

Special Focus

# INSIDIOUS SCOURGE

CRITICAL INFRASTRUCTURE  
AT BIOLOGICAL RISK

A REPORT BY THE  
BIPARTISAN COMMISSION ON BIODEFENSE

*October 2021*



**BIPARTISAN  
COMMISSION  
ON BIODEFENSE**

SPECIAL FOCUS

# **INSIDIOUS SCOURGE**

CRITICAL INFRASTRUCTURE  
AT BIOLOGICAL RISK

A REPORT BY THE  
BIPARTISAN COMMISSION ON BIODEFENSE

*October 2021*





Copyright © 2021 by the Bipartisan Commission on Biodefense.

All rights reserved.

[www.biodefensecommission.org](http://www.biodefensecommission.org)

Graphics and design by Factor3 Digital.

Base cover image courtesy of Shutterstock.com.

#### **SUGGESTED CITATION**

Bipartisan Commission on Biodefense. (2021). *Insidious Scourge: Critical Infrastructure at Biological Risk*. Bipartisan Commission on Biodefense: Washington, DC.

## **COMMISSIONERS**

Joseph I. Lieberman, Chair

Thomas J. Ridge, Chair

Donna E. Shalala

Thomas A. Daschle

James C. Greenwood

Kenneth L. Wainstein

## **EX OFFICIO MEMBERS**

Yonah Alexander, PhD

William B. Karesh, DVM

Rachel Levinson, MA

Lewis Libby, JD

Gerald W. Parker, DVM, PhD

George Poste, DVM, PhD, DSc

Tevi Troy, PhD

## **STAFF**

Asha M. George, DrPH, Executive Director

John T. O'Brien, MS, Research Associate

Robert H. Bradley, Policy Associate

Patricia de la Sota, Operations Manager

# TABLE OF CONTENTS

**EXECUTIVE SUMMARY** .....1

**CASE STUDY: IMPACT OF ANTHRAX 2001 ON CRITICAL INFRASTRUCTURE** ..... 5

**CRITICAL INFRASTRUCTURE AND FUNCTIONS AT BIOLOGICAL RISK** .. 9

**BIODEFENSE OF CRITICAL INFRASTRUCTURE** ..... 15

**APPENDIX: RECOMMENDATIONS BY SECTOR** ..... 23

    CHEMICAL SECTOR.....24

    COMMERCIAL FACILITIES SECTOR.....26

    COMMUNICATIONS SECTOR.....28

    CRITICAL MANUFACTURING SECTOR.....30

    DAMS SECTOR.....32

    DEFENSE INDUSTRIAL BASE SECTOR.....34

    EMERGENCY SERVICES SECTOR.....36

    ENERGY SECTOR.....38

    FINANCIAL SERVICES SECTOR.....40

    FOOD AND AGRICULTURE SECTOR.....42

    GOVERNMENT FACILITIES SECTOR.....44

    HEALTHCARE AND PUBLIC HEALTH SECTOR .....46

    INFORMATION TECHNOLOGY SECTOR .....48

    NUCLEAR REACTORS, MATERIALS, AND WASTE SECTOR..... 50

    TRANSPORTATION SYSTEMS SECTOR .....52

    WATER AND WASTEWATER SECTOR .....54

**ACRONYMS** ..... 56

**ENDNOTES**..... 57

## ACKNOWLEDGMENTS

The Commission appreciates the willingness of critical infrastructure owners and operators to share their biodefense concerns and priorities with us. We greatly appreciate the perspectives of Henrik Birk, Bavarian Nordic; Jason Blumenauer, Cardinal Health, Inc.; Joe Coomer, AMB Sports and Entertainment; Dr. Malick Diaria, ExxonMobile Corporation; Terrell Harris, FedEx Corporation; Sara Roszak, National Association of Chain Drug Stores; and David Stoltzfus, Monsanto. We thank Ann Beauchesne and Jennifer Stone, President, Partner Forces, for their insights regarding critical infrastructure risk management. We thank our ex officio members for their advice and input. The Commission also gratefully acknowledges the financial support provided by our donors, and Hudson Institute, which serves as our fiscal sponsor.



# EXECUTIVE SUMMARY

Critical infrastructure and national critical functions are threatened by, vulnerable to, and experience the consequences of biological attacks, accidents, and naturally occurring diseases—in other words, they are at biological risk. Biological events could destroy, incapacitate, and disrupt critical infrastructure and prevent our society from both functioning properly and protecting itself. Illness and death, physical compromise of sectors, data theft and compromise, just-in-time inventories, mass gatherings, unprotected transit and other distribution systems, and poor awareness of where and how diseases spread are all of concern. When biological events overwhelm critical infrastructure, effects on society cascade, further weakening our country.

## Each critical infrastructure sector must:

- Maintain awareness of biological threats;
- Understand how and where they are vulnerable to biological threats;
- Predict the consequences of a variety of biological events that would affect their sectors if they occurred;
- Prevent and deter biological events from occurring that affect their sectors;
- Prepare for biological events;
- Detect biological events when they occur at or near their facilities;
- Respond to biological events efficiently and effectively;

## CRITICAL INFRASTRUCTURE

**16** sectors composed of physical and virtual assets, systems, and networks vital to national security, economic security, and public health and safety

## NATIONAL CRITICAL FUNCTIONS

**55** public and private sector functions that the United States requires for the economy and national public health, safety, and security

- Work with law enforcement and public health officials, as well as corporate security professionals, as they investigate the cause and nature of these events;
- Coordinate with public and private sector owners and operators to help their facilities and the communities in which these facilities reside to recover from biological events; and
- Mitigate the impact of future biological events by emplacing protections and measures to help sector facilities and personnel withstand biological attacks, accidental releases of organisms, and naturally occurring outbreaks.

The Commission held a special focus meeting in July 2018 at the U.S. Chamber of Commerce to examine the impact of large-scale biological events on business, finance, and the economy. Chaired by former Representative Jim Greenwood and former Senate Majority Leader Tom Daschle, the meeting featured experts who addressed biological risk to the Commercial Facilities Sector, Financial Services Sector, Food and Agriculture Sector, Healthcare and Public Health Sector, and Transportation Systems Sector. They described financial impacts of large-scale biological incidents, public-private partnerships, collaboration in advance of biological events, and what/how critical infrastructure owners and operators contribute to biodefense.

Based on input received during that meeting and additional research conducted thereafter, the Commission developed the following policy recommendations to strengthen the ability of the critical infrastructure community to reduce biological risk by protecting infrastructure, sharing and securing information, maintaining public works and services, and ensuring public health and safety. The Commission's recommendations build on those found in the Commission's 2015 report, *A National Blueprint on Biodefense: Leadership and Major Reform Needed to Optimize Efforts (Blueprint for Biodefense)* and subsequent Commission publications.

## NEW RECOMMENDATIONS for Biodefense of Critical Infrastructure

- Congress should mandate federal defense of critical infrastructure against biological threats.
- The Administration should establish a critical infrastructure biodefense program at the Department of Homeland Security.
- The Department of Homeland Security, sectors, and sector specific federal agencies should plan to protect critical infrastructure operators and ensure continued national critical functions during biological events.
- Sectors and sector specific federal agencies should maintain awareness of the disease environment in which critical infrastructure operates.
- Sectors and sector specific federal agencies should identify and eliminate vulnerabilities in critical infrastructure to biological threats.

- Sectors and sector specific federal agencies should take action to reduce the impact of biological events before they occur again.
- Sectors and sector specific federal agencies should ensure execution of national critical functions by taking sector-specific actions.

**SEE APPENDIX FOR SPECIFIC RECOMMENDATIONS  
FOR EACH CRITICAL INFRASTRUCTURE SECTOR.**

Novel coronavirus 2019 (COVID-19) continues to cause pain and suffering throughout the United States and the world. Our Nation's critical infrastructure is still functioning in the face of this disease, but it is not standing firm. The Administration, Congress, and critical infrastructure sector owners and operators can head off the sort of complex humanitarian emergency characteristic of failed nation-states by taking necessary, targeted actions. The federal government needs to exert leadership and work with its private sector and international partners to manage and reduce biological risk to critical infrastructure now. We must protect that which enables our society to function from the diseases that threaten the Nation today, and will continue to threaten it in the future.



## CASE STUDY

# IMPACT OF ANTHRAX 2001 ON CRITICAL INFRASTRUCTURE

In the late 1990s, President William J. Clinton was made aware of the biological threat to the United States and directed the federal government to take action to prepare for naturally occurring pandemics and biological attacks. Separately, he was briefed about multiple threats to the Nation's critical infrastructure and made infrastructure protection a top priority. Although the Clinton Administration issued several directives and executive orders addressing each of these threats,<sup>1</sup> they did not specifically direct the infrastructure community to help defend the Nation against, or address its collective vulnerability to, biological threats.

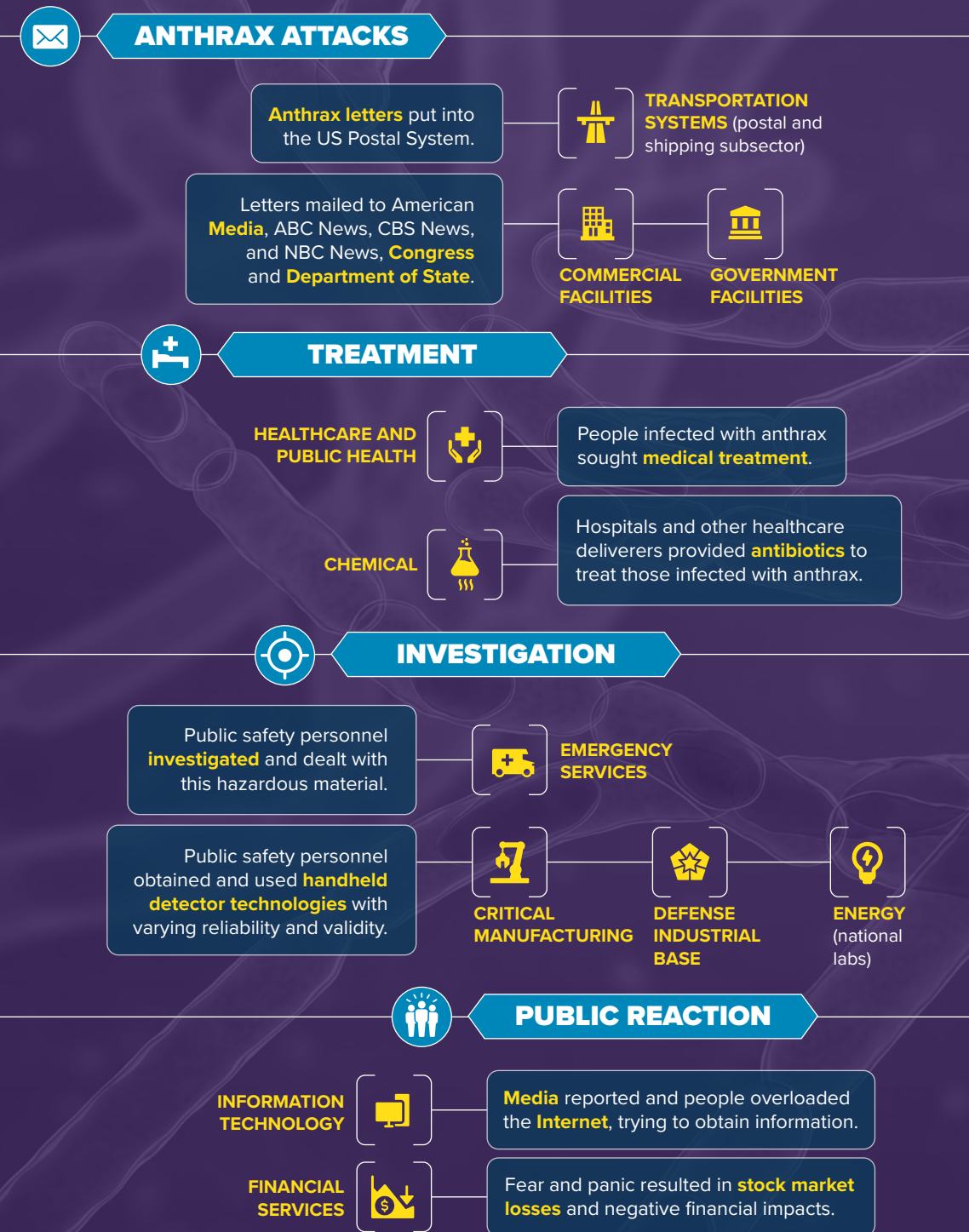
By the time the anthrax events occurred in 2001, however, the healthcare, law enforcement, military, and public health communities had already begun developing and implementing biodefense programs, including preparedness for an attack using weapons-grade biological agents (e.g., anthrax, brucellosis, botulism, plague, tularemia).<sup>2</sup> Despite understanding that large-scale biological events (e.g., pandemic influenza) would reduce the number of people able to operate critical infrastructure at capacity, most critical infrastructure sectors neither engaged in biodefense nor determined how they would continue to operate during biological events. As a result, when the anthrax events of 2001 occurred, the critical infrastructure sectors were caught unaware and unprepared.

Beginning with the first mailing on September 18, 2001, the anthrax letters impacted critical infrastructure. Letters were mailed in the U.S. Postal Service (USPS) and arrived at the offices of American Media in Boca Raton and NBC News in New York City, infecting people there who went to local hospitals. The letters disrupted activities at these organizations that are part of the **Commercial Facilities Sector**, shutting down newsrooms and media activities for organizations that were not accustomed to shifting operations to other sites.

Local and federal law enforcement begin investigating these acts of terrorism. These investigations added greatly to workload for these elements of the **Emergency Services Sector**, not just in Florida and New York, but throughout the Nation. Investigating biological incidents is never easy or straightforward, and at the time, the law enforcement community lacked needed science and technology to be able to quickly attribute the source and intent behind these events. The demand for handheld equipment capable of detecting biological agents (including, but not limited to anthrax) far outpaced the



Figure 1. Impact of the Anthrax Events of 2001 on Critical Infrastructure



ability of the **Critical Manufacturing Sector** and the **Defense Industrial Base Sector** to provide or produce such technology that generated valid and reliable results (a challenge that continues today). Some of the national laboratories assisted with law enforcement investigations and the application of science to better understand the characteristics of the anthrax used in these attacks, forcing these elements of the **Energy Sector** to divert time and attention to emergency response.

About a month after the initial letters were mailed, more letters containing anthrax arrived on Capitol Hill on October 15, including to the offices of former Senate Majority Leader Tom Daschle and Senator Patrick Leahy. More people were subsequently exposed to anthrax at CBS News (further affecting the Commercial Facilities Sector), postal facilities in Hamilton, NJ and Brentwood, Washington, DC, and a mailing room at the Department of State. The letters to Senator Daschle and Senator Leahy shut down the Hart Senate Office Building and greatly impeded Congressional business for many months afterwards. The letters also forced the postal and shipping subsector of the **Transportation Systems Sector** to stop operations in Brentwood and Hamilton and investigate whether other facilities were or could be affected. The appearance of a letter containing anthrax at the Department of State added to the impact on the **Government Facilities Sector**.

Public health officials sent alerts to the human and animal healthcare communities. Clinical, local, state, and federal laboratories conducted laboratory testing. Of the 22 people infected, 5 died and 17 recovered from illness due to inhaling anthrax. The demand for Ciprofloxacin and Doxycycline (two antibiotics used to treat patients with anthrax) skyrocketed, creating an unforeseen demand on the pharmaceutical subsector of the **Chemical Sector** (and Healthcare and Public Health Sector) that it could not meet immediately. The anthrax letters also placed an enormous burden on the **Healthcare and Public Health Sector**. The limited capacity of the public health community to respond placed a great strain on federal and non-federal assets alike, draining already limited budgets and human resources.

While more anthrax letters were sent and cross-contamination of mail began infecting people who were not intended recipients of the original letters, public demand for information exceeded that provided by the government and the media. The public turned to the Internet, greatly increasing the load on servers, generating opportunities for the spread of misinformation and disinformation, and creating enormous inefficiencies in the **Information Technology Sector**. The instability produced by poor communications and Internet-driven mass panic affected the stock market and became an issue with which the **Financial Services Sector** had to contend, especially after the discovery that anthrax could survive on banknotes.

