(U) U.S. CRITICAL INFRASTRUCTURE 2025: A STRATEGIC RISK ASSESSMENT

April 2016

NATIONAL PROTECTION AND PROGRAMS DIRECTORATE

OFFICE OF CYBER AND INFRASTRUCTURE ANALYSIS

(U) This page intentionally left blank.

(U) EXECUTIVE SUMMARY

(U) This strategic risk assessment provides an overview of six distinguishable trends emerging in U.S. critical infrastructure. These trends, when combined or examined singularly, are likely to significantly influence critical infrastructure and its resiliency during the next 10 years. The U.S. Department of Homeland Security/Office of Cyber and Infrastructure Analysis identified the following trends likely to have a profound effect on critical infrastructure:

- Convergence of the Cyber and Physical Domains
- Aerial Threats: NTAT (Non-Traditional Aviation Technology)
- Evolving Terrorist Threat
- Facing the Inevitable: The State of U.S. Infrastructure
- Extreme Weather: A Gloomy Forecast
- Next Pandemic: Emergence and Outbreak

(U) U.S. critical infrastructure is the foundation on which the Nation's economy, security, and health rely. Critical infrastructure sustains the American way of life and bolsters national competitiveness. It supplies industry and business with the means to sustain operational success, and it enables the United States to maintain influence in the global community. Infrastructure preserves a sound economy by keeping millions employed and inspires innovative technology to improve the welfare of Americans.

(U) The Nation's infrastructure comprises 16 sectors. Most notable are the physical facilities that supply communities with goods and services like water, energy, transportation, and fuel. The Nation's infrastructure also includes cyber technology that connects businesses; allows utilities to efficiently monitor energy supply and demand; and supports the critical infrastructure systems that ensure convenient access to funds in bank accounts, map the best route to a destination, and ensure an uninterrupted power supply. Ensuring the security and resilience of critical infrastructure is a national priority that requires planning and coordination across all levels of government and the private sector. Improving roads, bridges, water systems, electrical grids, and other vital infrastructure systems requires innovation, investment, and shared commitment.

(U) Some of the emerging trends influencing critical infrastructure in the United States are known and well understood; yet, their consequences are uncertain. Understanding the cascading impacts of these trends is challenging because of the interconnectedness of infrastructure and its environment. The failure of stakeholders and senior policy makers to anticipate and mitigate the consequences of these trends is likely to result in disruption of U.S. critical infrastructure. OCIA assesses that these trends, if left ignored, will weaken and degrade U.S. critical infrastructure during the next decade and likely lead to national security consequences.

(U) KEY FINDINGS

(U) The U.S. Department of Homeland Security/Office of Cyber and Infrastructure Analysis (DHS/OCIA) assesses that information and communication technology (ICT) is highly likely to continue being extensively incorporated into critical infrastructure during the next decade. As a result, the variety of cyber-physical system components (operating systems, computational hardware, and firmware) in ICT is likely to make universal security across critical infrastructure sectors problematic creating immeasurable vulnerabilities and attack vectors. Critical infrastructure is likely to see an increase in cyber-related incidents during the next decade.

(U) DHS/OCIA assesses that nefarious use of Non-Traditional Aviation Technology (NTAT) will increase during the next decade because of commercial availability, low cost, and easy operation. NTAT increases the capabilities of a malicious actor to exploit previously mitigated terrestrial attack vectors (e.g., walls, barriers, and checkpoints).

(U) DHS/OCIA assesses that terrorist organizations will continue to use the internal and social media platforms in evolving and dangerous ways. The recruitment and radicalization of individuals here in the United States will remain a priority for terrorist organizations, as will their targeting of critical infrastructure. Further, cyberterrorist capabilities are almost certain to become more sophisticated in the next 10 years; consequently, incidents of cyberterrorism are likely to increase during the next decade.

