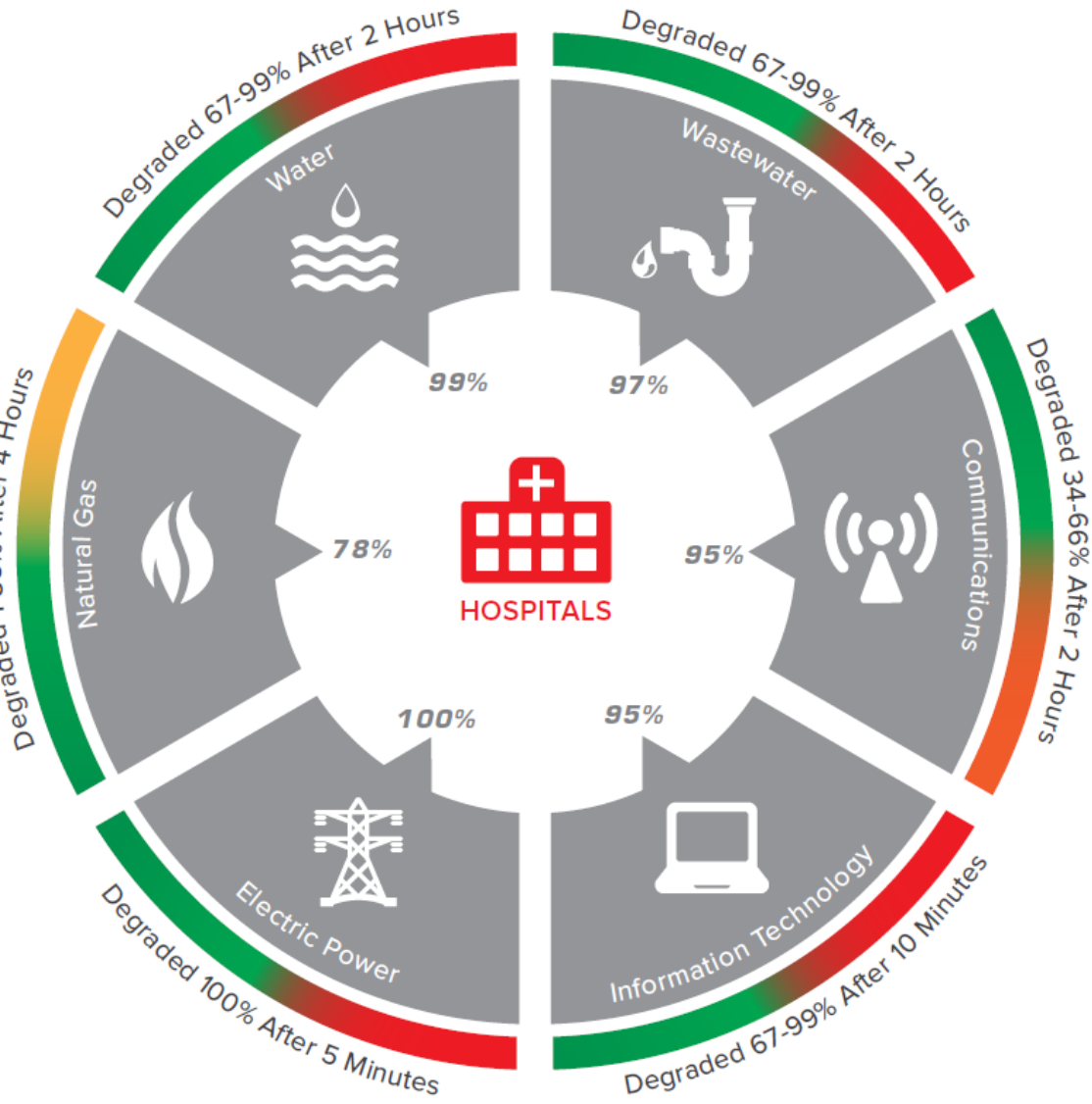
[36] Site assessments under the ECIP and RRAP are voluntary; they may not be representative of the entire sector. The information and data from the RRAP and the Infrastructure Survey Tool (IST, on which the ECIP security survey resides) are often protected as For Official Use Only or as Protected Critical Infrastructure Information; the information provided below has been sanitized to remove any facility, system, or regional references.