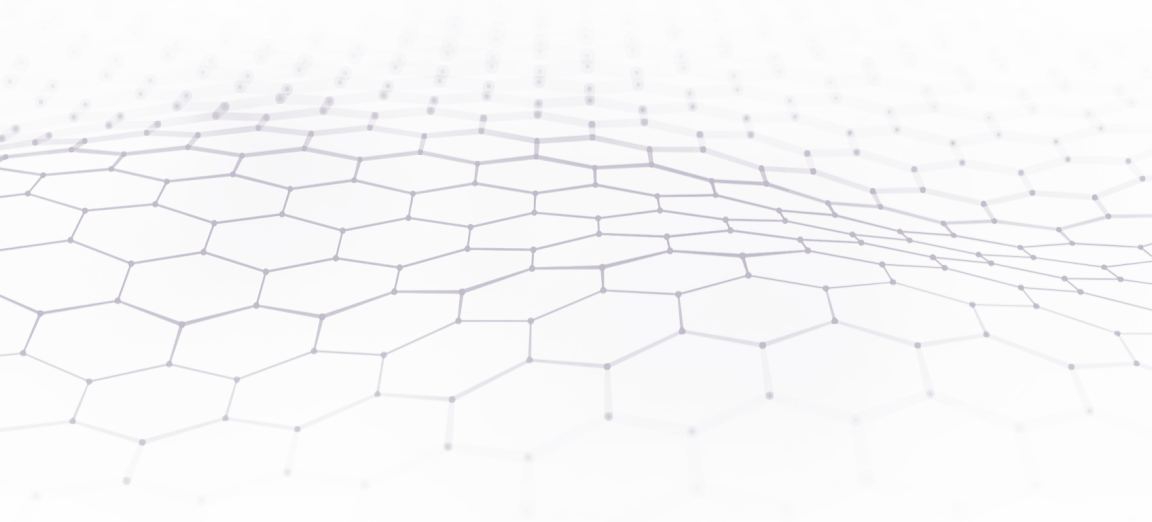
Over the course of the next seven years, law enforcement, postal service, and public health investigations continued. On July 29, 2008, Bruce E. Ivins (a scientist who conducted research at the U.S. Army Medical Research Institute of Infectious Diseases



in Fort Detrick, Maryland), suspected of perpetrating these attacks, committed suicide. Scientific reviews continued until the Department of Justice, Federal Bureau of Investigation (FBI), and U.S. Postal Inspection Service formally concluded their investigation in 2010, almost nine years after the letters were originally mailed.<sup>3</sup>

The cost of testing, remediation, and prevention of further anthrax contamination exceeded \$1 billion.<sup>4</sup> These costs included \$320 million for decontamination<sup>5</sup> and \$177 million for medical services.<sup>6</sup>

The anthrax events of 2001 impacted 11 critical infrastructure sectors. All 16 critical infrastructure sectors remain at biological risk today.



# CRITICAL INFRASTRUCTURE AND FUNCTIONS AT BIOLOGICAL RISK

There are certain physical and virtual assets, systems, and networks, as well as certain public and private sector functions, that the United States requires for national public health, safety, security, and economy. We use the terms critical infrastructure<sup>7</sup> and national critical functions,<sup>8</sup> respectively, to describe these, noting that their destruction, incapacitation, disruption, corruption, or dysfunction would negatively impact our society. Infrastructure security utilizes both constructs to protect and enable our society to function.

Utilities and their extensions (e.g., power stations, the energy grid) often come to mind immediately when talking about critical infrastructure, but 16 different sectors comprise critical infrastructure (see Figure 2) and 55 activities comprise the national critical functions set (see Figure 3). Most have little more in common than the labels and value we place on their contributions to society, except when various critical infrastructure sectors work together to execute different national critical functions. For example, the effective execution of the national critical function to provide medical care requires the efforts of the Healthcare and Public Health Sector, and the contributions of ten other sectors.<sup>9</sup>

The critical infrastructure sectors and national critical functions are all at biological risk (see Figure 4). Obviously, the illnesses and deaths associated with large-scale biological events affect critical infrastructure operators the same as with the rest of the population. For this reason, in March 2020, towards the beginning of the novel coronavirus 2019 (COVID-19) pandemic, the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) issued guidance regarding the essential critical infrastructure workforce to address this vulnerability.<sup>10</sup> Previously, the DHS Office of Infrastructure Protection examined the impact of pandemic influenza on critical infrastructure, determining that such a pandemic could greatly impact available manpower. However, the biological risk to critical infrastructure is not limited solely to manpower considerations.

**Figure 2: Critical Infrastructure Sectors**

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater

**Figure 3: National Critical Functions<sup>11</sup>**

CONNECT	
<ul style="list-style-type: none"> <li>Operate Core Network</li> <li>Provide Cable Access Network Services</li> <li>Provide Internet Based Content, Information, and Communication Services</li> <li>Provide Internet Routing, Access, and Connection Services</li> </ul>	<ul style="list-style-type: none"> <li>Provide Positioning, Navigation, and Timing Services</li> <li>Provide Radio Broadcast Access Network Services</li> <li>Provide Satellite Access Network Services</li> <li>Provide Wireless Access Network Services</li> <li>Provide Wireline Access Network Services</li> </ul>
DISTRIBUTE	
<ul style="list-style-type: none"> <li>Distribute Electricity</li> <li>Maintain Supply Chains</li> <li>Transmit Electricity</li> <li>Transport Cargo and Passengers by Air</li> <li>Transport Cargo and Passengers by Rail</li> </ul>	<ul style="list-style-type: none"> <li>Transport Cargo and Passengers by Road</li> <li>Transport Cargo and Passengers by Vessel</li> <li>Transport Materials by Pipeline</li> <li>Transport Passengers by Mass Transit</li> </ul>
MANAGE	
<ul style="list-style-type: none"> <li>Conduct Elections</li> <li>Develop and Maintain Public Works and Services</li> <li>Educate and Train</li> <li>Enforce Law</li> <li>Maintain Access to Medical Records</li> <li>Manage Hazardous Materials</li> <li>Manage Wastewater</li> <li>Operate Government</li> <li>Perform Cyber Incident Management Capabilities</li> <li>Prepare for and Manage Emergencies</li> <li>Preserve Constitutional Rights</li> <li>Protect Sensitive Information</li> <li>Provide and Maintain Infrastructure</li> <li>Provide Capital Markets and Investment Activities</li> </ul>	<ul style="list-style-type: none"> <li>Provide Consumer and Commercial Banking Services</li> <li>Provide Funding and Liquidity Services</li> <li>Provide Identity Management and Associated Trust Support Services</li> <li>Provide Insurance Services</li> <li>Provide Medical Care</li> <li>Provide Payment, Clearing, and Settlement Services</li> <li>Provide Public Safety</li> <li>Provide Wholesale Funding</li> <li>Store Fuel and Maintain Reserves</li> <li>Support Community Health</li> </ul>
SUPPLY	
<ul style="list-style-type: none"> <li>Exploration and Extraction of Fuels</li> <li>Fuel Refining and Processing Fuels</li> <li>Generate Electricity</li> <li>Manufacture Equipment</li> <li>Produce and Provide Agricultural Products and Services</li> <li>Produce and Provide Human and Animal Food Products and Services</li> <li>Produce Chemicals</li> </ul>	<ul style="list-style-type: none"> <li>Provide Metals and Materials</li> <li>Provide Housing</li> <li>Provide Information Technology Products and Services</li> <li>Provide Material and Operational Support to Defense</li> <li>Research and Development</li> <li>Supply Water</li> </ul>

















The malfunctioning of some sectors could exacerbate the impact of a biological event. For example, the physical compromise of Dams Sector water retention facilities could result in standing water that attracts mosquitoes and other vectors of disease. Physical compromise of the Water and Wastewater Systems Sector could result in inadequate water treatment and the continued presence of disease-causing organisms. Physical compromise of laboratories that work with organisms in the Chemical Sector, Food and Agriculture Sector, and Healthcare and Public Health Sector could result in the release of organisms to surrounding environments.

Cybersecurity compromises could create confusion and result in the theft of intellectual property and other information during disease outbreaks when clarity and trustworthy data are most needed. To manage disease and prevent its spread, we need to know where it is; how many people, animals, and/or plants have been infected; how many medicines and essential medical supplies we have on hand and inbound to the country; what organism we are dealing with; and what countermeasures are, or could be, effective in preventing and treating the disease. Stealing, corrupting, or changing data by compromising the Information Technology Sector, Food and Agriculture Sector, and Healthcare and Public Health Sector could produce disastrous results and render the Nation incapable of responding effectively. Additionally, malevolent disruption of the information technology systems used by the Healthcare and Public Health Sector and the Food and Agriculture Sector could delay the identification of organisms and hamper the ability of these sectors to track the spread of disease.

COVID-19 revealed the hyper-efficient but just-in-time nature of the global supply chains. Having been optimized for non-pandemic conditions, supply chains could not keep up with pandemic demands. In most cases, only two days of additional inventory were in transit throughout the world before the pandemic began. COVID-19 disrupted (in some cases, severely) supply chains delivering resources needed to develop medical countermeasures by the Chemical Sector and Healthcare and Public Health Sector; produce diagnostic tests and equipment by the Critical Manufacturing Sector and Nuclear Reactors, Materials, and Waste Sector; and provide medical care by the Emergency Services Sector and Healthcare and Public Health Sector. The Nation still suffers from shortages of ventilators and other medical devices, having found that we cannot obtain them from other countries or produce them in sufficient quantities ourselves. While availability of other supplies seems to have returned to pre-pandemic levels, the supply chains carrying them do so tenuously.

All critical infrastructure sectors are targets for biological attacks, but some are more attractive than others. The Commercial Facilities Sector and the Government Facilities Sector host gatherings that are a matter of national pride and identity. Large-scale, high-profile events such as the Super Bowl (held at a commercial venue) and July 4 celebrations (held at public venues, such as the National Mall) make attractive targets and

**Figure 4. Source of Biological Risk by Critical Infrastructure Sector**

SECTOR	AT BIOLOGICAL RISK	COULD BE USED TO SPREAD DISEASE	HOUSE ORGANISMS
 COMMUNICATIONS	●		
 ENERGY	●		
 INFORMATION TECHNOLOGY	●		
 NUCLEAR REACTORS, MATERIALS, AND WASTE	●		
 COMMERCIAL FACILITIES	●	●	
 DAMS	●	●	
 EMERGENCY SERVICES	●	●	
 FINANCIAL SERVICES	●	●	
 CHEMICAL	●	●	●
 CRITICAL MANUFACTURING	●	●	●
 DEFENSE INDUSTRIAL BASE	●	●	●
 FOOD AND AGRICULTURE	●	●	●
 GOVERNMENT FACILITIES	●	●	●
 HEALTHCARE AND PUBLIC HEALTH	●	●	●
 TRANSPORTATION SYSTEMS	●	●	●
 WATER AND WASTEWATER	●	●	●

have long been of concern. A biological event affecting key elements of the Government Facilities Sector (e.g., Congress) could greatly affect continuity of government and possibly continuity of society.

Biological attacks on/using subway systems and other modes of transportation are also worrisome and have been modeled<sup>12</sup> with exercises occurring in subway systems as far back as the 1960s.<sup>13</sup> Influenza virus can survive on banknotes, which suggests that other organisms, including some biological agents, could use the Financial Services Sector to spread disease intentionally.<sup>14</sup> Even without spreading disease through the sector, a significant biological event would result in the stock market dropping dramatically in a very short period of time, greatly affecting the Financial Services Sector as well as the national and global economies. A biological attack on agriculture (including food), would create shortages in the Food and Agriculture Sector.

Some sectors would have higher rates of exposure to a disease because they would be involved in the treatment and care of the exposed and ill. People and animals seeking treatment would increase risk to the Emergency Services Sector, Food and Agriculture Sector, and Healthcare and Public Health Sector workforces. Our Nation's hospitals ran close to capacity on a daily basis before COVID-19 and during the worst of the pandemic, the Healthcare and Public Health Sector had to run over capacity. Police, firefighters, and paramedics responding to other emergencies occurring in disease-ridden areas also put the Emergency Services Sector at greater risk of exposure, especially when not informed by the Food and Agriculture Sector and the Healthcare and Public Health Sector as to the geographic location of diseases and where they are expected to spread.

When it comes to a biological event and the spread of disease, it is highly unlikely that just one sector will be affected. An event might affect a few sectors directly, with cascading and indirect impacts affecting other critical infrastructure sectors. Further complicating matters, multiple sectors often need to execute national critical functions together. A biological event could affect sectors in different ways and to varying extents, making it impossible for them to pull together efficiently.

The biological risk to critical infrastructure is too great to ignore. As biological events continue to threaten the Nation, we must defend critical infrastructure against biological threats, eliminate sector vulnerabilities to disease, and prevent consequences for society that would weaken our country.



# BIODEFENSE OF CRITICAL INFRASTRUCTURE

With the passage of the Homeland Security Act in 2002, Congress made DHS responsible for protecting critical infrastructure and working in concert with other federal departments and agencies with particular responsibilities for certain sectors (referred to as sector specific agencies or sector risk management agencies). DHS is also the (or a) Sector Risk Management Agency for 10 sectors.<sup>15</sup> DHS began reducing biological risk to critical infrastructure when former Secretary of Homeland Security Janet Napolitano assigned this responsibility to the DHS Office of Infrastructure Protection. This office did not establish a formal biodefense program, but leadership did assign a few personnel and resources to reduce biological risk to critical infrastructure. For slightly more than a decade, the Office of Infrastructure Protection and later CISA:

- Reported biological incidents that affected critical infrastructure;
- Coordinated critical infrastructure responses to biological incidents;
- Protected chemical facilities from biological threats;
- Reached out to, and assessed the vulnerability of, critical infrastructure facilities that house biological materials;
- Maintained awareness of biological threats to special events and mass gatherings;
- Shared biological information with the sectors;
- Lead and coordinated the installation of biological detection systems in some high value critical infrastructure;
- Provided input to national and DHS policy documents that addressed the biological threat to critical infrastructure in part or whole;
- Established partnerships to address biological risk for critical infrastructure;
- Implemented (working with private sector critical infrastructure partners) DHS biological incident preparedness requirements;
- Provided input to DHS management regarding vaccination requirements for first responders and other critical infrastructure personnel that would be called upon to respond immediately during biological events;
- Informed the prioritization of vaccine allocations to the sectors;
- Conducted biological risk assessments and estimates;
- Provided biological modeling, simulation, and analysis;
- Identified Infrastructure of Concern affected by biological incidents; and
- Conducted Enhanced Critical Infrastructure Protection security surveys.

Ten years after these activities began, COVID-19 came to the United States. CISA realized that the pandemic would create shortages of human and other resources, making it difficult for any of the critical infrastructure sectors to operate at normal capacity and impeding the execution of national critical functions. The Commission commends CISA for developing and releasing guidance to identify those essential positions in each sector that were of greatest need of immediate protection.<sup>16</sup> The Commission also believes, however, that CISA and each of the sectors could have managed the biological risk posed by COVID-19 much earlier had they maintained the risk reduction activities described above.

CISA must eliminate the inefficiency created by only occasionally assessing, reducing, and managing biological risk to U.S. critical infrastructure and the effective execution of national critical functions. In accordance with *A National Blueprint for Biodefense*<sup>17</sup> the Commission now makes the following new recommendations:

### **RECOMMENDATION: Congress should mandate federal defense of critical infrastructure against biological threats.**

DHS cannot ensure biodefense of all critical infrastructure sectors and reduce the impacts of biological events on national critical functions by itself. Therefore, Congress should direct the Secretary of Homeland Security, in coordination with the Secretary of Agriculture, Secretary of Defense, Secretary of Energy, Secretary of Health and Human Services, Secretary of Transportation, Secretary of the Treasury, Administrator of the Environmental Protection Agency, Administrator of the Food and Drug Administration, and Director of the General Services Administration (as sector specific federal agencies), to develop and implement plans to defend the critical infrastructure for which they are responsible against biological threats.

### **RECOMMENDATION: The Administration should establish a critical infrastructure biodefense program at the Department of Homeland Security.**

Considering the importance of critical infrastructure to our country, the President should direct the Secretary of Homeland Security to formally establish a biological risk management program at CISA to: (1) identify biological risk management activities in which it previously engaged that would be helpful to reinstate permanently; (2) use the Agency's partnerships with the intelligence and law enforcement communities to obtain the actionable intelligence and information it needs to make decisions about protecting critical infrastructure from biological threats; (3) establish in-house subject matter expertise and analytical capability to support infrastructure biodefense requirements; (4) lead coordination of cross-sector biological risk management activities for national critical functions; (5) inform proactive risk management; and (6) inform emergency management.

The Secretary of Homeland Security should also require the Director of the Cybersecurity and Infrastructure Security Agency to: (1) report information to sector specific federal agencies about disease events that affect, or could affect, critical infrastructure assets in all 16 sectors, and private sector owners and operators; (2) determine what should be done if a naturally occurring disease outbreak, accidental pathogen release, or biological attack significantly affects critical infrastructure; (3) identify national critical functions most vulnerable to biological threats; and (4) work across all sectors to manage biological risk.

### **RECOMMENDATION: Sectors and the Department of Homeland Security Should Plan to Protect Critical Infrastructure Operators and Ensure Continued Critical Functions During Biological Events**

After COVID-19 spread to the United States, CISA produced guidance to help sectors identify essential critical infrastructure workers and direct limited resources for their protection during the pandemic.<sup>18</sup> Manpower reductions may be due to stay-at-home orders of the sort implemented during COVID-19, but all sectors must also consider the very real possibility that other diseases may also strike, sicken, and kill workers.