(U) DHS/OCIA assesses that a significant number of U.S. infrastructure assets are approaching the end of their designed life spans. Budget cuts across federal, state, and local governments limit the funding available for infrastructure inspections, maintenance, upgrades, and repairs. In some critical infrastructure sectors, a labor force shortage in the coming decades is likely to hamper efforts aimed at implementing and maintaining critical infrastructure upgrades. The risk of failure in the Transportation Systems, Energy, Water and Wastewater Systems, and Dams Sectors is highly likely to increase during the next 10 years.

(U) DHS/OCIA assesses that a possible increase in the frequency and severity of extreme weather events is likely to result in damage to critical infrastructure and could result in population shifts. Regions unaccustomed to extreme weather will become more susceptible and vulnerable to storm surges in the coming decades.

(U) DHS/OCIA assesses that the Healthcare and Public Health, Emergency Services, Transportation Systems, Water and Wastewater Systems, and Energy (Electrical Power) Sectors are most likely to be affected by a pandemic. All other critical infrastructure sectors are likely to be affected to some degree by the unavailability of personnel needed to maintain operations. The economic impact of a pandemic will depend on its severity and duration and mitigation efforts by federal, state, and local governments and the public. Estimates of loss in gross domestic product during the first year of a pandemic range from less than 1 percent in a mild pandemic up to 4.25 percent during a severe pandemic.

(U) SCOPE

(U) This assessment is based on the analysis of six emerging trends and their potential consequences on U.S. critical infrastructure. The goal of this strategic risk assessment is to inform private and public stakeholders and senior policy makers about these current and future trends so they anticipate and adopt measures to mitigate the effect and consequences of them on critical infrastructure. The trends identified are not intended to be an exhaustive list; however, OCIA assesses that these trends will likely have the most profound impact on U.S. critical infrastructure by 2025.

(U) The research conducted for this assessment began in early May 2015 and concluded in February 2016. The trends discussed in this assessment were based on a comprehensive review of DHS and OCIA products, government documents, academic peer-reviewed journals, and case studies highlighting the major trends perceived to affect critical infrastructure during the next decade. This product was reviewed by the DHS/Office of Intelligence and Analysis and Office of Infrastructure Protection, the U.S. Department of Energy, and the U.S. Department of Health and Human Services.

(U) DHS/OCIA hopes this assessment inspires a deeper analytical discussion of these trends and their direct influence on critical infrastructure by sector operators and owners, their sector-specific agency counterparts, and senior policy makers.

CONTENTS

FIGURES

TABLES

(U) GROWING CONVERGENCE OF CYBER AND PHYSICAL DOMAINS

(U) U.S. critical infrastructure relies on and is likely to increasingly depend on information and communication technology (ICT) in the next decade. ICT is present, in various extents, in all 16 critical infrastructure sectors. Although this dependency creates numerous advantages in efficiency, production, and livelihood for Americans, ICT inherent reliance on a network connection for functionality creates numerous vulnerabilities.[1] The U.S. Department of Homeland Security/Office of Cyber and Infrastructure Analysis (DHS/OCIA) assesses that the following key ICT will have a profound effect on U.S. critical infrastructure during the next 10 years: cyber-physical systems (CPS), global positioning system (GPS), "Smart Cities," Internet of Things (IoT), and "cloud" technology.

(U) Cyber-Physical Systems: CPS technology is a bridge for physical objects to communicate with a computer via a network to perform various functions. These functions can range from facilitating manufacturing processes that control the flow of gas through a pipeline to monitoring energy usage. CPS technology allows for critical infrastructure owners and operators to improve processes and production providing vital analytics to reduce unnecessary energy expenditures. Investments in CPS are expected to increase during the next decade as more critical infrastructure sectors seek to incorporate the technology. OCIA assesses that the components involved in CPS devices (operating systems, computational hardware, and firmware) will make universal security extremely difficult and improbable, allowing cyber attackers to more easily exploit critical infrastructure.[2]