[37] In the survey, facilities are asked for the purpose of the backup generator: life safety, graceful shutdown, core operations, or entire facility load.

[38] The Joint Commission accredits and certifies more than 20,500 health care organizations and programs in the United States. www.jointcommission.org/about_us/about_the_joint_commission_main.aspx. accessed December 3, 2014.

[39] Schneider Electric, "Improve Patient Safety Through Power Availability and Reliability," June 2011, www2.schneider-electric.com/documents/support/white-papers/wp_Healthcare_reliability.pdf, accessed July 11, 2014.

they use an uninterruptible power supply for a graceful shutdown, typically of IT and communications systems, while another 35 percent use the uninterruptible power supplies for life safety.



Note: This data represents a majority of hospitals (60 percent or greater) that are dependent on the external product or service.

FIGURE 1—Percent of assessed hospitals dependent upon external products or services, and percent degradation from their loss (Courtesy of DHS and Argonne National Laboratory)

NATURAL GAS

As depicted in Figure 1, though nearly 80 percent of hospitals rely on natural gas for on-site heat, hot water, and food preparation, its loss does not cause as large an impact on the hospital's core functions as the loss of other resources. The impact from the loss of natural gas is very specific

to location and function. For example, if a hospital uses natural gas for heating and it loses the source during a typical northeastern winter, patients may be forced to evacuate after 1–2 days.[40]

WATER AND WASTEWATER

All but three of the 222 surveyed hospitals require external water. The three that stated they do not require external water services have their own internal water treatment plant and wells that can support 100 percent of the facilities' water demands. For those hospitals that do require external water services, these services are required for domestic purposes, core operations (i.e., rinse waters or process water), and 78 percent of the hospitals use water for cooling purposes. The Centers for Disease Control and Prevention (CDC), in conjunction with the American Water Association, recommends stopping nonessential services in the event of a disruption in the main water supply. These services include psychiatric services, elective surgeries, and physical therapy, among others.[41]

Similarly, all but six of the 222 surveyed hospitals required external wastewater service. Hospitals require external wastewater services for domestic (sanitation) purposes. The six that stated they do not require external wastewater services are able to independently provide their own internal wastewater discharge service such as an onsite sewage treatment.

If water and wastewater is significantly degraded more than 48 hours, standards and regulations may require the hospital to shut down. For example, the Joint Commission has established a 96-hour rule under the emergency management standards that requires a hospital to determine if it has sufficient capabilities to sustain itself (independently through backups or by the local community) for 96 hours (including fuel capacity, water for drinking and patient care, or water for process equipment and sanitation and wastewater services).[42] While the Joint Commission's requirements are focused on obtaining accreditation, HHS states in their Hospital Evacuation Decision Guide that, "water loss of unknown duration (more than 1–2 days) is almost always cause for evacuation." Also, the loss of water in support the fire suppression systems may necessitate a complete shutdown much sooner.[43]

COMMUNICATIONS

Hospitals rely on radio, telephone, and data communications for a wide variety of operations (i.e., emergency operations, interoperable communications with emergency services organizations, and business operations). Of the 222 hospitals surveyed, 210 were dependent on external communication sources for operations. Of those that indicated they were dependent on external communications providers, the most critical communication source was data for general business, administration, or customer services function. Survey respondents indicated that loss of data access could degrade hospital functions up to 66 percent without considering backup or alternative measures.

---

[40] HHS, *Hospital Evacuation Decision Guide*, May 2010, http://archive.ahrq.gov/prep/hospevacguide/hospevac.pdf, accessed July 11, 2014.

[41] CDC and American Water Works Association, *Emergency Water Supply Planning Guide for Hospitals and Health Care Facilities*, 2012, www.cdc.gov/healthywater/pdf/emergency/emergency-water-supply-planning-guide.pdf, accessed July 11, 2014.

[42] The Joint Commission, "National Patient Safety Goals," January 1, 2014, www.jointcommission.org/assets/1/6/HAP_NPSG_Chapter_2014.pdf, accessed July 11, 2014.