Sectors should, at a minimum, use their experiences with COVID-19, the 2009–2010 H1N1 influenza pandemic, and the anthrax events of 2001 to estimate needs for personal protective equipment (PPE), essential medical supplies, and cleaning materials. The sectors should utilize a scenario for an extremely virulent pandemic (e.g., smallpox). While each sector may not be able to obtain, stockpile, and provide everything their employees need to remain healthy and keep infrastructure running, sector leadership can determine requirements in advance and obtain what they need in order to provide and support their most essential critical infrastructure workers. The Director of the Cybersecurity and Infrastructure Security Agency should identify core supplies and medicines, estimate costs to procure and distribute them, and report this information annually to Congress and sector leaders.

Scenario-based planning is not new to the private sector. Shell Oil began scenario-based planning in the 1970s for the purpose of identifying in advance what they would need to maintain continuity of operations during a variety of situations.<sup>19</sup> The Director of the Cybersecurity and Infrastructure Security Agency should work with all Sector Coordinating Councils to develop and examine biological scenarios and determine what the sectors can do to prevent the use of their assets to perpetrate and exacerbate biological events. In addition, all companies that comprise each critical infrastructure sector should develop biological scenarios and plan accordingly. These plans should be as specific as possible. For example:



- Pharmaceutical companies in the Chemical Sector and Healthcare and Public Health Sector must develop a strategy that helps them maintain operations safely and securely before, during, and after a biological event, so that they continue to provide the antibiotics and other medicines desperately needed for medical treatment.
- Venues in the Commercial Facilities Sector must develop and implement emergency action plans for the mass gatherings they host.
- Companies in the Defense Industrial Base Sector must work with the Assistant Secretary of Defense for Homeland Defense and Global Security and help identify unclassified assets that should be addressed by the Defense Critical Infrastructure Protection program, assess vulnerabilities of these assets to biological threats, and determine how to eliminate those vulnerabilities.
- The Financial Services Sector must review financial industry business continuity plans to prepare for, respond to, and recover from biological events, pandemics, and potential resulting degradation of financial services.
- Governmental agencies in the Food and Agriculture Sector must work to include food and agrodefense requirements in the National Biodefense Strategy.
- The Secretary of Homeland Security, in coordination with the Secretary of Energy, Secretary of Agriculture, and Secretary of Health and Human Services must develop a pandemic preparedness plan for the Nuclear Reactors, Materials, and Waste Sector to ensure the Nation has the radioisotopes it needs for medical diagnostic tests and can use U.S. commercial and non-commercial nuclear facilities to sterilize medical equipment.

### **RECOMMENDATION: Sectors and sector specific federal agencies should maintain awareness of the disease environment in which critical infrastructure operates.**

Diseases like COVID-19 still take the United States by surprise. The Centers for Disease Control and Prevention (CDC) and other federal agencies undertake numerous biosurveillance activities, but their efforts rarely result in comprehensive ongoing analysis. Most information flows upward from localities to the federal government, which usually only presents national disease pictures during biological events (i.e., not proactively). The critical infrastructure community cannot expect that the federal government will know where disease is occurring at any given moment or that it will communicate information it does possess directly to the sectors. When biological events begin to affect infrastructure and national security, CISA may decide to monitor the spread of disease and communicate relevant information to the sectors. However, CISA

may have other priorities, especially if the agency assumes that other federal programs (e.g., those implemented by the DHS National Biosurveillance Integration Center) are responsible for doing so.

Critical infrastructure sectors that pay attention to the environments in which their facilities operate, and how diseases factor into those environments, can reduce the impact of biological events on their ability to operate, save money, and turn a profit. Therefore, the sectors should carry out their own disease awareness efforts. For example,

- CISA should work with CDC and state, local, tribal, and territorial (SLTT) public health agencies to determine how biological events affect mass gatherings and how people leaving these gatherings spread disease throughout the communities surrounding venues and throughout the country.
- Congress should require public health departments that are part of the Healthcare and Public Health Sector to provide detailed information about where disease is present and spreading to the Emergency Services Sector so that it can determine how these biological threats could impact their operations.
- The Secretary of Energy should expand the Department of Energy (DOE) Partnering Service and COVID-19 Technical Assistance Program to enable other members of the U.S. scientific community to access resources, researchers, experts, intellectual property, and facilities at the national laboratories (technically part of the Energy Sector) to address the biological threat.
- Congress should direct the Secretary of Agriculture, Secretary of Health and Human Services, and the Financial Services Sector to monitor biological events and alert Congress well before those events impact the Sector's services and the economy.
- Congress should fund those national laboratories and academic facilities that are part of the Nuclear Reactors, Materials, and Waste Sector and possess particle accelerators to pursue to the use of their high-powered equipment to examine proteins that comprise illness-causing organisms.
- Congress should direct the Secretary of Homeland Security to acquire, procure, distribute, and employ functional biodetectors in subways and other conveyances that are part of the Transportation Systems Sector, recognizing the continued biological threat to transportation systems.
- Congress should direct the Environmental Protection Agency (EPA) and CDC to help wastewater treatment facilities in the Water and Wastewater Sector to test wastewater and provide another source of data that can help determine where diseases exist and are spreading.

## **RECOMMENDATION: Sectors and sector specific federal agencies should identify and eliminate critical infrastructure vulnerabilities to biological threats.**

Every biological event reveals vulnerabilities in critical infrastructure and its ability to continue operating. COVID-19 most recently revealed vulnerabilities in the supply chain; ability to deliver medical care, support community health, and provide public safety; and ability of all sectors to operate with manpower restrictions. Sectors should identify and eliminate vulnerabilities to biological attacks, accidental releases of organisms from laboratories and other facilities that contain them, and naturally occurring diseases before the next biological event occur. While all critical infrastructure sectors are vulnerable to biological events, the nature of those vulnerabilities (and the actions needed to ameliorate them) are specific to each sector. For example,

- Congress should direct CISA to work with the Dams Sector to identify any problems with operating that may result in standing water because it attracts disease-carrying vectors like mosquitos. The standing water itself need not be infected with a biological agent, but attracted mosquitos could be, and in turn, they could carry disease away from the area.
- Congress should direct the Secretary of Health and Human Services to work with the Healthcare and Public Health Sector to identify all weaknesses and shortcomings revealed by COVID-19 and conduct a full-scale examination of the public health system.
- The Secretary of Homeland Security, in coordination with the FBI National Cyber Investigative Joint Task Force and the Department of Health and Human Services (HHS) Chief Information Officer to work with the Information Technology Sector to identify and assess vulnerabilities to healthcare and biomedical research infrastructure, especially since malevolent actors have exploited numerous healthcare data system vulnerabilities in the last year and cyberattacks are increasing.
- Congress should establish domestic production of medical isotopes and other radioactive sources for diagnostics and therapy, so that the United States will no longer depend so greatly on other countries to provide the medical isotopes it needs for medical diagnostics and imaging.
- The Secretary of Homeland Security should direct the Administrator of the Transportation Security Agency to work with the Commandant of the U.S. Coast Guard, Chief Executive Officer of Amtrak, Postmaster General of the U.S. Postal Services, Chief Executive Officers of commercial postal and shipping carriers, and other subsectors to prevent and control the spread of disease throughout the Transportation Systems Sector. All transportation conveyances (i.e., not just aviation) are vulnerable to the introduction and spread of disease.

## **RECOMMENDATION: Sectors and sector specific federal agencies should take action to reduce the impact of biological events before they occur again.**

When natural disasters like earthquakes occur, localities take action to prevent them from affecting communities as badly when they occur again. This preventive work is called mitigation. There is no reason for the critical infrastructure community to assume that COVID-19 will be a once-in-a-century event, especially considering the increasing frequency of biological events over the last 50 years. What is required to mitigate the impacts of biological events on critical infrastructure varies by sector. For example,

- Congress should direct the Chairman of the Federal Communications Commission (part of the Communications Sector) to work with fixed-wireless Internet service providers to ensure that rural, tribal, and territorial communities can access broadband permanently (enabling them to isolate as required during biological events).
- Congress should direct the Secretary of Energy to work with the Energy Sector to anticipate, articulate, and prepare for the same and greater energy demands that occurred during COVID-19 for all future pandemics and other biological events.
- Congress should direct the HHS Assistant Secretary for Preparedness and Response to provide Hospital Preparedness Program grants to the Healthcare and Public Health Sector to reinforce the stratified hospital system they piloted previously in some regions of the country and informally established by hospitals in response to COVID-19, to ensure that different levels of hospitals are able to treat and refer patients with novel diseases and illnesses caused by future biological threats.
- Congress should direct the Transportation Security Administration (TSA) (in coordination with the CDC and Federal Aviation Administration (FAA)) and the Department of Transportation (DOT), (in coordination with the CDC and TSA) to issue public health rules and regulations for transportation conveyances, so that they can reduce the impact on the Transportation Systems Sector when biological events occur again in the future that take advantage of the rapidity and vulnerabilities associated with national and global transit.



## RECOMMENDATION: Ensure execution of national critical functions by taking sector-specific actions

All critical infrastructure sectors and sector specific federal agencies must:

- Maintain awareness of biological threats;
- Understand how and where they are vulnerable to biological threats;
- Predict the consequences of a variety of biological events that would affect their sectors if they occurred;
- Prevent and deter biological events from occurring that affect their sectors;
- Prepare for biological events;
- Detect biological events when they occur at or near their facilities;
- Respond to biological events efficiently and effectively;
- Work with law enforcement and public health officials, as well as corporate security professionals, as they investigate the cause and nature of these events;
- Coordinate with public and private sector partners to help their facilities and the communities in which they reside recover from biological events; and
- Mitigate the impact of future biological events by emplacing protections and measures to help their facilities and personnel withstand attacks, accidents, and naturally occurring outbreaks.

**RECOMMENDATIONS SPECIFIC TO EACH CRITICAL INFRASTRUCTURE SECTOR FOLLOW IN APPENDIX A.**

## Conclusion

We depend on critical infrastructure and suffer when biological threats exploit sector vulnerabilities and create consequences for which we are unprepared. When biological events occur, they affect many (if not all) critical infrastructure sectors and put our national, economic, and public health security in jeopardy. DHS bears a great deal of responsibility in this arena and should continue to build on previous activities to manage and reduce biological risk to critical infrastructure. However, all other sector specific federal agencies, as well as the owners and operators of the individual sectors, must also devote resources to help defend critical infrastructure against biological threats.

Our Nation's critical infrastructure stands, but it does not stand firm, in the face of COVID-19. Targeted action by Congress, the Administration, and the private sector today will alleviate the strain caused by the next biological event, prevent cascading failures throughout critical infrastructure, and reduce the pain and suffering disease inflicts on the country.

# APPENDIX: RECOMMENDATIONS BY SECTOR

COVID-19 has created an opportunity to address shortcomings in the ability of critical infrastructure and society to withstand the effects of biological events. DHS CISA hurriedly developed and released guidance to assist critical infrastructure owners and operators in identifying their most essential workers who must be protected at all costs during a biological event like COVID-19.<sup>20</sup> However, for the most part, the sectors respond to the pandemic on their own having not prepared sufficiently beforehand.

The Bipartisan Commission on Biodefense developed this report to help each of the critical infrastructure sectors defend against biological threats. Sector-specific descriptions, discussions, and congressional jurisdictions follow below. Descriptions provide a broad overview of each sector, their subsectors, and their sector specific federal agencies. Discussions briefly address and provide recommendations to improve each sector's ability to address biological events. Finally, congressional jurisdictions address congressional oversight and appropriations for each sector.

# CHEMICAL SECTOR

## SECTOR DESCRIPTION

Chemical Sector facilities convert raw materials into products. The Sector is composed of the following distinct segments: (1) basic chemicals; (2) specialty chemicals; (3) agricultural chemicals; (4) pharmaceuticals; and (5) consumer products.<sup>21</sup> DHS is the designated sector specific federal agency responsible for risk management of the Chemical Sector.<sup>22</sup>

## DISCUSSION

The Chemical Sector faced significant challenges throughout the COVID-19 pandemic. Supply chain disruptions and decreased demand for many chemical products proved detrimental to numerous segments of the sector.<sup>23</sup> In particular, the pharmaceutical segment of the Chemical Sector (also of the Healthcare and Public Health Sector) suffered greatly from supply chain disruptions because over 70% of manufacturing sites for pharmaceutical precursor ingredients are overseas.<sup>24</sup> The pandemic caused widespread drug shortages and crippled the global medical supply chain.<sup>25</sup> The Food and Drug Administration (FDA) reported 114 drug shortages through March 2021.<sup>26</sup>

The pharmaceutical segment of the Chemical Sector plays a critical role in biodefense. It enables the production of medicines and medical countermeasures necessary for disease treatment. During a biological event, activities and facilities that enable pharmaceutical research, development, and production must be protected and, if possible, strengthened. In September 2020, CISA, the FBI Weapons of Mass Destruction Directorate, and the Defense Threat Reduction Agency collaborated to produce a guide for chemical companies and facilities to help them maintain operations safely and securely before, during, and after a pandemic.<sup>27</sup>

Unfortunately, this document does not contain any specifics for the pharmaceutical segment. While it is important for the sector to greatly emphasize the Chemical Facility Anti-Terrorism Standards program,<sup>28</sup> neither CISA nor the sector can do so to the exclusion of other activities, including biodefense.

**RECOMMENDATION:** The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, should work with the Chemical Sector Coordinating Council to develop and examine biological risk and threat scenarios and determine what the sector can do to prevent the use of its assets to perpetrate and exacerbate biological events.

**RECOMMENDATION:** The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, and in coordination with the Administrator of the Environmental Protection Agency, should work with the Chemical Sector Coordinating Council to provide a dedicated forum for all organizations that comprise the sector to develop requirements to protect the entire sector and their facilities against biological events, identify sector vulnerabilities in need of strengthening, continue operations during biological events, and prevent the loss of intellectual property. The Director of the Cybersecurity and Infrastructure Security Agency should report results (including identified strengths and weaknesses) from, and make recommendations to address problems revealed during, these fora.

**RECOMMENDATION:** Congress should amend the Homeland Security Act of 2002 (P.L. 107-296, 116 Stat. 2135, 6 U.S.C. 298) to direct the Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, and in coordination with the Commissioner of the Food and Drug Administration, the Assistant Director of the Federal Bureau of Investigation Weapons of Mass Destruction Directorate, and the Director of the Defense Threat Reduction Agency, to work with pharmaceutical companies to develop a strategy that helps them maintain operations safely and securely before, during, and after a biological event. This strategy should draw from the experiences of the COVID-19 pandemic and provide recommendations to prevent pharmaceutical supply chain failures in anticipation of future biological events.

CONGRESSIONAL JURISDICTION	
AUTHORIZATION COMMITTEES:	House Committee on Homeland Security
	Senate Committee on Homeland Security and Governmental Affairs
	House Committee on Energy and Commerce
	Senate Committee on Energy and Natural Resources
APPROPRIATIONS SUBCOMMITTEES:	Homeland Security

# COMMERCIAL FACILITIES SECTOR

## SECTOR DESCRIPTION

The Commercial Facilities Sector includes privately owned and operated business, entertainment, lodging, and shopping venues that host publicly accessible mass gatherings. The Commercial Facilities Sector is composed of the following subsectors: (1) entertainment and media; (2) gaming; (3) lodging; (4) outdoor events; (5) public assembly; (6) real estate; (7) retail; and (8) sports leagues.<sup>29</sup> DHS is the designated sector specific federal agency responsible for risk management of the Commercial Facilities Sector.<sup>30</sup>

## DISCUSSION

Many commercial facilities host mass gatherings. As such, they are at greater risk for biological attacks and could amplify the spread of disease. During COVID-19, public health restrictions affected these facilities first and they had to cancel events. The resulting economic impact clearly underscores the need for the sector to plan for biological events that affect their facilities.

The pandemic also illuminated the public service role the Commercial Facilities Sector can play during response to biological events.<sup>31</sup> Commercial facilities can provide surge capacity when outbreaks overwhelm Healthcare and Public Health Sector assets. For example, during the COVID-19 pandemic, states across the Nation converted field houses, stadiums (including National Football League stadiums), arenas, and parking lots into testing centers, field hospitals, and morgues.<sup>32</sup> Commercial facilities also must actively engage in biodetection and biosurveillance efforts since disease outbreaks could start there (a famous example is that of an outbreak of Legionella, which began at an American Legion convention with 4,000 in attendance over three days in 1976<sup>33</sup>) and the mass gatherings they host could become superspreader events.<sup>34</sup>

**RECOMMENDATION:** The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, should work with the Commercial Facilities Sector Coordinating Council to develop and examine biological risk and threat scenarios and determine what the sector can do to prevent the use of its assets to perpetrate and exacerbate biological events.