(U) Global Positioning System: Cyber-physical systems also include GPS-based technologies, which have almost replaced paper maps in recent years. U.S. critical infrastructure sectors are increasingly at risk from a growing dependency on GPS for positioning, navigation, and timing. Awareness that GPS-supported services and applications are integrated in sector operations is somewhat limited, prompting the idea that GPS is a largely invisible utility. Therefore, dependence on GPS is likely to be significantly underestimated because many of the critical infrastructure sectors depend on the GPS timing function. OCIA assesses that the increasing convergence of critical infrastructure dependency on GPS services with the likelihood that threat actors will exploit their awareness of that dependency presents a growing risk to the United States.[3]

(U) Smart Cities: Smart Cities have been defined as urban centers that integrate CPS technologies and infrastructure to create environmental and economic efficiency.[4] The goals of these new cities are to create a higher quality of life and a more efficient use of available resources. ICT is the fundamental element involved in developing Smart Cities.[5] Smart Cities rely on the effective networking of computer systems and physical devices, CPS, and the IoT.[6] Examples of Smart Cities technologies are interconnected power grids reducing power waste, smarter transportation resulting in improved traffic management, and smarter infrastructure reducing hazards and increasing efficiency.[7] However, pitfalls exist in the emerging trend of Smart Cities.

(U) According to a report issued by the Brookings Metropolitan Policy Program and Barcelona's ESADE Business School, the majority of cities are not in a position to purchase and integrate smart technologies.[8] Cities will need to develop long-term economic goals that identify critical infrastructure's future growth potential.[9] A comprehensive economic vision is needed for cities to understand what policies to adopt and what products to demand.[10] Securing the necessary capital needed to integrate Smart Technology into cities is a key issue. According to one report, the U.S. Smart Cities market will be worth an estimated $392.41 billion by 2019.[11] The global market for Smart Cities is expected to be $1.2 trillion by 2019.[12] The Brookings and ESADE report indicates that the impetus will be on cities, and less on the

[1] (U) National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf, accessed 26 May 2015.

[2] (U) Peisert, Sean, "Designed-in Security for Cyber-Physical Systems," http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6924670 , accessed 26 May 2015.

[3] (U) U.S. Department of Homeland Security (DHS), OCIA, National Risk Estimate: Risks to U.S. Critical Infrastructure From Global Positioning System Disruption,Washington , D.C.,, November 2012, p. 3

[4] (U) In addition, a smart city "gathers data from smart devices and sensors embedded in its roadways, power grids, buildings, and other assets. It shares that data via a smart communications system that is typically a combination of wired and wireless. It then uses smart software to create valuable information and digitally enhanced services." (Smart Cities Council "Vision," http://smartcitiescouncil.com/category-vision, accessed 4 February 2015).

[5] (U) Chouradi, Hafedh, et al., "Understanding Smart Cities: An Integrative Framework," https://www.ctg.albany.edu/publications/journals/hicss_2012_smartcities/hicss_2012_smartcities.pdf, , accessed 20 May 2015

[6] (U) National Institute of Standards and Technology, *Global City Teams Challenge Kick-Off*, http://www.nist.gov/cps/global-city-teams-challenge-workshop.cfm, accessed 1 December 2014.

[7] (U) U.S. Department of Homeland Security (DHS), OCIA, The Future of Smart Cities: Cyber-Physical Infrastructure Risk,Washington, D.C., August 2015, p. 2, .

[8] (U) Brookings Institute, "Cities Need to Develop Plans to be Smart About Implementing Smart Technologies," http://www.brookings.edu/~/media/research/files/papers/2014/04/smart-cities/smart-cities-press-release_-final.pdf , accessed 5 June 2015.

[9] (U) Ibid.

[10] (U) Brookings Institute, "Getting Smarter About Smart Cities," http://www.brookings.edu/research/papers/2014/04/23-smart-cities-puentes-tomer, accessed 5 June 2015.

[11] (U) Schwartz, Heidi, "Global Market for Smart Cities to Reach 1,265.85 Billion by 2019," http://businessfacilities.com/2014/07/global-market-for-smart-cities-to-reach-1265-85-billion-by-2019/, accessed 30 June 2015.