[43] Agency for Healthcare Research and Quality, "Hospital Evacuation Decision Guide," 2010, www.ahrq.gov/prep/hospevacguide, accessed June 1, 2014.

INFORMATION TECHNOLOGY

Hospitals rely on IT for business operations, clinical information (i.e., medical records), and medical equipment. Of the 222 hospitals surveyed, 210 were dependent on IT. Of those that indicated they were dependent on IT, all indicated they used IT for their business network, and 59 percent responded they also have a control network for supervisory control and data acquisition and process control systems. Loss of IT could degrade hospital functions as much as 99 percent due to inability to access patient records, to monitor and control equipment or to access critical software without considering backup or alternative measures.

In addition to IT's dependence on electric power, it is important to maintain a stable and consistent capability for cooling the network servers that house the electronic health records, communications systems, and automated command and control systems within a hospital. These servers are typically located in closed, secure rooms, and must be kept cool or risk network shut-down due to overheating. This overheating could occur in a matter of minutes without adequate cooling.

RECOVERY MECHANISMS

The assessments conducted by DHS capture information regarding the facilities' recovery mechanisms specific to their dependencies on external utility providers. If the facility assessed is dependent upon an external utility provider, additional information on the backup or alternate utility source, contingency planning, and priority restoration planning are collected to identify the recovery mechanisms in place. Descriptions of each of the recovery mechanisms as well as detailed statistics for the Hospitals Segment are provided in Table 1.

- A facility may have several types of alternatives or backups if there is a loss of the external service source. In some cases, facilities may also have a secondary site to maintain functionality.
- A contingency and business continuity plan with a provider for restoration addresses the service level agreements between the facility and the provider of the external service.
- A priority plan is a list of facilities that will be restored before other facilities, based on the criticality of the services they provide (i.e., human health facilities such as hospitals and nursing homes are often prioritized before other customers).

TABLE 1—Hospital dependencies and recovery mechanisms

Utility Provider Type	Dependent upon External Utility Provider (%)	Backup or Alternate Utility Source (%)	Contingency Plan with Provider (%)	Priority Restoration Plan with Provider (%)
Electric Power	100	99	64	75
Natural Gas	78	58	47	61
Water	99	48	51	61
Wastewater Treatment	97	10	43	48
Communications	95	72	52	57
Information Technology	95	61	59	62

CRITICAL ACCESS HOSPITAL DEPENDENCY VARIATIONS

Of the 222 hospitals surveyed, 24 are critical access hospitals, which are certified as being in a rural area (at least 35 miles from another hospital) and having no more than 25 inpatient beds, as well as comply with additional criteria on length of stay and availability of emergency services.[44] As critical access hospitals are typically the sole local source of patient care in rural communities, loss of external utility services may greatly impact patient care delivery for the community if services are not restored quickly or backups are not in place. Similar to other hospitals, critical access hospitals have heavy reliance on key utilities, however, the amount of facilities that have backups, contingency plans, or priority restoration plans is noticeably lower (Table 2).

[44] Department of Health and Human Services, Centers for Medicare and Medicaid Services, "Critical Access Hospital Fact Sheet," 2013, www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/downloads/CritAccessHospfctsht.pdf, accessed June 1, 2014.

TABLE 2—Critical access hospital dependencies and recovery mechanisms

Utility Provider Type	Dependent upon External Utility Provider (%)	Backup or Alternate Utility Source (%)	Contingency Plan with Provider (%)	Priority Restoration Plan with Provider (%)
Electric Power	100	100	24	41
Natural Gas	86	52	24	36
Water	100	33	24	34
Wastewater Treatment	100	16	24	17
Communications	100	50	14	10
Information Technology	97	33	16	50

IMPACTS TO CRITICAL INFRASTRUCTURE

While hospitals provide critical services to a community, no given community or even sector is directly dependent on hospitals. However, the criticality of a hospital is apparent during domestic incidents and general emergencies. During these events, hospitals typically are the first to become overwhelmed as they serve as surge support to emergency services to triage patients while continuing to provide routine and critical medical care.[45] Hospitals typically train and plan for mass casualty and surge events to ensure staff are prepared to handle these events.