**RECOMMENDATION:** The Secretary of Homeland Security should direct the Director of the Cybersecurity and Infrastructure Security Agency to work with the CDC and SLTT public health agencies (local to each venue) to gather and analyze data to determine the effect of biological events on mass gatherings and the resulting relationship with increased spread of disease throughout surrounding communities.

**RECOMMENDATION:** Congress should amend the Homeland Security Act of 2002 (P.L. 107-296, 116 Stat. 2135, 6 U.S.C. 298) to direct the Secretary of Homeland Security to take the unique needs of National Special Security Events, other special events of national significance,<sup>35</sup> and large-scale events hosted at commercial venues into consideration, and develop biodetection technology (other than Department of Homeland Security BioWatch detectors) appropriate for use at venues and surrounding locations where these events occur.

**RECOMMENDATION:** The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, should work with the Commercial Facilities Sector Coordinating Council to: (1) provide a dedicated forum for facilities to develop and issue guidance for venues at which special events and mass gatherings are held, to prevent, prepare for, detect, respond to, recover from, and mitigate biological events; and (2) provide technical assistance to commercial venues to help them develop emergency actions plans for the mass gatherings they host.

CONGRESSIONAL JURISDICTION	
AUTHORIZATION COMMITTEES:	House Committee on Homeland Security Senate Committee on Homeland Security and Governmental Affairs
APPROPRIATIONS SUBCOMMITTEES:	Homeland Security

# COMMUNICATIONS SECTOR

## SECTOR DESCRIPTION

The Communications Sector enables all other sectors to function and uses interrelated terrestrial, satellite, and wireless transmission systems to access voice, video, and data services. The sector is composed of the following segments: (1) broadcasting; (2) cable; (3) satellite; (4) wireless; and (5) wireline.<sup>36</sup> DHS is the designated sector specific federal agency responsible for risk management of the Communications Sector.<sup>37</sup>

## DISCUSSION

Demands upon the Sector greatly increased during the COVID-19 pandemic, and the communications industry expanded to alleviate the strain placed on terrestrial, satellite, and wireless transmission systems.<sup>38</sup> Demand remains high as the COVID-19 pandemic continues to affect the world, and extra capacity will be necessary if pandemic influenza and other biological events occur. The sector should anticipate and prepare for the same and even greater demands during future biological events.

When the Nation transitioned to working from home during the COVID-19 pandemic, we immediately increased demand, reliance, and pressure on, wireless broadband services. The Federal Communications Commission (FCC) temporarily increased rural access to high-speed internet access (known as broadband) to support telework, telemedicine, and distance learning.<sup>39</sup> Without robust wireless broadband services, some areas cannot easily use teleconferencing platforms to communicate during biological events that prevent in-person meetings. For example, the Navajo Nation lacked sufficient communications infrastructure to use these platforms during the COVID-19 pandemic.<sup>40</sup>

**RECOMMENDATION:** The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, should work with the Communications Sector Coordinating Council to develop and examine biological risk and threat scenarios and determine what the sector can do to prevent the use of its assets to perpetrate and exacerbate biological events.

**RECOMMENDATION:** Congress should direct the Chairman of the Federal Communications Commission to work with fixed-wireless internet service providers to ensure that rural communities, tribes, and territories can access broadband permanently.

**RECOMMENDATION:** Congress should build on the FCC COVID-19 Telehealth Program<sup>41</sup> and amend the Communications Act of 1934 (47 U.S.C. 151 et seq.) to authorize a broader FCC Telehealth Program using modern telecommunications technology. Congress should authorize cross-state licensure for practitioners providing telemedicine and provide financial assistance to healthcare deliverers to pay for the remote delivery of healthcare, and to public health professionals to pay for the remote reporting and sharing of biosurveillance data and information.

CONGRESSIONAL JURISDICTION	
AUTHORIZATION COMMITTEES:	House Committee on Homeland Security
	Senate Committee on Homeland Security and Governmental Affairs
	House Committee on Energy and Commerce
	Senate Committee on Commerce, Science and Transportation
APPROPRIATIONS SUBCOMMITTEES:	Homeland Security

# CRITICAL MANUFACTURING SECTOR

## SECTOR DESCRIPTION

The Critical Manufacturing Sector is composed of the following manufacturing industries: (1) primary metals; (2) machinery; (3) electrical equipment, appliances, and components; and (4) transportation equipment.<sup>42</sup> DHS is the designated sector specific federal agency responsible for risk management of the Critical Manufacturing Sector.<sup>43</sup>

## DISCUSSION

President Trump invoked the Defense Production Act (DPA) of 1950 (P.L. 81–774, 50 U.S.C. §4501 et seq.) to order vehicle manufacturers and other manufacturing entities to use their facilities to produce needed ventilators, PPE, and tests. However, the Trump Administration only sporadically and narrowly utilized the DPA.<sup>44</sup> Most of the funding to use the DPA went to national defense (not pandemic response). The Trump Administration also attempted to use the DPA to compel companies to expedite PPE manufacturing.<sup>45</sup> President Biden also invoked the DPA to address the pandemic shortly after entering office to boost production of vaccines, point-of-care tests, and PPE.<sup>46,47</sup> The Biden Administration used it to expand vaccine production through a manufacturing collaboration between competitors Merck and Johnson & Johnson.<sup>48</sup>

Some of the differences between the Biden and Trump Administrations approaches reflected differing needs during each stage of the pandemic.<sup>49</sup> For instance, the Trump Administration’s use largely focused on ventilators that were urgently needed when COVID-19 began spreading throughout the United States, while the Biden Administration shifted focus to vaccine production after the FDA issued emergency use authorizations for several vaccines in late 2020 and early 2021.

**RECOMMENDATION:** The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, should work with the Critical Manufacturing Sector Coordinating Council to develop and examine biological risk and threat scenarios and determine what the sector can do to prevent the use of its assets to perpetrate and exacerbate biological events.

**RECOMMENDATION:** Having observed how hard it was to shift manufacturing from cars to ventilators, Congress should amend the Homeland Security Act of 2002 (P.L. 107-296, 116 Stat. 2135, 6 U.S.C. 298) to direct the Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, to work with the Critical Manufacturing Sector Coordinating Council to provide a forum to plan for similar requirements during pandemics and other large-scale biological events. While this Council cannot predict every type of equipment that might be needed, they can at least identify common factors for consideration (e.g., intellectual property rights, additional training, regulatory approvals, unique safety requirements, software). The plan should also address the need to learn from, and establish partnerships with, medical and biotechnological manufacturing companies in advance of biological events.

CONGRESSIONAL JURISDICTION	
AUTHORIZATION COMMITTEES:	House Committee on Homeland Security Senate Committee on Homeland Security and Governmental Affairs
APPROPRIATIONS SUBCOMMITTEES:	Homeland Security

# DAMS SECTOR

## SECTOR DESCRIPTION

The Dams Sector is responsible for water retention and control to provide for: (1) hydroelectric power generation; (2) municipal and industrial water supplies; (3) agricultural irrigation, sediment, and flood control; (4) river navigation for inland bulk shipping; (5) industrial waste management; and (6) recreation.<sup>50</sup> DHS is the designated sector specific federal agency responsible for risk management of the Dams Sector.<sup>51</sup>

## DISCUSSION

While the usual operation of the Dams Sector does not carry with it many implications for biodefense, the malfunctioning of the Sector does. Improperly managed dams could affect the environment in ways that make it easier for diseases to spread. Dams that do not release water consistently could create standing water covering large geographic areas. Standing water attracts mosquitoes, which in turn could be disease vectors. These conditions could also increase the amount of pathogens in the water.

Dam failure could impact public health.<sup>52</sup> The loss or loss of control of the water supply and power would prove particularly detrimental during a biological event anywhere dams provide either. The sector greatly affects public health and manipulation or destruction of sector assets could be part of a biological attack, especially on the food supply.

**RECOMMENDATION:** The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, should work with the Dams Sector Coordinating Council to develop and examine biological risk and threat scenarios and determine what the sector can do to prevent the use of its assets to perpetrate and exacerbate biological events.

**RECOMMENDATION:** Congress should amend the Homeland Security Act of 2002 (P.L. 107-296, 116 Stat. 2135, 6 U.S.C. 298) to direct the Director of the Cybersecurity and Infrastructure Security Agency—in coordination with the Department of Health and Human Services Assistant Secretary for Preparedness and Response, Department of Agriculture (USDA) Assistant Secretary for Administration, and Food and Drug Administration Director of the Center for Food Safety and Applied Nutrition—to articulate how the Dams Sector contributes to public health and biodefense (especially with respect to food safety) and take steps to strengthen those contributions and better secure the sector.

CONGRESSIONAL JURISDICTION	
AUTHORIZATION COMMITTEES:	House Committee on Homeland Security
	Senate Committee on Homeland Security and Governmental Affairs
	House Committee on Transportation and Infrastructure
	Senate Committee on Environment and Public Works
	House Committee on Natural Resources
	Senate Committee on Energy and Natural Resources
	Senate Committee on Indian Affairs
	House Committee on Agriculture
	Senate Committee on Agriculture
APPROPRIATIONS SUBCOMMITTEES:	Homeland Security
	Interior, Environment, and Related Agencies
	Energy and Water Development, and Related Agencies
	Agriculture, Rural Development, Food and Drug Administration, and Related Agencies

# DEFENSE INDUSTRIAL BASE SECTOR

## SECTOR DESCRIPTION

The Defense Industrial Base Sector meets U.S. military requirements for military weapons systems, subsystems, and components or parts needed to mobilize, deploy, and sustain military operations through: (1) research and development; and (2) design, production, delivery, and maintenance.<sup>53</sup> The Department of Defense (DOD) is the designated sector specific federal agency responsible for risk management of the Defense Industrial Base Sector.<sup>54</sup>

## DISCUSSION

COVID-19 delayed the development and delivery of some military supplies and programs.<sup>55,56</sup> The Defense Industrial Base has overcome supply chain disruptions and challenges associated with social distancing. However, should the pandemic become more severe, additional diseases compound COVID-19, or another biological event occur before COVID-19 declines, unavoidable delays and precautions would affect the warfighter and our national defense.

DOD does not identify critical infrastructure assets (including networks, assets, and associated dependencies) that it considers critical for the Department’s operations or defense of the Nation in the same way that civilian sector specific agencies do<sup>57</sup> or to the same extent. The Defense Critical Infrastructure Program also does not receive as much attention as its civilian counterpart (DHS CISA). The Program depends on the Defense Industrial Base, the critical infrastructure assets the Defense Industrial Base owns and operates, and the interdependencies between defense industrial and civilian critical infrastructure.

**RECOMMENDATION:** The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, should work with the Defense Industrial Base Sector Coordinating Council to develop and examine biological scenarios and determine what the sector can do to prevent the use of its assets to perpetrate and exacerbate biological events.

**RECOMMENDATION:** Through the annually reauthorized National Defense Authorization Act, Congress should direct the Under Secretary of Defense for Policy to collaborate with the Joint Staff, combatant commands, military services, other defense agencies, and the Defense Industrial Base Sector Coordinating Council to compile a list, and provide that list to Congress annually, of all DOD- and non-DOD-owned unclassified, classified, and Special Access Program<sup>58</sup> critical infrastructure (including networks, assets, and associated dependencies) necessary for DOD to fulfill its responsibilities to fulfill the National Biodefense Strategy,<sup>59</sup> National Defense Strategy,<sup>60</sup> and National Security Strategy<sup>61</sup> with regard to defending the United States and its interests overseas from biological threats.

**RECOMMENDATION:** Through the annually reauthorized National Defense Authorization Act, Congress should direct the Assistant Secretary of Defense for Homeland Defense and Global Security to work with the Defense Industrial Base Sector Coordinating Council to: (1) produce a list of unclassified assets addressed by the Defense Critical Infrastructure Protection program; (2) assess vulnerabilities of these assets to biological threats; (3) determine how to eliminate those vulnerabilities; and (4) provide this information to Congress annually.

CONGRESSIONAL JURISDICTION	
AUTHORIZATION COMMITTEES:	House Committee on Armed Services
	Senate Committee on Armed Services
APPROPRIATIONS SUBCOMMITTEES:	Defense; Military Construction, Veterans Affairs, and Related Agencies



# EMERGENCY SERVICES SECTOR

## SECTOR DESCRIPTION

The Emergency Services Sector provides assistance during emergencies and disasters to save lives, property, and the environment. It is composed of the following disciplines: (1) law enforcement; (2) fire and rescue services; (3) emergency medical services; (4) emergency management; and (5) public works.<sup>62</sup> DHS is the designated Sector-Specific Agency responsible for risk management of the Emergency Services Sector.<sup>63</sup>

## DISCUSSION

While the first responders that operate in this sector are the first line of defense (including biodefense), they are also often the first to provide medical treatment and support the health of groups and communities impacted by emergencies. Few first responders obtain epidemiological information directly from their SLTT departments of health. Preexisting connections between departments are minimal. For its part, the Healthcare and Public Health Sector does not seem to take the Emergency Services Sector into consideration beyond certifications for emergency medical services (EMS) volunteers and professionals.

Historically, fusion centers made working with law enforcement a top priority. While they are trying to work with more sectors, many of the Nation’s fusion centers still do not work with EMS and other elements of the sector as much as they do with law enforcement.<sup>64</sup> The COVID-19 pandemic necessitates increased cooperation and data sharing among fusion centers, public health, and all emergency services. Relationships established by fusion centers during the pandemic will be needed again when the next biological event occurs.

**RECOMMENDATION:** The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, should work with the Emergency Services Sector Coordinating Council to develop and examine biological risk and threat scenarios and determine what the sector can do to prevent the use of its assets to perpetrate and exacerbate biological events.

**RECOMMENDATION:** Congress should amend the Homeland Security Act of 2002 (P.L. 107-296, 116 Stat. 2135, 6 U.S.C. 298) to require SLTT public health departments to provide, and relevant Inspectors General to audit the provision of, periodic, detailed information to law enforcement, fire, emergency medical services, hazardous materials teams, emergency managers, emergency dispatchers, and public works personnel regarding biological threats with the potential to impact response operations. The Federal Emergency Management Agency (FEMA) should make providing this information a requirement for participation in the DHS State Homeland Security Grant Program and the Urban Area Security Initiative, to help sector personnel understand the spread and technical aspects of disease in their areas of operation. The frequency and specificity of the information shared with emergency services personnel should scale in accordance with the severity of the biological threat. FEMA should also require grant applicants for Staffing for Adequate Fire and Emergency Response grants to prioritize the hiring of firefighters with public health experience.

**RECOMMENDATION:** Congress should amend the Homeland Security Act of 2002 (P.L. 107-296, 116 Stat. 2135, 6 U.S.C. 298) to direct the Secretary of Homeland Security, acting through the Under Secretary of the Office of Intelligence and Analysis, to provide technical assistance to the Nation’s fusion centers to work with state and local departments of health and agriculture to help the fusion centers determine: (1) where disease is present; (2) impact of disease on human and animal workforces; (3) the extent to which personal protective equipment and other measures would be helpful; and (4) how to modify their operations during biological events.

CONGRESSIONAL JURISDICTION	
AUTHORIZATION COMMITTEES:	House Committee on Homeland Security Senate Committee on Homeland Security and Governmental Affairs House Committee on the Judiciary Senate Committee on the Judiciary House Committee on Energy and Commerce Senate Committee on Health, Education, Labor, and Pensions House Committee on Transportation and Infrastructure Senate Committee on Commerce, Science and Transportation
APPROPRIATIONS SUBCOMMITTEES:	Homeland Security Commerce, Justice, Science, and Related Agencies Labor, Health and Human Services, Education, and Related Agencies Transportation, and Housing and Urban Development, and Related Agencies

# ENERGY SECTOR

## SECTOR DESCRIPTION

The Energy Sector enables all other critical infrastructure sectors to function and is composed of three interrelated segments: (1) electricity; (2) oil; and (3) natural gas.<sup>65</sup> The DOE is the designated sector specific federal agency responsible for risk management of the Energy Sector.<sup>66</sup>

## DISCUSSION

Fluctuating energy demands throughout the COVID-19 pandemic challenged the sector. Demands for renewable energy sources, residential consumption, and the manufacturing of medical products and PPE greatly increased. Confinement measures to contain the spread of the disease, establishment of new supply chains to obtain materials during the emergency, and waste disposal all created additional demands for energy. Energy demands decreased for fossil fuels, commercial and industrial entities, and production of regular goods (e.g., clothes). As lockdown measures lift, demands increase.<sup>67</sup>

During the pandemic, DOE established a COVID-19 Innovation Portal and Assistance Program through its Lab Partnering Service and COVID-19 Technical Assistance Program.<sup>68</sup> These initiatives enabled American innovators to readily access resources and partner with experts at the National Laboratories to combat the virus.

**RECOMMENDATION:** The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, should work with the Energy Sector Coordinating Council to develop and examine biological risk and threat scenarios and determine what the sector can do to prevent the use of its assets to perpetrate and exacerbate biological events.