[12] (U) Ibid.

Federal Government, to pay for Smart Technology.[13] During the next decade, local and state governments will need to acquire the means to pay for and maintain Smart Technologies. Failure to build private and public partnerships could stall Smart Cities initiatives.

(U) In addition to urban and economic planning, local governments will need to develop the ICT infrastructure necessary to support and sustain a Smart City. Furthermore, Smart Technology will create not only Smart Cities, but also whole networks of Smart Cities with shared dependencies on utilities, energy resources, and medical services. Such networks are likely to require collaboration and partnerships across county and state lines. More important, local governments will need to create an environment conducive to industrial development for their Smart Cities to mature.[14]

(U) Many U.S. cities are experiencing substantial population growth, and state and local governments are struggling to keep up with congestion, pollution, and the increased demands being placed on aging and failing infrastructure. Municipal governments are increasingly looking to address these concerns by networking various infrastructure Smart technologies, which can support increased automation and responsiveness.[15] The growth of Smart Cities will also influence a new brand of governing, referred to as "smart governance."

(U) Smart governance is a compilation of technologies, people, policies, practices, resources, social norms, and information fused to support city governing activities.[16] This type of governance depends on citizen, private, and public partnerships at every level.[17] Policy and decision makers' inability to foster smart governance could hinder local communities and states from properly developing Smart Cities. Further, a lack of smart governance could have severe economic and security consequences for communities and states. OCIA assesses that gaps in policies and regulations could result in inefficient security protocols, leaving regional critical infrastructure vulnerable to exploitation through cyber attacks.

(U) Internet of Things: IoT uses CPS technology as a bridge to connect with higher level services. The IoT allows for various devices, such as domestic appliances, automobiles, and production lines, to be controlled and managed remotely and automatically.[18] OCIA assesses that IoT will influence and affect multiple critical infrastructure Sectors, ranging from Healthcare and Public Health, Information Technology, Critical Manufacturing, and Transportation Systems during the next decade.[19] Further, IoT will continue to be a key tool in the development of Smart Cities.[20]

(U) The National Security Telecommunications Advisory Committee states that water, power, emergency services, health care, and transportation systems increasingly depend on IoT devices.[21] The Smart America project, a White House Presidential Innovation Fellow project, analyzed the effect of emerging IoT technologies and on cities and economic sectors (e.g., transportation and energy). Although the project highlighted the potential benefits of IoT, it identified two points for consideration:

- (U) The engineering and design culture of the IoT places functionality and speed to market as priorities above security concerns.
- (U) No accepted repository, clearing house, or organization exists to capture lessons learned.[22]

(U) The widespread use and prevalence of IoT devices does not appear to be slowing down. The pace of adoption and scale of deployment of IoT devices are unprecedented; estimates are that in 5 years, 26–50 billion IoT devices will exist.[23] The advantages of this technology come with inherent vulnerabilities. Billions of interconnected IoT devices creating, transmitting, and storing data will result in "data exhaust," which allows threat actors to gain significant insights into sensitive information such as telemetry, voice, video, health, and infrastructure component status data.[24] In January 2014, the Director of National Intelligence stated, "…threat actors can easily cause security and safety problems in these systems."[25] The IoT reliance on a network connection for proper functionality will remain a vulnerability that malicious actors are likely to exploit for the foreseeable future.[26,27]

[13] (U) Brookings Institute, "Getting Smarter About Smart Cities," http://www.brookings.edu/research/papers/2014/04/23-smart-cities-puentes-tomer, accessed 5 June 2015.

[14] (U) Chouradi, Hafedh, et al., "Understanding Smart Cities: An Integrative Framework," https://www.ctg.albany.edu/publications/journals/hicss_2012_smartcities/hicss_2012_smartcities.pdf, accessed 20 May 2015.

[15] (U) U.S. Department of Homeland Security (DHS), OCIA, The Future of Smart Cities: Cyber-Physical Infrastructure Risk,Washington, D.C., , August 2015, p. 7.