The importance of a hospital and its preparedness becomes even more apparent when the hospital itself is impacted by an event. During the 2011 Joplin, Missouri EF-5 tornado, St. John's hospital sustained a direct hit. Utilities damaged at the hospital included: heating, ventilation, and air conditioning equipment torn off the roof; destroyed generators; broken fire suppression sprinklers systems causing 2-inches of standing water; broken and leaking natural gas lines; and raw sewage pumping into the hospital.[46] This damage rendered St. John's itself a disaster site unfit for continuation of medical treatment and resulted in immediate evacuation and transfer of patients to nearby hospitals and the deployment of triage tents in the parking lot to continue patient care operations. Through the transferring of patients and the eventual use of on-site patient care tents, St. John's, while degraded, was still able to triage and treat some patients, highlighting that hospital patient services are at least somewhat resilient beyond the building itself.

[45] Mehta, S., "Disaster and Mass Casualty Management in a Hospital: How Well Are We Prepared?," J Postgrad Med (52)(2): pp. 89-90, April 2006, www.bioline.org.br/pdf?jp06028, accessed August 1, 2014.

[46] South Dakota Department of Health, "August 2, 2011 Medical Response to Joplin Tornado May 22, 2011," 2011, http://doh.sd.gov/documents/Providers/Prepare/Joplin.pdf, accessed July 28, 2014.

RESILIENCE ISSUES AND BEST PRACTICES

Table 3 presents commonly observed resilience issues and best practices summarized for two categories of users: hospital systems or facilities, and community risk management organizations (i.e., State or local emergency operation centers, emergency managers, public works, utility managers, and disaster relief organizations). The issues and best practices listed in Table 3 were identified in RRAPs, from among the results of ECIP assessments, and from general literature reviews.[47] The information is meant for general application across the Hospitals Segment and affected sectors and customers. The issues and best practices identified may also apply to other regions, facilities or other types of assets. See the Appendix for supporting resources and references.

TABLE 3—Resilience issues and best practices

FOR HOSPITAL SYSTEMS/FACILITIES
Critical utility lines are either co-located with other utility lines, or are unprotected from both manmade and natural disasters
▪ Harden or relocate at-risk critical equipment to prepare for region-specific common natural disasters such as flooding or tornados. ▪ Consider geographically separating utility lines to provide less chance of losing all dependent services in the event of an incident. ▪ Install protective measures, such as bollards, fencing, or electronic security measures, around equipment that is at risk of sabotage or accidents and, if necessary, install fire/blast walls to protect adjacent equipment. ▪ Consider acquiring additional backup or alternative equipment to deliver critical utilities.
Facilities may have not identified preparedness and mitigation measures (e.g., surge support) to respond to the impacts of a catastrophic event
▪ Identify preparedness and mitigation measures to limit the long-term impacts of catastrophic events and improve resilience posture. ▪ Develop plans to meet increased demands and surge support during and after a catastrophic event (i.e., hurricane or multiple-IED attacks.) ▪ Consider developing a regional healthcare disaster recovery plan to address how demands will be met for critical care, trauma, and at-risk patient populations. ▪ Utilize resources from the HHS program for at-risk individuals to implement best practices of outreach and care of at-risk individuals before, during, and following public health emergencies, and the Federal Emergency Management Agency's (FEMA's) Disability Coordinator to strengthen disaster planning for disabled individuals. (See www.phe.gov/Preparedness/planning/abc/Pages/default.aspx, www.phe.gov/Preparedness/legal/pahpa/Documents/pahpa-at-risk-report0901.pdf, or www.fema.gov/pdf/about/odic/written_statement_roth.pdf). ▪ Develop memoranda of agreement with local utility providers (e.g., electric power, water, and telecommunication) to implement priority restoration of services in the event of their loss. ▪ Exercise plans and procedures emphasizing the loss of utilities and plan annually with local providers.
Facilities may lack comprehensive business continuity plans
▪ Develop, train, and test a business continuity plan to enable personnel to respond quickly to potential disasters, increasing the likelihood of quicker restoration of core operations.