**RECOMMENDATION:** Congress should amend the Department of Energy Organization Act of 1977 (P.L. 95–91, 91 Stat. 565, as amended) to direct the Secretary of Energy to anticipate, articulate, and prepare for the same and greater energy demands experienced to-date during the COVID-19 pandemic for future pandemics and biological events. Current demand will remain high as COVID-19 continues to affect the world. The Nation will also need extra energy capacity when pandemic influenza and other biological events occur in the future.

**RECOMMENDATION:** The Secretary of Energy should expand the DOE Lab Partnering Service and COVID-19 Technical Assistance Program to enable the broader (non-DOE) U.S. scientific community to access resources, researchers, experts, intellectual property, and facilities at the National Laboratories as it works to address the biological threat.

CONGRESSIONAL JURISDICTION	
AUTHORIZATION COMMITTEES:	House Energy and Commerce
	Senate Committee on Energy and Natural Resources
APPROPRIATIONS SUBCOMMITTEES:	Energy and Water Development, and Related Agencies

# FINANCIAL SERVICES SECTOR

## SECTOR DESCRIPTION

The Financial Services Sector provides the following products and services: (1) deposit, consumer credit, and payment systems products; (2) credit and liquidity products; (3) investment products; and (4) risk transfer products.<sup>69</sup> The Department of Treasury is the designated sector specific federal agency responsible for risk management of the Financial Services Sector.<sup>70</sup>

## DISCUSSION

Pandemics and other large-scale biological events affect the economy. For example, the COVID-19 pandemic created a recession in the United States.<sup>71</sup> COVID-19 also triggered one of the worst stock market crashes in U.S. history, with stock markets having to halt trading several times as markets plummeted.<sup>72</sup> The Financial Services Sector has responded by taking several actions to reduce the economic consequences of this biological event. For example, the Federal Reserve System<sup>73</sup> created temporary U.S. dollar liquidity swap lines<sup>74</sup> with nine central banks<sup>75</sup> and kept interest rates close to zero.<sup>76</sup>

The impacts of biological events vary widely in severity across the sector and require swift action to blunt their consequences. Congress passed, and President Trump signed, the Coronavirus Aid, Relief, and Economic Security Act (P.L. 116-136) to stimulate the economy. The bill provided fiscal support to the Nation’s employers, consumers, investors, and governmental organizations. Fiscal stimuli like this are vital to keeping the economy afloat during a protracted crisis like a pandemic.

**RECOMMENDATION:** The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, should work with the Financial Services Sector Coordinating Council to develop and examine biological risk and threat scenarios and determine what the sector can do to prevent the use of its assets to perpetrate and exacerbate biological events.

**RECOMMENDATION:** The sector must assume that large-scale biological events are likely to occur far more frequently than in times past (perhaps annually) and plan to respond accordingly. Congress must also assume the same. The House and Senate Financial Services Committees should direct the Secretary of Agriculture and the Secretary of Health and Human Services to monitor biological events, outbreaks, epidemics, and pandemics that affect or could affect the United States and alert these Committees regarding disease events so that they can determine what actions Congress must take to preserve the economy.

**RECOMMENDATION:** The Secretary of Treasury, in coordination with the Financial Services Coordinating Council for Critical Infrastructure Protection and Homeland Security, and Financial and Banking Information Infrastructure Committee should: (1) identify significant impacts to the Financial Services Sector during and after biological events and pandemics; (2) review financial industry plans to prepare for, respond to, and recover from biological events and pandemics; (3) develop and execute exercises<sup>77</sup> that address biological events and pandemics; and (4) require organizations that comprise the sector to address biological events, pandemics, and potential degradation of financial services in business continuity plans.

CONGRESSIONAL JURISDICTION	
AUTHORIZATION COMMITTEES:	House Committee on Financial Services
	Senate Committee on Banking, Housing, and Urban Affairs
	Senate Committee on Finance
APPROPRIATIONS SUBCOMMITTEES:	Financial Services and General Government

# FOOD AND AGRICULTURE SECTOR

## SECTOR DESCRIPTION

The Food and Agriculture Sector produces, processes, and delivers food to humans and animals and is categorized as follows: (1) supply; (2) processing, packaging, and production; (3) agriculture and food product storage; (4) agricultural and food product transportation; (5) agricultural and food processing product distribution; (6) agricultural and food supporting facilities; (7) regulatory, oversight, and industry organizations; and (8) other agriculture and food.<sup>78</sup> HHS and USDA are the designated sector specific federal agencies responsible for risk management of the Food and Agriculture Sector.<sup>79</sup>

## DISCUSSION

Diseases threaten plants, animals, and humans. Bad actors have planned biological attacks against all three. As the Nation deals with the impact of COVID-19 on the human population, it must also assume that the same or worse could occur with plants and animals. The negative impact of attacks on food and agriculture would affect the national and global economies immediately and demonstrably. Wildlife can also serve as sources or become new reservoirs of disease, complicating response, recovery, and mitigation from biological events affecting the sector.

When it comes to diseases affecting animal agriculture, the sector often resorts to isolating infected populations and killing diseased domestic animals through mass culling. This is ineffective for diseases established in wild populations. Plant diseases can move even faster and destroy entire crops.

The Secretary of Agriculture and the Administrator of the Food and Drug Administration have not made biodefense enough of a priority. For example, the USDA biodefense program is so small that it is often overlooked when other federal government departments and agencies engage in biodefense activities. The size of this program seems inversely proportional to the \$1 trillion this sector contributes annually to the U.S. economy.<sup>80</sup>

**RECOMMENDATION:** The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, should work with the Food and Agriculture Sector Coordinating Council to develop and examine biological risk and threat scenarios and determine what the sector can do to prevent the use of its assets to perpetrate and exacerbate biological events.

**RECOMMENDATION:** In the annually reauthorized National Defense Authorization Act, Congress should direct the Secretary of Defense, Secretary of Agriculture, Secretary of Health and Human Services, and Secretary of Homeland Security to incorporate defense against biological threats to food and agriculture into the National Biodefense Strategy<sup>81</sup> and strengthen coordination with federal and state wildlife authorities. The President should then rescind Homeland Security Presidential Directive 9.<sup>82</sup>

**RECOMMENDATION:** In the next Agriculture Improvement Act (also known as the Farm Bill), Congress should direct the Secretary of Agriculture to establish a robust biodefense program in the Office of the Secretary. Congress should also amend the FDA Reauthorization Act of 2017 (P.L. 115-52) to establish a robust biodefense program in the Office of the Commissioner. Congress should make these programs responsible for defense against biological events affecting plants and animals, defense against biological attacks on food and agriculture, and protection of food and agriculture related supply chains.

CONGRESSIONAL JURISDICTION	
AUTHORIZATION COMMITTEES:	House Committee on Agriculture
	House Committee on Homeland Security
	Senate Committee on Homeland Security and Governmental Affairs
	Senate Committee on Agriculture, Nutrition, and Forestry
	House Committee on Energy and Commerce
	Senate Committee on Health, Education, Labor, and Pensions
APPROPRIATIONS SUBCOMMITTEES:	Agriculture, Rural Development, Food and Drug Administration, and Related Agencies
	Labor, Health, and Human Services, Education, and Related Agencies; Homeland Security

# GOVERNMENT FACILITIES SECTOR

## SECTOR DESCRIPTION

The Government Facilities Sector includes federal and SLTT government buildings and is composed of three subsectors: (1) education facilities; (2) national monuments and icons; and (3) election infrastructure.<sup>83</sup> DHS and the General Services Administration (GSA) are the designated sector specific federal agencies responsible for risk management of the Government Facilities Sector.<sup>84</sup>

## DISCUSSION

Unlike other critical infrastructure sectors, the Government Facilities Sector has been dealing with biological threats since 2001. Envelopes and packages containing (or suspected to contain) suspicious powders continue to be sent to government facilities. Regardless, over the past decade, questions have arisen as to whether N95 masks should be stockpiled and made available to employees, and whether preparedness and training for response to biological attacks should continue. Some government facilities are also the sites of mass gatherings that amplify the spread of a disease. Additionally, educational institutions receive too little funding, and response plans often only involve sending children home and using gymnasiums for disaster evacuation.

**RECOMMENDATION:** The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, should work with the Government Facilities Sector Coordinating Council to develop and examine biological risk and threat scenarios and determine what the sector can do to prevent the use of its assets to perpetrate and exacerbate biological events.

**RECOMMENDATION:** Congress should amend Federal Property and Administrative Services Act of 1949 (P.L. 152, Ch. 288, 63 Stat. 377/ 40 and 41 U.S.C.) to codify GSA biodefense activities and direct the Administrator of the Government Services Administration to: (1) create buying guides for products and services that agencies need to respond to biological events; (2) develop Market Research as a biodefense service resource; (3) enable buyers to procure non-Trade Agreement Act compliant essential products for biodefense; (4) provide SLTT agencies access to GSA Multiple Award Schedules Purchasing Programs that would apply to biodefense; (5) develop, compile, and provide biodefense acquisition information and resources on acquisition platforms; and (6) develop, modify, and incorporate biodefense standards in GSA custodial contracts in federally-owned buildings.<sup>85</sup>

**RECOMMENDATION:** The Secretary of Homeland Security, acting through the Director of the Federal Protective Service, should establish a biodefense program for the Federal Protective Service (FPS). For occupants of all federal facilities under FPS jurisdiction, the Program should: (1) increase awareness of naturally occurring, accidentally released, and intentionally introduced biological events; (2) provide biodefense training; (3) support planning for sheltering in place, occupant emergency response, and evacuation; and (4) conduct biological risk assessments of federal buildings under their authority and convey the results to Congress annually.

**RECOMMENDATION:** Congress should amend the Homeland Security Act of 2002 (P.L. 107-296, 116 Stat. 2135, 6 U.S.C. 298) to direct the Director of the Federal Protective Service to: (1) develop, train, test, and evaluate procedures to respond to the use or suspected use of biological agents in, and attacks on, federal buildings; (2) train all FPS law enforcement personnel to respond to the use or suspected use of biological agents in, and attacks on, federal buildings; (3) certify some FPS personnel as Hazardous Materials Technicians that can deal with biological agents and materials; (4) direct local FPS chemical, biological, radiological, nuclear, and explosive coordinators to develop relationships with responders and planners that would respond to biological crises; and (5) support local biological emergency preparedness, response, recovery, and mitigation efforts.<sup>86</sup>

**RECOMMENDATION:** Congress should amend the Department of Education Organization Act of 1979 (P.L. 96-88) to direct the Secretary of Education, in coordination with the Secretary of Health and Human Services, to develop and implement guidelines for closing and opening schools during biological events and provide resources on how to manage educational requirements when prolonged absences due to quarantines prevent children from physically going to school.

CONGRESSIONAL JURISDICTION	
AUTHORIZATION COMMITTEES:	House Committee on Homeland Security
	Senate Committee on Homeland Security and Governmental Affairs
	House Committee on Transportation and Infrastructure
	House Committee on Education and Labor
	Senate Committee on Health, Education, Labor, and Pensions
APPROPRIATIONS SUBCOMMITTEES:	Homeland Security
	Financial Services and General Government
	Labor, Health and Human Services, Education, and Related Agencies

# HEALTHCARE AND PUBLIC HEALTH SECTOR

## SECTOR DESCRIPTION

The Healthcare and Public Health Sector is composed of six nongovernmental subsectors and two governmental subsectors. The six private subsectors are: (1) direct patient care; (2) health information technology; (3) health plans and payers; (4) mass fatality management services; (5) medical materials; and (6) laboratories, blood, and pharmaceuticals.<sup>87</sup> The two governmental subsectors are: (1) public health; and (2) federal response and program offices.<sup>88</sup> HHS is the designated Sector-Specific Agency responsible for risk management of the Healthcare and Public Health Sector.<sup>89</sup>

## DISCUSSION

All these subsectors have been involved significantly with COVID-19 response and all were unprepared for the demands that this and previous pandemics placed upon them. This sector needs more than just funding to ensure preparedness. Regarding hospitals, the Commission previously recommended the establishment of a national stratified hospital system for biodefense.<sup>90</sup> The HHS Assistant Secretary for Preparedness and Response piloted a regional hospital system addressing this recommendation before COVID-19 began,<sup>91</sup> but has yet to take further action. However, in response to COVID-19, hospitals throughout the country also informally created a national stratified hospital system to treat patients infected by Severe Acute Respiratory Syndrome coronavirus 2 (SARS-CoV-2). The Centers for Medicare and Medicaid Services (CMS) further strengthened the system when it approved reimbursement for COVID-19 treatment.<sup>92, 93</sup>

COVID-19, tuberculosis, and a host of other diseases reveal how weak the U.S. public health system has become. When COVID-19 began to overwhelm hospitals and PPE supplies ran short, the Strategic National Stockpile failed to provide enough needed equipment. In addition, DOD often had to come to the aid of HHS to help with the logistics of their response. While not ideal, the current state of the U.S. healthcare and public health systems will likely require DOD support in responding to future biological events. DOD has considerable resources and expertise that this sector and HHS simply do not.

**RECOMMENDATION:** The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, should work with the Healthcare and

Public Health Sector Coordinating Council to develop and examine biological risk and threat scenarios and determine what the sector can do to prevent the use of its assets to perpetrate and exacerbate biological events.

**RECOMMENDATION:** The Administrator of the Centers for Medicare and Medicaid Services should establish requirements for CMS to designate and approve reimbursement for novel diseases within four weeks of the declaration of a public health emergency by the Secretary of Health and Human Services or a national emergency by the President of the United States.

**RECOMMENDATION:** Congress should amend the Pandemic and All-Hazards Preparedness Act of 2006 (P.L. 109-417) to direct the Department of Health and Human Services Assistant Secretary for Preparedness and Response to provide Hospital Preparedness Program<sup>94</sup> grants to reinforce this stratified hospital system, ensuring that the high-level hospitals are able to treat patients with novel diseases and illnesses caused by biological threats.

**RECOMMENDATION:** Congress should amend Section 319 of the Public Health Service Act of 1944 to (42 U.S.C. 201 et seq.) to direct the Secretary of Health and Human Services to undertake a full-scale examination of the public health system. In carrying out this mandate, the Secretary of Health and Human Services should seek input from SLTT public health professionals, accredited schools of public health, public health associations, U.S. Public Health Service professionals, DOD, Department of Interior, HHS, and USDA public health agencies.

**RECOMMENDATION:** In the annually reauthorized National Defense Authorization Act, Congress should direct the Secretary of Defense to update public health emergency protocols and health protection conditions, develop scenarios involving naturally occurring diseases and biological attacks, and reexamine DOD health protection condition levels, taking historical biological events and these scenarios into consideration.

CONGRESSIONAL JURISDICTION	
AUTHORIZATION COMMITTEES:	House Committee on Homeland Security
	Senate Committee on Homeland Security and Governmental Affairs
	House Committee on Transportation and Infrastructure
	Senate Committee on Commerce, Science, and Transportation
	House Committee on Energy and Commerce
	Senate Committee on Health, Education, Labor, and Pensions
APPROPRIATIONS SUBCOMMITTEES:	Labor, Health and Human Services, Education, and Related Agencies



# INFORMATION TECHNOLOGY SECTOR

## SECTOR DESCRIPTION

The Information Technology (IT) Sector enables all other sectors to function and provides the following: (1) IT products and services; (2) incident management capabilities; (3) domain name resolution services; (4) identity management and associated trust support services; (5) internet-based content, information, and communication services; and (6) internet routing, access, and connection services.<sup>95</sup> (Note that health information technology is also a private subsector of the Healthcare and Public Health Sector.<sup>96</sup>) DHS is the designated sector specific federal agency responsible for risk management of the Information Technology Sector.<sup>97</sup>

## DISCUSSION

Disruption of the IT Sector would negatively affect other sectors engaged in response to a biological event since all sectors are dependent on the IT sector. Biological attacks and cyberattacks could occur at the same time, each exacerbating the impact of the other.

Unfortunately, the healthcare and public health communities have not taken, or been able to take, full advantage of available IT storage, retrieval, and transmission equipment and systems. Partly this is due to lack of funding. Additionally, strong biodefense depends on real time situational awareness, only made possible with standards, ontological dictionaries, interoperability, and the ability to integrate distributed devices and large servers, many of which are currently lacking.

Reliance on IT during COVID-19 led to a major increase in cyberattacks on IT infrastructure throughout the pandemic.<sup>98,99</sup> Even before the disease spread to the United States, the high value of their data and low value placed on securing those data made the healthcare systems vulnerable to cyberattacks.<sup>100</sup>

The race to develop a vaccine for COVID-19 made the industry even more attractive to hackers (including state actors)<sup>101</sup> and many vaccine manufacturers faced high volumes of cyberattacks.<sup>102, 103</sup> Numerous cybersecurity threats related to the COVID-19 vaccine occurred, ranging from stealing data to sabotaging supply chains.<sup>104</sup>

The Office of the National Coordinator for Health IT (ONC),<sup>105</sup> within HHS, coordinates nationwide efforts to implement and use advanced health IT and data sharing. However, the Office focuses on health more broadly and needs to focus more on public health to leverage IT fully when addressing biological threats. More attention to the adoption of IT for public health and to the exchange of information would improve readiness for the next biological event.