[16] (U) Chouradi, Hafedh, et al., "Understanding Smart Cities: An Integrative Framework," https://www.ctg.albany.edu/publications/journals/hicss_2012_smartcities/hicss_2012_smartcities.pdf

[17] (U) Ibid., 2292.

[18] (U) Wylie, Ian, "Danger in the Digital Age: the Internet of Vulnerable Things," http://www.ft.com/cms/s/0/fc2570f0-cef4-11e4-b761-00144feab7de.html#axzz42Pce4dRu, accessed 17 June 2015.

[19] (U) IDC Press Release, "New IDC Forecast Asserts Worldwide Internet of Things Market to Grow 19% in 2015, Led by Digital Signage", https://www.idc.com/getdoc.jsp?containerId=prUS25633215, accessed 30 June 2015.

[20] (U) National Security Telecommunications Advisory Committee, NSTAC Report to the President on the Internet of Things, Washington, D.C., , July 2015, p. 6, https://www.dhs.gov/sites/default/files/publications/IoT%20Final%20Draft%20Report%2011-2014.pdf, accessed 3 February 2016.

[21] (U) Ibid., 4.

[22] (U) Ibid., 7.

[23] (U) Ibid., 4.

[24] (U) Ibid., 7.

[25] (U) Ibid., 5.

[26] (U) Wylie, Ian, "Danger in the Digital Age: the Internet of Vulnerable Things," http://www.ft.com/cms/s/0/fc2570f0-cef4-11e4-b761-00144feab7de.html#axzz42Pce4dRu, accessed June 17 2015.

- (U) Hewlett-Packard: In a 2015 study, Hewlett-Packard conducted an experiment on popular IoT devices. Hewlett-Packard found that 70 percent of the devices did not encrypt communications to the Internet and local network, and 60 percent did not use encryption when downloading software updates.[28]
- (U) Chrysler: In July 2015, Chrysler announced a recall of 1.4 million vehicles after security researchers successfully hacked Chrysler's Uconnect dashboard computer system, an IoT device, in a controlled experiment. During the experiment, the researchers gained control of the steering, transmission, and brake capabilities of the targeted vehicle. [29]

(U) OCIA assesses that critical infrastructure IoT device failures could result in economic loss through lost productivity and damage to the national economy. Moreover, critical infrastructure IoT device failure can adversely affect public safety through physical infrastructure damage or catastrophic infrastructure failure.[30]

(U) Cloud Technology: Cloud computing technologies, or virtualized infrastructure, services, and networks, have been increasingly adopted across the critical infrastructure community for the past 15 years.[31] The move to the cloud has produced significant mid-term cost savings for industry, business, and government. In addition, cloud technology provides a distributed capability that proponents say may offer better availability than traditional in IT and hosted services; however, OCIA assesses that cloud technologies also pose significant challenges in providing adequate security. The attack surface of a cloud environment is much larger than a traditional IT infrastructure implementation, and cloud technologies make some specific attack vectors easier to exploit. A weakness of cloud security models is that attacks provide many opportunities for unauthorized access and escalation of privileges.[32]

(U) The cloud brings unique risks to each critical infrastructure sector. The Energy Sector Electricity Subsector cloud-based risks are primarily found in "smart grid" technologies implemented to improve the efficiency and resiliency of the electrical transmission and distribution systems. The main concerns of the Financial Services Sector cloud technology deployment are confidentiality and integrity of data, between the individual and the financial institution.