[47] The degradation and recovery information and data from the RRAP and the IST are often protected as For Official Use Only or as Protected Critical Infrastructure Information; the information in Table 3 has been sanitized to remove any facility, system, or regional references.

- Communicate plans to all personnel, and conduct frequent training and exercise (especially with first responders).
- Exercise plans with local first responders to ensure familiarity with the facility and emergency procedures in the event of an actual incident.
- Review DHS and FEMA resources for business continuity planning at www.ready.gov/business.

Some facilities lack written comprehensive cybersecurity plans and have not conducted cybersecurity assessments

- Establish a written cybersecurity policy that encompasses critical items such as privacy, data security, network security, email policies, employee responsibilities, incident response and reporting, and policy development and management guidelines.
- Review guides to assist in the development of cyber security plans (e.g., www.transition.fcc.gov/cyber/cyberplanner.pdf).
- Arrange a cybersecurity assessment, many of which are available from Government sources or a third-party private provider at no cost to the facility. The DHS Office of Cybersecurity and Communications (CS&C) conducts voluntary cybersecurity assessments to evaluate operational resilience and cybersecurity capabilities within all 16 critical infrastructure sectors as well as State, local, Tribal and Territorial governments. For more information visit www.us-cert.gov/ccubedvp/self-service-crr, or contact the program directly at CSE@hq.dhs.gov.
- Identify alternative backup computer server and data management center locations in an offsite location to enhance redundancy. Utilize data management experts to identify offsite storage locations.
- Tailor cybersecurity policies and configurations for the supervisory control and data acquisition (SCADA) network in accordance with guidelines established in formal cybersecurity guidance such as the National Institute of Standards and Technology (NIST) Special Publications 800-series, ISO/IEC 27001, CoBIT, ITIL (http://csrc.nist.gov/publications/PubsSPs.html).

Customers need to be informed of evacuation and shelter procedures

- Hospitals should create emergency action charts and post them throughout the facilities for quick reference of actions to take during emergency situations.
- Hospitals should clearly identify and communicate egress routes in the event of a mass evacuation.
- Hospitals should clearly identify shelter-in-place locations in the event of a disaster in which evacuation is not an option.

FOR COMMUNITY RISK-MANAGEMENT ENTITIES

Facilities lack local, regional planning for mitigation and redundancy efforts

- Develop a hospital resilience checklist that identifies critical infrastructure redundancies that exist at other hospitals and communities which could strengthen their disaster mitigation programs.
- Conduct drills to test the ability of local hospitals to provide temporary medical care in staging areas while patients are awaiting transport to receiving hospitals during a no-notice evacuation event.
- Identify how staging areas or assembly points will protect critical care patients. (See www.hsph.harvard.edu/policy-translation-leadership-development/files/2013/05/MDPH-Hospital-Evacuation-Toolkit2.pdf).

Community plans addressing holistic preparedness and resource shortages are lacking

- Form a Catastrophic Healthcare Recovery Committee (CHRC) with hospital and government officials that would identify emergency transportation alternatives.
- Develop and/or revise public and private entity catastrophic recovery plans.
- Organize a series of exercises to test mass-evacuation and mass-care plans.

APPENDIX

RESILIENCE ISSUES AND BEST PRACTICES: REFERENCES AND RESOURCES

The following references provide the reader with more in-depth information on the Hospitals Segment, including vulnerabilities, gaps, resilience technology, and other sector-specific guidance.

American Hospital Association

- *Fast Facts on U.S. Hospitals*, www.aha.org/research/rc/stat-studies/fast-facts.shtml.
- *The Fragile State of Critical Access Hospitals—Infographic*, www.aha.org/content/13/infographic-cah.pdf.

American Hospital Directory

- *Hospital Statistics by State*, www.ahd.com/state_statistics.html.

American Trauma Society

- *Trauma Categorization Explained*, www.amtrauma.org/resources/trauma-categorization/index.aspx.

Argonne National Laboratory

- *Resilience: Theory and Applications*, www.dis.anl.gov/pubs/72218.pdf.