**RECOMMENDATION:** The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, should work with the IT Sector Coordinating Council to develop and examine biological risk and threat scenarios and determine what the sector should do to prevent the use of its assets to perpetrate and exacerbate biological events.

**RECOMMENDATION:** The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, and in coordination with the Director of the FBI National Cyber Investigative Joint Task Force and the HHS Chief Information Officer, should assess cyberthreats to healthcare and biomedical research facilities before, during, and after a biological event. The assessment should: (1) examine cyberattacks targeting these facilities during the COVID-19 pandemic; (2) identify major cyber vulnerabilities of these facilities; and (3) provide recommendations and guidance to eliminate vulnerabilities and strengthen cybersecurity of these facilities.

**RECOMMENDATION:** Congress should amend the Health IT for Economic and Clinical Health Act of 2009 (part of the American Recovery and Reinvestment Act of 2009, P.L. 111-5) to direct the Secretary of Health and Human Services to establish within the ONC a Chief Public Health Officer responsible for ensuring that ONC serves as a resource for the national public health system to: (1) support the adoption of IT to improve public health; and (2) promote a nationwide public health information exchange to improve public health. The ONC Chief Public Health Officer should advance population-based health; transform public health; foster research, science, and innovation; and enhance the Nation’s public health IT infrastructure.

CONGRESSIONAL JURISDICTION	
AUTHORIZATION COMMITTEES:	House Committee on Homeland Security Senate Committee on Homeland Security and Governmental Affairs House Committee on Energy and Commerce Senate Committee on Health, Education, Labor, and Pensions
APPROPRIATIONS SUBCOMMITTEES:	Homeland Security Labor, Health, and Human Services, Education, and Related Agencies



# NUCLEAR REACTORS, MATERIALS, AND WASTE SECTOR

## SECTOR DESCRIPTION

The Nuclear Reactors, Materials, and Waste Sector (described in short as the Nuclear Sector) is composed of and deals with: (1) nuclear power plants with commercial reactors; (2) research, training, and test reactors; (3) deactivated nuclear facilities; (4) fuel cycle facilities; (4) nuclear materials transport; (5) radioactive waste management; and (6) radioactive materials.<sup>106</sup> DHS is the designated Sector-Specific Agency responsible for risk management of the Nuclear Reactors, Materials, and Waste Sector.<sup>107</sup>

## DISCUSSION

Medical diagnostics tests and imaging use isotopes.<sup>108</sup> The United States imports more than 90% of the medical isotopes it uses from a handful of reactors overseas<sup>109</sup> and it cannot be sure it will always be able to get the supplies the Nation needs.<sup>110</sup> During a pandemic, should tests and imaging that utilize medical isotopes prove useful in identifying infections, global demand would skyrocket. As with some medicines and essential medical supplies, the United States should not depend entirely on foreign countries for all the medical isotopes it needs now and may need in the future.

As biological events spread, they overwhelm the ability of hospitals and other healthcare facilities to understand and keep up with sterilization requirements. The Nuclear sector could use the radiation facilities it possesses to sterilize medical equipment and food, and study associated degradation.<sup>111</sup>

Additionally, some sector facilities possess high-powered equipment to examine nuclear particles. This equipment could also examine proteins that make up viruses and other microorganisms with atomic resolution.<sup>112</sup> Information this granular could prove useful in developing medical countermeasures that bind to specific proteins, limiting the ability of these microorganisms to replicate.

**RECOMMENDATION:** The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, should work with the Nuclear Reactors, Materials, and Waste Sector Coordinating Council to develop and examine biological risk and threat scenarios and determine what the sector can do to prevent the use of its assets to perpetrate and exacerbate biological events.

**RECOMMENDATION:** Congress should amend the American Medical Isotopes Production Act of 2012 (P.L. 112-239) to: (1) authorize and provide funds for the development of additional research and test reactors in the United States and establish domestic production of more medical isotopes and other radioactive sources needed for medical diagnostics; and (2) develop a pandemic preparedness plan for the radioisotope industry.<sup>113</sup>

**RECOMMENDATION:** The Secretary of Homeland Security, in coordination with the Secretary of Energy, Secretary of Agriculture, and Secretary of Health and Human Services should develop plans for the use of U.S. commercial and non-commercial nuclear facilities to sterilize medical equipment and prepare to provide such assistance early during biological events, before health care facilities are overrun with patients.

**RECOMMENDATION:** As part of the annual appropriations process, Congress should fund those national laboratories and academic facilities that possess particle accelerators to pursue immediately the use of high-powered equipment to examine proteins that comprise viruses and other microorganisms so that they will be able to contribute to national preparedness for and response to biological events.

CONGRESSIONAL JURISDICTION	
AUTHORIZATION COMMITTEES:	House Committee on Homeland Security
	Senate Committee on Homeland Security and Governmental Affairs
	House Committee on Energy and Commerce
	Senate Committee on Energy and Natural Resources
APPROPRIATIONS SUBCOMMITTEES:	Homeland Security
	Energy and Water Development, and Related Agencies

# TRANSPORTATION SYSTEMS SECTOR

## SECTOR DESCRIPTION

This sector is composed of seven subsectors: (1) aviation; (2) highway and motor carrier; (3) maritime transportation; (4) mass transit and passenger rail; (5) pipeline; (6) freight rail; and (7) postal and shipping.<sup>114</sup> DHS and DOT are the designated sector specific federal agencies responsible for risk management of the Transportation Systems Sector.<sup>115</sup>

## DISCUSSION

While COVID-19 and other diseases have taken advantage of air transit to spread throughout the world, all conveyances can spread disease. Despite paying a great deal of attention to the aviation subsector since September 11, 2001, TSA had few assets in place to protect against the introduction of biological agents and diseases into the air transit system, and fewer for other types of transit.

In response to biological threats against this Sector (and the Government Facilities Sector), DHS deployed BioWatch equipment in major metropolitan transit systems in order to detect a small set of biological agents.<sup>116</sup> Unfortunately, the technology currently utilized by BioWatch is insufficient and ineffective, leaving transit systems without adequate biodetection. Major metropolitan areas (e.g., New York City) have conducted their own research to examine biodetection in their subway systems and are moving forward on their own. The DHS Science and Technology Directorate has also developed biological detectors independent of the DHS Countering Weapons of Mass Destruction Office where the BioWatch and BD21 programs reside.

TSA, FAA<sup>117</sup>, and CDC issued limited guidance regarding airports and airlines over the past year.<sup>118</sup> TSA Federal Security Directors, airports, and airlines filled the void by making their own policy decisions and implementing policies independently at the Nation’s airports.<sup>119</sup> TSA claims responsibility for securing the Nation’s transportation systems.<sup>120</sup> The FAA retains responsibility for aviation public safety.<sup>121</sup> Both agencies expect the CDC to take responsibility for transportation-related public health, but the CDC is not authorized to regulate transportation, and generally only addresses disease reporting and infection control for various conveyances (including, but not limited to aviation). This means that none of these agencies are regulating the airline industry to ensure the health of the traveling public.

**RECOMMENDATION:** The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, should work with the Transportation Systems Sector Coordinating Council to develop and examine biological risk and threat scenarios and determine what the sector can do to prevent the use of its assets to perpetrate and exacerbate biological events.

**RECOMMENDATION:** The Secretary of Homeland Security should direct the Administrator of the Transportation Security Administration to address all conveyances equally with regard to preventing and controlling the spread of disease throughout the Sector, and work with important subsector-specific agencies and organizations, including the Commandant of the U.S. Coast Guard (with regard to the maritime system), Chief Executive Officer of Amtrak (with regard to passenger rail), the Postmaster General of the USPS, and Chief Executive Officers of commercial carriers (e.g., UPS, FedEx) (with regard to postal and shipping) to accomplish these objectives.

**RECOMMENDATION:** Congress should amend the Homeland Security Act of 2002 (P.L. 107-296, 116 Stat. 2135, 6 U.S.C. 298) to mandate that the Secretary of Homeland Security, acting through the Under Secretary of Science and Technology, obtain functional biodetection technology and reinvigorate BioWatch by 2023 or put an end to this program and any other acquisition program to replace BioWatch detectors (e.g., BD21).

**RECOMMENDATION:** Congress should amend the Homeland Security Act of 2002 (P.L. 107-296, 116 Stat. 2135, 6 U.S.C. 298) to direct the TSA, in coordination with the CDC and FAA, to develop and issue public health regulations for aviation conveyances, so that this element of the Transportation Systems Sector understands what they must do during a biological event and acts uniformly. Congress should also amend the Department of Transportation Act of 1966 (P.L. 89-670, 80 Stat. 931) to direct the DOT, in coordination with TSA and CDC, ensure that public health regulations are developed for all other conveyances similarly.

CONGRESSIONAL JURISDICTION	
AUTHORIZATION COMMITTEES:	House Committee on Homeland Security
	Senate Committee on Homeland Security and Governmental Affairs
	House Committee on Transportation and Infrastructure
	Senate Committee on Commerce, Science and Transportation
	Senate Committee on Banking, Housing, and Urban Affairs
APPROPRIATIONS SUBCOMMITTEES:	Homeland Security
	Transportation, and Housing and Urban Development, and Related Agencies

# WATER AND WASTEWATER SECTOR

## SECTOR DESCRIPTION

The Water and Wastewater Systems Sector is composed of: (1) drinking water infrastructure; and (2) wastewater infrastructure.<sup>122</sup> The EPA is the designated sector specific federal agency responsible for risk management of the Water and Wastewater Sector.<sup>123</sup>

## DISCUSSION

Concerns remain regarding the introduction of biological agents into the Nation’s water supplies. While drinking water treatment processes destroy most microbes, it is possible to find or develop pathogens hardy enough to resist water treatment. Bad actors may also attempt to disrupt water treatment processes. Additionally, not all water sources are treated (e.g., rivers, lakes, ponds, oceans). Agencies that monitor the environment test water sources for contamination but are often under-resourced and do not have the capacity, capability, or technology needed to test for all pathogens.

Sewage can be monitored for the presence of pathogens prior to treatment. Testing of sewage for the presence of COVID-19 is underway in the United States and overseas.<sup>124</sup> Such testing can provide valuable information for biosurveillance (e.g., which strain of a disease is present in which geographic areas, how much of the virus is present per measure of volume), but it cannot tell how many people have a particular disease.

**RECOMMENDATION:** The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, should work with the Waste and Wastewater Sector Coordinating Council to develop and examine biological scenarios and determine what the sector can do to prevent the use of its assets to perpetrate and exacerbate biological events.

**RECOMMENDATION:** For diseases that affect national security, Congress should amend the Federal Water Pollution Control Act of 1948 (also known as the Clean Water Act, 33 U.S.C. 1251 – 1376) to direct the EPA,<sup>125</sup> in coordination and cooperation with the CDC to: (1) identify sensitive, standardized methods (such as those recommended in the Commission’s *Apollo Program for Biodefense*<sup>126</sup> report) to detect novel and other diseases in wastewater; (2) develop, evaluate, and apply methods for concentrating and quantifying novel and other diseases in wastewater; and (3) develop assays to test wastewater. It should be feasible for wastewater treatment facilities throughout the Nation to use these methods, both technologically and financially.

CONGRESSIONAL JURISDICTION	
AUTHORIZATION COMMITTEES:	House Committee on Natural Resources
	Senate Committee on Energy and Natural Resources
	House Committee on Transportation and Infrastructure
	Senate Committee on Environment and Public Work
APPROPRIATIONS SUBCOMMITTEES:	Energy and Water Development and Related Agencies
	Interior, Environment, and Related Agencies

# ACRONYMS

<b>CDC</b>	Centers for Disease Control and Prevention
<b>CISA</b>	DHS Cybersecurity and Infrastructure Security Agency
<b>CMS</b>	Centers for Medicare and Medicaid Services
<b>COVID-19</b>	novel coronavirus 2019
<b>DHS</b>	Department of Homeland Security
<b>DOD</b>	Department of Defense
<b>DOE</b>	Department of Energy
<b>DOT</b>	Department of Transportation
<b>DPA</b>	Defense Production Act of 1950
<b>EMS</b>	Emergency Medical Services
<b>EPA</b>	Environmental Protection Agency
<b>FAA</b>	Federal Aviation Administration
<b>FBI</b>	Federal Bureau of Investigation
<b>FCC</b>	Federal Communications Commission
<b>FDA</b>	HHS Food and Drug Administration
<b>FEMA</b>	Federal Emergency Management Agency
<b>FPS</b>	Federal Protective Service
<b>GSA</b>	General Services Administration
<b>HHS</b>	Department of Health and Human Services
<b>IT</b>	information technology
<b>ONC</b>	HHS Office of the National Coordinator for Health IT
<b>PPE</b>	personal protective equipment
<b>SARS</b>	Severe Acute Respiratory Syndrome
<b>SARS-CoV-2</b>	SARS coronavirus 2
<b>SLTT</b>	state, local, tribal, and territorial
<b>TSA</b>	Transportation Security Administration
<b>USDA</b>	Department of Agriculture
<b>USPS</b>	United States Postal Service

# ENDNOTES

<sup>1</sup> Examples include: Executive Order 12938: Proliferation of Weapons of Mass Destruction, November 14, 1994 (see: <https://www.presidency.ucsb.edu/documents/executive-order-12938-proliferation-weapons-mass-destruction>); Executive Order 13010: Critical Infrastructure Protection, July 15, 1996 (see: Federal Register (July 17, 1996), v.61 no.138, p.37345-37350), and Presidential Decision Directive 63: Critical Infrastructure Protection, May 20, 1998 (<https://clinton.presidentiallibraries.us/items/show/12762>).

<sup>2</sup> High-priority biological agents deemed by the Centers for Disease Control and Prevention (CDC) to pose the greatest risk to the United States included anthrax. For more information and lists of Category A, B, and C biological agents, see: <https://emergency.cdc.gov/agent/agentlist-category.asp>.

<sup>3</sup> Department of Justice. (2010). Just Department and FBI Announce Formal Conclusion of Investigation into 2001 Anthrax Attacks. Retrieved from: <https://www.justice.gov/opa/pr/justice-department-and-fbi-announce-formal-conclusion-investigation-2001-anthrax-attacks>.

<sup>4</sup> Chapman R.E. and Leng C.J. (2004). Cost Effective Responses to Terrorist Risks in Constructed Facilities (NISTIR 7073). Washington, DC: National Institute of Standards and Technology, p. 1. See: <https://www.govinfo.gov/content/pkg/GOVPUB-C13-49a19c65c1886391034e1e9cc190151e/pdf/GOVPUB-C13-49a19c65c1886391034e1e9cc190151e.pdf>.

<sup>5</sup> Schmitt, K. and Zacchia, N. (2012). Total Decontamination Cost of the Anthrax Letter Attacks. *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* 10(1): 98-107. See: <https://www.liebertpub.com/doi/10.1089/bsp.2010.0053>.

<sup>6</sup> Zacchia N. and Schmitt K. (2018). Medical Spending for the 2001 Anthrax Letter Attacks. Cambridge University Press. See: <https://www.cambridge.org/core/journals/disaster-medicine-and-public-health-preparedness/article/abs/medical-spending-for-the-2001-anthrax-letter-attacks/A82DC64F622633EB22E7BEEA02F08FAA>.

<sup>7</sup> For more information on the Nation's critical infrastructure sectors, see: <https://www.cisa.gov/critical-infrastructure-sectors>.

<sup>8</sup> For more information on the National Critical Functions, see: <https://www.cisa.gov/national-critical-functions>.

<sup>9</sup> In addition to the Healthcare and Public Health Sector, the following critical infrastructure sectors also contribute to the effective execution of the national critical function to provide medical care: Chemical Sector; Communications Sector; Critical Manufacturing Sector; Emergency Services Sector; Energy Sector; Food and Agriculture Sector; Information Technology Sector; Nuclear Reactors, Materials, and Waste Sector; Transportation Systems Sector; and Water and Wastewater Sector.

<sup>10</sup> The Department of Homeland Security updated this guidance in August 2020. For more information, see Cybersecurity and Infrastructure Security Agency. (2020). Guidance on the Essential Critical Infrastructure Workforce: Ensuring Community and National Resilience in COVID-19 Response. Washington, DC: Department of Homeland Security. Retrieved from: [https://www.cisa.gov/sites/default/files/publications/ECIW\\_4.0\\_Guidance\\_on\\_Essential\\_Critical\\_Infrastructure\\_Workers\\_Final3\\_508\\_0.pdf](https://www.cisa.gov/sites/default/files/publications/ECIW_4.0_Guidance_on_Essential_Critical_Infrastructure_Workers_Final3_508_0.pdf).

- <sup>11</sup> Cybersecurity and Infrastructure Security Agency. (2019). National Critical Functions Set. Washington, DC: Department of Homeland Security. Retrieved from: <https://www.cisa.gov/national-critical-functions-set>.
- <sup>12</sup> Argonne National Laboratory, for example, utilizes computational modeling to assess the dispersion of biological agents in a subway system. For more information, see: <https://www.anl.gov/sss/the-argonne-below-ground-model-for-the-assessment-of-subway-threats>.
- <sup>13</sup> Lardner G. (1980). Army Report Details Germ War Exercise in NY Subway in '66. *The Washington Post*. See: <https://www.washingtonpost.com/archive/politics/1980/04/22/army-report-details-germ-war-exercise-in-ny-subway-in-66/70772a8b-8223-47de-99b4-876d5e57dd9c/>.
- <sup>14</sup> Yves T., Vogel G., Wunderli W., Suter P., Witschi, M, Koch D., Tapparel C., and Kaiser L. (2008). Survival of Influenza Virus on Banknotes. *Applied and Environmental Microbiology* 74(10): 3002-3007. See: doi: 10.1128/AEM.00076-08.
- <sup>15</sup> Cybersecurity and Infrastructure Security Agency. Sector Risk Management Agencies. Washington, DC: Department of Homeland Security. Retrieved from: <https://www.cisa.gov/sector-risk-management-agencies>.
- <sup>16</sup> Guidance on the Essential Critical Infrastructure Workforce: Ensuring Community and National Resilience in COVID-19 Response. Washington, DC: Department of Homeland Security. Retrieved from: [https://www.cisa.gov/sites/default/files/publications/ECIW\\_4.0\\_Guidance\\_on\\_Essential\\_Critical\\_Infrastructure\\_Workers\\_Final3\\_508\\_0.pdf](https://www.cisa.gov/sites/default/files/publications/ECIW_4.0_Guidance_on_Essential_Critical_Infrastructure_Workers_Final3_508_0.pdf).
- <sup>17</sup> Bipartisan Commission on Biodefense. (2015). A National Blueprint for Biodefense: Leadership and Major Reform Needed to Optimize Efforts. Washington, DC: Bipartisan Commission on Biodefense. Available at: <https://biodefensecommission.org/reports/a-national-blueprint-forbiodefense/>.
- <sup>18</sup> Cybersecurity and Infrastructure Security Agency. (2020). Guidance on the Essential Critical Infrastructure Workforce: Ensuring Community and National Resilience in COVID-19 Response. Washington, DC: Department of Homeland Security. Retrieved from: [https://www.cisa.gov/sites/default/files/publications/ECIW\\_4.0\\_Guidance\\_on\\_Essential\\_Critical\\_Infrastructure\\_Workers\\_Final3\\_508\\_0.pdf](https://www.cisa.gov/sites/default/files/publications/ECIW_4.0_Guidance_on_Essential_Critical_Infrastructure_Workers_Final3_508_0.pdf).
- <sup>19</sup> Shell Global. Shell Scenarios. Retrieved from: <https://www.shell.com/energy-and-innovation/the-energy-future/scenarios.html>.
- <sup>20</sup> The Department of Homeland Security issued this guidance in March 2020 and updated it in August 2020. For more information, see Cybersecurity and Infrastructure Security Agency. (2020). Guidance on the Essential Critical Infrastructure Workforce: Ensuring Community and National Resilience in COVID-19 Response. Washington, DC: Department of Homeland Security. Retrieved from: [https://www.cisa.gov/sites/default/files/publications/ECIW\\_4.0\\_Guidance\\_on\\_Essential\\_Critical\\_Infrastructure\\_Workers\\_Final3\\_508\\_0.pdf](https://www.cisa.gov/sites/default/files/publications/ECIW_4.0_Guidance_on_Essential_Critical_Infrastructure_Workers_Final3_508_0.pdf).
- <sup>21</sup> Cybersecurity and Infrastructure Security Agency. Chemical Sector: Sector Overview. Retrieved from: <https://www.cisa.gov/chemical-sector>.
- <sup>22</sup> Cybersecurity and Infrastructure Security Agency. Sector Risk Management Agencies. Retrieved from: <https://www.cisa.gov/sector-risk-management-agencies>.

- <sup>23</sup> American Chemistry Council. (2020). Chemical Industry Outlook: Recovery from the COVID-19 Global Recession. American Chemistry Council. Retrieved from: <https://www.americanchemistry.com/Media/PressReleasesTranscripts/ACC-news-releases/Chemical-Industry-Outlook-Recovery-from-the-covid-19-Global-Recession.html>.
- <sup>24</sup> Lakavage A. (2020). COVID-19 has Exposed Cracks in the Global Medicines Supply Chain. We need to fix them. *STAT News*. Retrieved from: <https://www.statnews.com/2020/06/02/covid-19-exposed-cracks-global-medicines-supply-chain/>.
- <sup>25</sup> Bookwalter C.M. (2021). Drug Shortages Amid the COVID-19 Pandemic. *U.S. Pharmacist* 46 (2): 25-28. Retrieved from: <https://www.uspharmacist.com/article/drug-shortages-amid-the-covid19-pandemic#:~:text=Some%20drugs%20that%20have%20been,and%20chloroquine%2C%20and%20sedation%20medications>.
- <sup>26</sup> Food and Drug Administration. (2021). FDA Drug Shortages. Washington, DC: Department of Health and Human Services. Retrieved from: <https://www.accessdata.fda.gov/scripts/drugshortages/default.cfm>.
- <sup>27</sup> Cybersecurity and Infrastructure Security Agency. (2020). Secure Your Chemicals: Before, During, and After a Pandemic. Washington, DC: Department of Homeland Security. Retrieved from: <https://www.cisa.gov/publication/secure-chemicals-pandemic>.
- <sup>28</sup> Cybersecurity and Infrastructure Security Agency. (2020). Chemical Facility Anti-Terrorism Standards. Washington, DC: Department of Homeland Security. Retrieved from: <https://www.cisa.gov/chemical-facility-anti-terrorism-standards>.
- <sup>29</sup> Cybersecurity and Infrastructure Security Agency. Commercial Facilities Sector. Retrieved from: <https://www.cisa.gov/commercial-facilities-sector>.
- <sup>30</sup> Cybersecurity and Infrastructure Security Agency. Sector Risk Management Agencies. Retrieved from: <https://www.cisa.gov/sector-risk-management-agencies>.
- <sup>31</sup> Markowitz A. (2020). Outbreak Turns Stadiums into Hospitals and Food Pantries. *AARP*. Retrieved from: <https://www.aarp.org/health/conditions-treatments/info-2020/coronavirus-sports-stadiums.html>.
- <sup>32</sup> Thompson T. (2020). See how Sports Stadiums have Transformed to Help Pandemic Relief Efforts. *National Geographic*. Retrieved from: <https://www.nationalgeographic.com/history/article/sports-stadiums-transformed-help-pandemic-relief-efforts>.
- <sup>33</sup> Armstrong D. (2017). A Look Back: 1976, and how Legionnaires' Disease Got its Name. *Legionnaires' Disease News*. Retrieved from: <https://www.legionnairesdiseasenews.com/2017/07/look-back-1976-legionnaires-disease-got-name/>.
- <sup>34</sup> Musumeci N. (2020). What's a COVID-19 Superspreader Event? Six glaring examples. *New York Post*. Retrieved from: <https://nypost.com/article/what-is-a-covid-19-superspreader-event-definition-examples/>.
- <sup>35</sup> Congressional Research Service. (2020). National Special Security Events: Fact Sheet. Washington, DC: Congressional Research Service, p. 1. Retrieved from: <https://crsreports.congress.gov/product/pdf/R/R43522/11>.



- <sup>36</sup> Department of Homeland Security. (2015). Communications Sector-Specific Plan: an annex to the NIPP 2013. Washington, DC: Department of Homeland Security. Retrieved from: <https://www.cisa.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf>.
- <sup>37</sup> Cybersecurity and Infrastructure Security Agency. Sector Risk Management Agencies. Retrieved from: <https://www.cisa.gov/sector-risk-management-agencies>.
- <sup>38</sup> PwC. (2020). COVID-19 and the Telecommunications Industry: Practical Steps for Responding to the Coronavirus Crisis. PwC. Retrieved from: <https://www.pwc.com/us/en/library/covid-19/coronavirus-telecommunication-impact.html>.
- <sup>39</sup> Wharton School. (2020). Combating COVID-19: Lessons from Singapore, South Korea, and Taiwan. Retrieved from: <https://knowledge.wharton.upenn.edu/article/singapore-south-korea-taiwan-used-technology-combat-covid-19/>.
- <sup>40</sup> Francisco P. (2021). Comments before the Bipartisan Commission on Biodefense: Holding the Line on Biodefense: Supporting First Response to Large-Scale Biological Events (March 23, 2021). Retrieved from: <https://biodefensecommission.org/events/holding-the-line-on-biodefense-supporting-first-response-to-large-scale-biological-events/>.
- <sup>41</sup> Federal Communications Commission. (2020). COVID-19 Telehealth Program. Washington, DC: Federal Communications Commission. Retrieved from: <https://www.fcc.gov/covid-19-telehealth-program>.
- <sup>42</sup> Cybersecurity and Infrastructure Security Agency. Critical Manufacturing Sector: Sector Overview. Retrieved from: <https://www.cisa.gov/critical-manufacturing-sector>.
- <sup>43</sup> Cybersecurity and Infrastructure Security Agency. Sector Risk Management Agencies. Retrieved from: <https://www.cisa.gov/sector-risk-management-agencies>.
- <sup>44</sup> Congressional Research Service. (2020, July 28). Defense Production Act (DPA): Recent Developments in Response to COVID-19. Washington, DC: Congressional Research Service. Retrieved from: <https://crsreports.congress.gov/product/pdf/IN/IN11470>.
- <sup>45</sup> Jacobs A. (2021). Despite Claims, Trump Rarely Uses Wartime Law in Battle Against COVID. *The New York Times*. Retrieved from: <https://www.nytimes.com/2020/09/22/health/Covid-Trump-Defense-Production-Act.html>.
- <sup>46</sup> Executive Order 13987. (2021). Organizing and Mobilizing the United States Government to Provide a Unified and Effective Response to Combat COVID-19 and to Provide United States Leadership on Global Health and Security. Washington, DC: The White House. Retrieved from: <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/20/executive-order-organizing-and-mobilizing-united-states-government-to-provide-unified-and-effective-response-to-combat-covid-19-and-to-provide-united-states-leadership-on-global-health-and-security/>.
- <sup>47</sup> Executive Order 14001. (2021). A Sustainable Public Health Supply Chain. Washington, DC: The White House. Retrieved from: <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/21/executive-order-a-sustainable-public-health-supply-chain/>.

- <sup>48</sup> Department of Health and Human Services Press Office. (2021). Biden Administration Announces Historic Manufacturing Collaboration Between Merck and Johnson & Johnson to Expand Production of COVID-19 Vaccines. Washington, DC: Department of Health and Human Services. Retrieved from: <https://www.hhs.gov/about/news/2021/03/02/biden-administration-announces-historic-manufacturing-collaboration-between-merck-johnson-johnson-expand-production-covid-19-vaccines.html>.
- <sup>49</sup> Karbassi S. (2021). Understanding Biden's Invocation of the Defense Production Act. *Lawfare Blog*. Retrieved from: <https://www.lawfareblog.com/understanding-bidens-invocation-defense-production-act>.
- <sup>50</sup> Department of Homeland Security. (2015). Dams Sector-Specific Plan: an annex to the NIPP 2013. Washington, DC: Department of Homeland Security, p. 2. Retrieved from: <https://www.cisa.gov/sites/default/files/publications/nipp-ssp-dams-2015-508.pdf>.
- <sup>51</sup> Cybersecurity and Infrastructure Security Agency. Sector Risk Management Agencies. Retrieved from: <https://www.cisa.gov/sector-risk-management-agencies>.
- <sup>52</sup> Cybersecurity and Infrastructure Security Agency. Dams Sector Snapshot. Washington, DC: Department of Homeland Security, p.2. Retrieved from: [https://www.dhs.gov/xlibrary/assets/nipp\\_snapshot\\_dams.pdf#:~:text=and%20severe%20long-term%20consequences.%20Residual%20effects%20of%20dam,impact%20C%20dams%20are%20considered%20a%20possible%20terrorist%20target](https://www.dhs.gov/xlibrary/assets/nipp_snapshot_dams.pdf#:~:text=and%20severe%20long-term%20consequences.%20Residual%20effects%20of%20dam,impact%20C%20dams%20are%20considered%20a%20possible%20terrorist%20target).
- <sup>53</sup> Cybersecurity and Infrastructure Security Agency. Defense Industrial Base Sector. Retrieved from: <https://www.cisa.gov/defense-industrial-base-sector>.
- <sup>54</sup> Cybersecurity and Infrastructure Security Agency. Sector Risk Management Agencies. Retrieved from: <https://www.cisa.gov/sector-risk-management-agencies>.
- <sup>55</sup> Mehta A. (2020). How Coronavirus Could Impact the Defense Supply Chain. *Defense News*. Retrieved from: <https://www.defensenews.com/industry/2020/03/20/how-coronavirus-could-impact-the-defense-supply-chain/>.
- <sup>56</sup> Gould J. (2020). COVID Closed Mexican Factories that Supply U.S. Defense Industry. The Pentagon Wants Them Opened. *Defense News*. Retrieved from: <https://www.defensenews.com/2020/04/21/covid-closed-mexican-factories-that-supply-us-defense-industry-the-pentagon-wants-them-opened/>.
- <sup>57</sup> Department of Defense. (2018). Instruction 3020.45: Mission Assurance Construct. Washington, DC: Department of Defense. Retrieved from: <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/302045p.pdf?ver=2018-08-14-081232-450>.
- <sup>58</sup> "A Special Access Program is established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level." Defense Counterintelligence and Security Agency. Special Access Programs. Washington, DC: Department of Defense. Retrieved from: <https://www.cdse.edu/catalog/sap.html>.
- <sup>59</sup> The White House. (2018). National Biodefense Strategy. Washington, DC: The White House. Retrieved from: <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Biodefense-Strategy.pdf>.

- <sup>60</sup> Department of Defense. (2018). Summary of the 2018 National Defense Strategy of the United States of America. Retrieved from: <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.
- <sup>61</sup> The White House. (2017). National Security Strategy of the United States of America. Retrieved from: <https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.
- <sup>62</sup> Cybersecurity and Infrastructure Security Agency. Emergency Services Sector: Sector Overview. Retrieved from: <https://www.cisa.gov/emergency-services-sector>.
- <sup>63</sup> Cybersecurity and Infrastructure Security Agency. Sector Risk Management Agencies. Retrieved from: <https://www.cisa.gov/sector-risk-management-agencies>.
- <sup>64</sup> Committee on Homeland Security. (2017). Advancing the Homeland Security Information Sharing Environment: A Review of the National Network of Fusion Centers. Washington, DC: U.S. House of Representatives. Retrieved from: <https://www.hsdl.org/?abstract&did=805450>.
- <sup>65</sup> Cybersecurity and Infrastructure Security Agency. Energy Sector: Sector Overview. Retrieved from: <https://www.cisa.gov/energy-sector>.
- <sup>66</sup> Cybersecurity and Infrastructure Security Agency. Sector Risk Management Agencies. Retrieved from: <https://www.cisa.gov/sector-risk-management-agencies>.
- <sup>67</sup> Jiang P., Fan Y.V., Kleme? J.J. (2021). Impacts of COVID-19 on Energy Demand and Consumption: Challenges, Lessons and Emerging Opportunities. *Applied Energy* 285: 116441. Retrieved from: doi:10.1016/j.apenergy.2021.116441.
- <sup>68</sup> Department of Energy. (2020). Department of Energy Announces COVID-19 Innovation Portal and Assistance Program. Washington, DC: Department of Energy. Retrieved from: <https://www.energy.gov/articles/department-energy-announces-covid-19-innovation-portal-and-assistance-program>.
- <sup>69</sup> Department of Homeland Security. (2015). Financial Services Sector-Specific Plan, p. 6. Washington, DC: Department of Homeland Security. Retrieved from: <https://www.cisa.gov/sites/default/files/publications/nipp-ssp-financial-services-2015-508.pdf>.
- <sup>70</sup> Cybersecurity and Infrastructure Security Agency. Sector Risk Management Agencies. Retrieved from: <https://www.cisa.gov/sector-risk-management-agencies>.
- <sup>71</sup> Marte J. (2021). Fed Officials Say U.S. Economy Still in Depths of Recession, More Relief Needed. *Reuters*. Retrieved from: <https://www.reuters.com/article/us-usa-fed-labor/fed-officials-say-u-s-economy-still-in-depths-of-recession-more-relief-needed-idUSKBN2A13MC>.
- <sup>72</sup> Schieber J., Crichton D. (2020). Stock Markets Halted for Unprecedented Third Time Due to Coronavirus Scare. *TechCrunch*. Retrieved from: <https://techcrunch.com/2020/03/16/stock-markets-halted-for-third-time-as-heavy-selling-trips-circuit-breakers-due-to-coronavirus-scare/>.