Boston Green Ribbon Commission

- *Powering the Future of Health Care, Financial and Operational Resilience: A Combined Heat and Power Guide for Massachusetts Hospital Decision Makers*, www.greenribboncommission.org/downloads/CHP_Guide_091013.pdf.

Centers for Disease Control and Prevention

- *Planning Resources by Setting: Hospitals and Healthcare Systems*, www.cdc.gov/phpr/healthcare/hospitals.htm.
- *First Human Avian Influenza A (H5N1) Virus Infection Reported in Americas*, www.cdc.gov/flu/news/first-human-h5n1-americas.htm.
- *Hospital Discussion Guide for Pandemic Influenza Planning*, www.cdc.gov/phpr/healthcare/documents/Discussion_Guide_for_Hospitals.pdf.
- *Emergency Water Supply Planning Guide for Hospitals and Health Care Facilities*, www.cdc.gov/healthywater/pdf/emergency/emergency-water-supply-planning-guide.pdf.

Department of Homeland Security

- *National Infrastructure Protection Plan 2013, Partnering for Critical Infrastructure Security and Resilience*, www.dhs.gov/national-infrastructure-protection-plan.
- *Presidential Policy Directive 8: National Preparedness* (PPD-8), www.dhs.gov/presidential-policy-directive-8-national-preparedness.

- *Healthcare and Public Health Sector-Specific Plan*, www.dhs.gov/xlibrary/assets/nipp-ssp-healthcare-and-public-health-2010.pdf.
- *Critical Infrastructure Cyber Community (C^3) Voluntary Program* helps critical infrastructure sectors and organizations reduce and manage their cyber risk by connecting them to existing cyber risk management capabilities provided by DHS, other U.S. Government organizations, and the private sector. At the time of launch in February 2014, available resources primarily consisted of DHS programs, which will grow to include cross-sector, industry, and State and local resources. Available at www.us-cert.gov/ccubedvp.
- *Office of Health Affairs*, www.dhs.gov/office-health-affairs.
- *National Biosurveillance Integration Center (NBIC),* www.dhs.gov/national-biosurveillance-integration-center.
- *Pandemic Influenza, Preparedness, Response, and Recovery: Guide for Critical Infrastructure and Key Resources,* 2006, www.flu.gov/planning-preparedness/business/cikrpandemicinfluenzaguide.pdf.

Department of Health and Human Services

- *Critical Access Hospitals*, www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/downloads/CritAccessHospfctsht.pdf.
- *What are Critical Access Hospitals?*, www.hrsa.gov/healthit/toolbox/RuralHealthITtoolbox/Introduction/critical.html.
- *About the Flu*, www.flu.gov/about_the_flu/index.html.
- *Public Health Emergency: Public Health and Medical Emergency Support for a Nation Prepared,* www.phe.gov/preparedness/Pages/default.aspx.

Federal Emergency Management Agency

- *Texas Medical Center Task Force Tropical Storm Allison Final Report*, available at the Harris County (Texas) Flood Control District, www.hcfcd.org/downloads/reports/TS-Allison_PubReportENGLISH.pdf.
- *Security Risk Management Publications*, www.fema.gov/what-mitigation/security-risk-management-series-publications.

Flex Monitoring Team

- *Critical Access Hospital Locations,* www.flexmonitoring.org/data/critical-access-hospital-locations.

Food and Drug Administration (FDA)

- *FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Networks*, www.fda.gov/medicaldevices/safety/alertsandnotices/ucm356423.htm.

Rural Assistance Center

- *Critical Access Hospitals*, www.raconline.org/topics/critical-access-hospitals.

U.S. Department of Labor Occupational Safety and Health Administration (OSHA)

- *Hospital eTool*, www.osha.gov/SLTC/etools/hospital.

The Office of Cyber and Infrastructure Analysis (OCIA) produces Sector Resilience Reports to improve partner and stakeholder understanding of the interdependencies and resilience of certain aspects of specific sectors. The information is provided to support the activities of the Department, and to inform Federal, State, local, and private-sector partner strategies designed to deter, prevent, preempt, and respond to all-hazards disruptions to infrastructure in the United States. For more information, contact OCIA@hq.dhs.gov or visit www.dhs.gov/office-cyber-infrastructure-analysis.