- <sup>73</sup> “The Federal Reserve System is the central bank of the United States. It performs five general functions to promote the effective operation of the U.S. economy and, more generally, the public interest. The Federal Reserve: (1) conducts the nation’s monetary policy to promote maximum employment, stable prices, and moderate long-term interest rates in the U.S. economy; (2) promotes the stability of the financial system and seeks to minimize and contain systemic risks through active monitoring and engagement in the U.S. and abroad; (3) promotes the safety and soundness of individual financial institutions and monitors their impact on the financial system as a whole; (4) fosters payment and settlement system safety and efficiency through services to the banking industry and the U.S. government that facilitate U.S.-dollar transactions and payments; and (5) promotes consumer protection and community development through consumer-focused supervision and examination, research and analysis of emerging consumer issues and trends, community economic development activities, and the administration of consumer laws and regulations.” Board of Governors of the Federal Reserve System. (2020). About the Fed. Washington, DC: Board of Governors of the Federal Reserve System. Retrieved from: <https://www.federalreserve.gov/aboutthefed.htm>.
- <sup>74</sup> A currency swap line is an agreement between two central banks to exchange currencies, allowing a central bank to obtain foreign currency liquidity from the central bank that issues it to provide liquidity to domestic commercial banks. European Central Bank. (2021). What are Currency Swap Lines? Retrieved from: [https://www.ecb.europa.eu/explainers/tell-me-more/html/currency\\_swap\\_lines.en.html](https://www.ecb.europa.eu/explainers/tell-me-more/html/currency_swap_lines.en.html).
- <sup>75</sup> Board of Governors of the Federal Reserve System. Coronavirus Disease 2019 (COVID-2019). Retrieved from: <https://www.federalreserve.gov/covid-19.htm>.
- <sup>76</sup> Board of Governors of the Federal Reserve System. Coronavirus Disease 2019 (COVID-2019): General Frequently Asked Questions. Retrieved from: <https://www.federalreserve.gov/covid-19-faqs.htm>.
- <sup>77</sup> “The exercise, conducted between September 24 and October 12, 2007, was the largest pandemic exercise ever held for financial services industry. The Treasury Department, in partnership with FSSCC [Financial Services Sector Coordinating Council] and FBIIIC [Financial and Banking Information Infrastructure Committee], and the Securities Industry and Financial Management Association (SIFMA) sponsored the sector-wide pandemic.” Department of the Treasury. (2008). US Financial Sector Pandemic Flu Exercise Prompts Enhanced Industry Preparations. Washington, DC: Department of the Treasury. Retrieved from: <https://www.treasury.gov/press-center/press-releases/Pages/hp769.aspx>.
- <sup>78</sup> Food and Drug Administration, Department of Agriculture, and Department of Homeland Security. (2015). Food and Agriculture Sector-Specific Plan, p. 4. Retrieved from: <https://www.cisa.gov/sites/default/files/publications/nipp-ssp-food-ag-2015-508.pdf>.
- <sup>79</sup> Cybersecurity and Infrastructure Security Agency. Sector Risk Management Agencies. Retrieved from: <https://www.cisa.gov/sector-risk-management-agencies>.
- <sup>80</sup> Economic Research Service. (2020). Ag and Food Sectors and the Economy. Washington, DC: Department of Agriculture. Retrieved from: <https://www.ers.usda.gov/data-products/ag-and-food-statistics-charting-the-essentials/ag-and-food-sectors-and-the-economy/>.

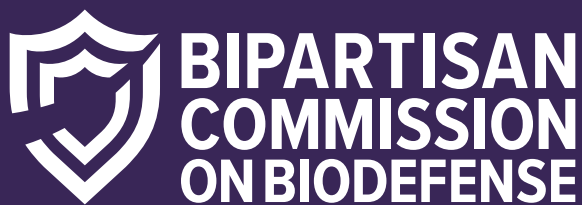


- <sup>81</sup> The White House. (2018). National Biodefense Strategy. Washington, DC: The White House. Retrieved from: <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Biodefense-Strategy.pdf>.
- <sup>82</sup> The White House. (2004). Homeland Security Presidential Directive 9: The Defense of United States Agriculture and Food. Retrieved from: <https://georgewbush-whitehouse.archives.gov/news/releases/2004/02/20040203-2.html>.
- <sup>83</sup> Cybersecurity and Infrastructure Security Agency. Government Facilities Sector: Sector Overview. Retrieved from: <https://www.cisa.gov/government-facilities-sector>.
- <sup>84</sup> Cybersecurity and Infrastructure Security Agency. Sector Risk Management Agencies. Retrieved from: <https://www.cisa.gov/sector-risk-management-agencies>.
- <sup>85</sup> For more information about COVID-19 (Coronavirus) GSA Activities, see: <https://www.gsa.gov/governmentwide-initiatives/emergency-response/covid19-coronavirus>.
- <sup>86</sup> Federal Protective Service. (2018). Hazardous Response Program. Washington, DC: Department of Homeland Security. Retrieved from: <https://www.dhs.gov/hazardous-response-program>.
- <sup>87</sup> Department of Health and Human Services and Department of Homeland Security. (2016). Healthcare and Public Health Sector-Specific Plan, p.5. Washington, DC: Department of Health and Human Services and Department of Homeland Security. Retrieved from: <https://www.cisa.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf>.
- <sup>88</sup> Department of Health and Human Services and Department of Homeland Security. (2016). Healthcare and Public Health Sector-Specific Plan, p.6. Washington, DC: Department of Health and Human Services and Department of Homeland Security. Retrieved from: <https://www.cisa.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf>.
- <sup>89</sup> Cybersecurity and Infrastructure Security Agency. Sector Risk Management Agencies. Retrieved from: <https://www.cisa.gov/sector-risk-management-agencies>.
- <sup>90</sup> Bipartisan Commission on Biodefense. (2015). A National Blueprint for Biodefense: Leadership and Major Reform Needed to Optimize Efforts. Washington, DC: Bipartisan Commission on Biodefense, p. 41. Available at: <https://biodefensecommission.org/reports/a-national-blueprint-forbiodefense/>.
- <sup>91</sup> Department of Health and Human Services. (2018). HHS Selects Pilot Projects to Demonstrate Better Approach to Disaster Medical Care. Washington, DC: Department of Health and Human Services. Retrieved from: <https://www.hhs.gov/about/news/2018/09/27/hhs-selects-pilot-projects-demonstrate-better-approach-disaster-medical-care.html>.
- <sup>92</sup> American Medical Association. (2020). CMS Payment Policies and Regulatory Flexibilities During COVID-19 Emergency. Retrieved from: <https://www.ama-assn.org/practice-management/medicare/cms-payment-policies-regulatory-flexibilities-during-covid-19>.
- <sup>93</sup> Centers for Medicare and Medicaid Services. (2021). New COVID-19 Treatments Add-On Payment. Washington, DC: Department of Health and Human Services. Retrieved from: <https://www.cms.gov/medicare/covid-19/new-covid-19-treatments-add-payment-ncap>.

- <sup>94</sup> “The Hospital Preparedness Program (HPP) is a cooperative agreement program administered by ASPR that establishes a foundation for national health care preparedness. As the only source of federal funding for health care system preparedness and response, HPP promotes a consistent national focus to improve patient outcomes during emergencies and disasters and enables rapid recovery.” Office of the Assistant Secretary for Preparedness Response. (2020). Hospital Preparedness Program. Washington, DC: Department of Health and Human Services. Retrieved from: <https://www.phe.gov/preparedness/planning/hpp/pages/default.aspx>.
- <sup>95</sup> Department of Homeland Security. (2016). Information Technology Sector-Specific Plan: an annex to the NIPP 2013, p.3. Washington, DC: Department of Homeland Security. Retrieved from: <https://www.cisa.gov/sites/default/files/publications/nipp-ssp-information-technology-2016-508.pdf>.
- <sup>96</sup> Department of Health and Human Services and Department of Homeland Security. (2016). Healthcare and Public Health Sector-Specific Plan, p.5. Washington, DC: Department of Health and Human Services and Department of Homeland Security. Retrieved from: <https://www.cisa.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf>.
- <sup>97</sup> Cybersecurity and Infrastructure Security Agency. Sector Risk Management Agencies. Retrieved from: <https://www.cisa.gov/sector-risk-management-agencies>.
- <sup>98</sup> Lohrmann D. (2020). 2020: The Year the COVID-19 Crisis Brought a Cyber Pandemic. *Government Technology*. Retrieved from: <https://www.govtech.com/blogs/lohmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html>.
- <sup>99</sup> Katz J. (2021). CrowdStrike: Pandemic Drove 2020 Uptick in Cyberattacks. *Federal Computer Week*. Retrieved from: <https://fcw.com/articles/2021/02/22/crowdstrike-cyber-ransomware-covid.aspx>.
- <sup>100</sup> Kellermann T. (2021). Hackers are Targeting COVID-19 Vaccinations. Here's How to Stop Them. *CNBC*. Retrieved from: <https://www.cnbc.com/2021/02/17/op-ed-how-to-stop-hackers-targeting-covid-19-vaccinations.html>.
- <sup>101</sup> Sebenius A. and Martin A. (2020). Russia, North Korea Targeted COVID Research with Cyber-Attacks. *Bloomberg*. Retrieved from: <https://www.bloomberg.com/news/articles/2020-11-13/russia-north-korea-targeted-covid-research-with-cyber-attacks>.
- <sup>102</sup> Osborne R. (2020). As COVID-19 Vaccine Research Revs Up, So Do Cyberattacks. *BioWorld*. Retrieved from: <https://www.bioworld.com/articles/500361-as-covid-19-vaccine-research-revs-up-so-do-cyberattacks-report>.
- <sup>103</sup> Cowan R. (2020). Cyber Attacks Seen on Coronavirus Vaccine Infrastructure - U.S. Senator Peters. *Reuters*. Retrieved from: <https://www.reuters.com/article/health-coronavirus-vaccine-cyber/cyber-attacks-seen-on-coronavirus-vaccine-infrastructure-u-s-senator-peters-idUSKBN28K2BR>.
- <sup>104</sup> Pompon R. (2021). Cybersecurity Threats to the COVID-19 Vaccine. *F5 Labs*. Retrieved from: <https://www.f5.com/labs/articles/threat-intelligence/cybersecurity-threats-to-the-covid-19-vaccine>.

- <sup>105</sup> The Office of the National Coordinator for Health Information Technology. (2019). About ONC. Washington, DC: Department of Health and Human Services. Retrieved from: <https://www.healthit.gov/topic/about-onc>.
- <sup>106</sup> Department of Homeland Security. (2015). Nuclear Reactors, Materials, and Waste Sector-Specific Plan: an annex to the NIPP 2013, p. 4-8. Washington, DC: Department of Homeland Security. Retrieved from: <https://www.cisa.gov/sites/default/files/publications/nipp-ssp-nuclear-2015-508.pdf>.
- <sup>107</sup> Cybersecurity and Infrastructure Security Agency. Sector Risk Management Agencies. Retrieved from: <https://www.cisa.gov/sector-risk-management-agencies>.
- <sup>108</sup> Department of Homeland Security. (2019). Nuclear Reactors, Materials, and Waste Sector Overview. Washington, DC: Department of Homeland Security. Retrieved from: <https://www.cisa.gov/nuclear-reactors-materials-and-waste-sector>.
- <sup>109</sup> Department of Homeland Security (2015). Nuclear Reactors, Materials, and Waste Sector-Specific Plan. Washington, DC: Department of Homeland Security, p. v. Retrieved from: <https://www.cisa.gov/sites/default/files/publications/nipp-ssp-nuclear-2015-508.pdf>.
- <sup>110</sup> TRIUMF. (2008). Making Medical Isotopes: Report of the Task Force on Alternatives for Medical-Isotope Production. Vancouver, BC: TRIUMF. Retrieved from: <https://www.triumf.ca/sites/default/files/Making-Medical-Isotopes-PREPUB.pdf>.
- <sup>111</sup> Cybersecurity and Infrastructure Security Agency. (2015). Nuclear Reactors, Materials, and Waste Sector-Specific Plan. Washington, DC: Department of Homeland Security, p. 8. Retrieved from: <https://www.cisa.gov/sites/default/files/publications/nipp-ssp-nuclear-2015-508.pdf>.
- <sup>112</sup> Office of Scientific and Technical Information (2020.) DOE National Laboratory Capabilities for COVID-19 Response. Washington, DC: Department of Energy. Retrieved from: <https://science.osti.gov/-/media/nvbl/pdf/DOE-Laboratory-Capabilities-100120-final.pdf?la=en&hash=DBC7FB3CEFC5B15D2352EBAD695F6EF4D98955D2&hash=DBC7FB3CEFC5B15D2352EBAD695F6EF4D98955D2>.
- <sup>113</sup> Cybersecurity and Infrastructure Security Agency. (2015). Nuclear Reactors, Materials, and Waste Sector-Specific Plan. Washington, DC: Department of Homeland Security, p. 16. Retrieved from: <https://www.cisa.gov/sites/default/files/publications/nipp-ssp-nuclear-2015-508.pdf>.
- <sup>114</sup> Cybersecurity and Infrastructure Security Agency. Transportation Systems Sector: Sector Overview. Retrieved from: <https://www.cisa.gov/transportation-systems-sector>.
- <sup>115</sup> Cybersecurity and Infrastructure Security Agency. Sector Risk Management Agencies. Retrieved from: <https://www.cisa.gov/sector-risk-management-agencies>.
- <sup>116</sup> Countering Weapons of Mass Destruction Office. (2020). Detecting Bioterrorist Attacks. Washington, DC: Department of Homeland Security. Retrieved from: <https://www.dhs.gov/biowatch-program>.
- <sup>117</sup> The Federal Aviation Administration's "...mission is to provide the safest, most efficient aerospace system in the world." Federal Aviation Administration. (2020). Washington, DC: Department of Transportation. Retrieved from: <https://www.faa.gov/about/>.

- <sup>118</sup> For example, see Centers for Disease Control and Prevention. (2020). Updated Interim Guidance for Airlines and Airline Crew: Coronavirus Disease 2019 (COVID-19). Washington DC: Department of Health and Human Services. Retrieved from: <https://www.cdc.gov/quarantine/air/managing-sick-travelers/ncov-airlines.html>.
- <sup>119</sup> Aratani L. (2020). With Few Rules in Place, Airlines, Airports Adopt Their Own Strategies for Combating the Coronavirus. *The Washington Post*. Retrieved from: [https://www.washingtonpost.com/local/trafficandcommuting/with-few-rules-in-place-airlines-airports-adopt-their-own-strategies-for-combating-the-coronavirus/2020/06/27/8719037e-b4b0-11ea-aca5-ebb63d27e1ff\\_story.html](https://www.washingtonpost.com/local/trafficandcommuting/with-few-rules-in-place-airlines-airports-adopt-their-own-strategies-for-combating-the-coronavirus/2020/06/27/8719037e-b4b0-11ea-aca5-ebb63d27e1ff_story.html).
- <sup>120</sup> Transportation Security Administration. About Mission. Washington, DC: Transportation Security Administration. Retrieved from: <https://www.tsa.gov/about/tsa-mission>.
- <sup>121</sup> Federal Aviation Administration. (2019). About FAA, Mission. Washington, DC: Federal Aviation Administration. Retrieved from: <https://www.faa.gov/about/mission/>.
- <sup>122</sup> Department of Homeland Security and Environmental Protection Agency. (2015). Water and Wastewater Systems Sector-Specific Plan, p. 2-8. Washington, DC: Department of Homeland Security and Environmental Protection Agency. Retrieved from: <https://www.cisa.gov/sites/default/files/publications/nipp-ssp-water-2015-508.pdf>.
- <sup>123</sup> Cybersecurity and Infrastructure Security Agency. Sector Risk Management Agencies. Retrieved from: <https://www.cisa.gov/sector-risk-management-agencies>.
- <sup>124</sup> Centers for Disease Control and Prevention. (2020). Developing a Wastewater Surveillance Sampling Strategy. Washington, DC: Department of Health and Human Services. Retrieved from: <https://www.cdc.gov/coronavirus/2019-ncov/cases-updates/wastewater-surveillance/developing-a-wastewater-surveillance-sampling-strategy.html>.
- <sup>125</sup> The Environmental Protection Agency protects human health and environment. Environmental Protection Agency. About EPA. Washington, DC: Environmental Protection Agency. Retrieved from: <https://www.epa.gov/aboutepa>.
- <sup>126</sup> Bipartisan Commission on Biodefense. (2021). The Apollo Program for Biodefense: Winning the Race Against Biological Threats. Washington, DC: Bipartisan Commission on Biodefense, p. 16. Available at: <https://biodefensecommission.org/reports/the-apollo-program-for-biodefense-winning-the-race-against-biological-threats/>.



[www.biodefensecommission.org](http://www.biodefensecommission.org)