(U) Within the Transportation Systems Sector, the airline industry relies on cloud systems for scheduling passengers, flights, and cargo. A failure of cloud systems could result in disruptions to air traffic. Disruptions to cloud systems in the cross-country and logistic industries and the maritime shipping and ports industries can result in misrouted commercial and freight transportation and adverse effects to manufacturing supply chains.[33]

(U) Industrial control systems (ICS), such as Supervisory Control and Data Acquisition (SCADA) systems, distributed control systems, and process control systems, used in critical infrastructure pose security risks that differ from those of traditional IT systems. For one, these systems are designed to control physical systems that directly affect physical systems and processes (e.g., energy, water, critical manufacturing). A compromise of such a system could have a direct physical effect on supply chains and human life.[34] Based on a limited number of cross-sector observations, OCIA subject matter experts agree that wherever ICS environments are connected to cloud infrastructure, the cloud will be burdened by the additional security needs of these legacy environments. Cloud providers are generally not prepared or equipped to address many of these specialized needs. As these systems are further integrated into critical infrastructure, OCIA foresees an increase in cyber-related incidents.

(U) OCIA assesses that the potential consequences of cloud technology integration are hard to determine; however, a compromise of critical infrastructure SCADA systems that are connected to cloud infrastructure could have a direct physical effect on human life.[35]

(U) Cyberespionage and Cyber Disruption: The threat to critical infrastructure is highly likely to continue to grow as nation-states, cybercriminals, and non-state actors enhance their technical capabilities.[36] A large portion of our critical infrastructure operates on networks connected to the Internet, creating numerous vulnerabilities that if exploited could have devastating consequences. During the next decade, the number and level of critical infrastructure connected to ICT and computer networks are expected to increase. Projections indicate that approximately 50 billion

[27] (U) Norton, Steven, "Internet of Things Market to Reach 1.7 trillion by 2020: IDC," http://www.marketwatch.com/story/internet-of-things-market-to-reach-17-trillion-by-2020-idc-2015-06-02-8103241, accessed June 30 2015.

[28] (U) Hewlett-Packard Enterprise, "Internet of things research study," http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf, accessed 16 December 2015.

[29] (U) Greenberg, Andy, "After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix," http://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/, accessed 11 August 2015.

[30] (U) National Security Telecommunications Advisory Committee, NSTAC Report to the President on the Internet of Things, Washington, D.C.,, p. 7, https://www.dhs.gov/sites/default/files/publications/IoT%20Final%20Draft%20Report%2011-2014.pdf, accessed 29 July 2015.

[31] (U) U.S. Department of Homeland Security (DHS), OCIA, Potential Risks of Cloud Technology Adoption, Washington, D.C. October 2015, p. iii,.

[32] (U) Ibid., iii.

[33] (U) Ibid., iii.

[34] (U) Ibid., 18.

[35] (U) U.S. Department of Homeland Security (DHS), OCIA, Potential Risks of Cloud Technology Adoption, Washington, D.C., October 2015, p. 18,.

[36] (U) U.S. Department of Homeland Security, "The Homeland Security Environment 2014–2019," Washington, D.C., 2014.

Internet-connected devices are likely to exist by 2020.[37] The Sectors likely to be most affected by cybersecurity are Financial Services, Energy, Transportation Systems, Information Technology, Communications, Defense Industrial Base, and Healthcare and Public Health.[38, 39] Nation-states are likely to continue targeting these Sectors to improve their own political and economic advantage through the theft of trade secrets and sensitive data.[40] In 2014, former U.S. Cyber Command General Keith Alexander estimated an economic loss of $300 billion per year because of the theft of intellectual property and trade secrets.[41] A rise in cyberespionage will degrade U.S. competitive advantage at home and abroad, resulting in job and economic losses.

- (U) China: On May 19, 2014, the U.S. Department of Justice charged five Chinese military officials with cyberespionage against six American companies in nuclear power, metals, and solar product industries. The charges allege that the individuals stole trade secrets beneficial to Chinese companies.[42]
- (U) Aetna: On February 4, 2015, health insurance company Anthem stated that a database containing approximately 80 million patient records was breached during a cyber attack. According to a former White House and Defense Department cybersecurity official, the information stolen was primarily used for cyberespionage, rather than cybercriminal purposes.[43]
- (U) Office of Personnel Management (OPM): On April 4, 2015, OPM notified current and former federal employees of a "cybersecurity incident" affecting approximately 21.5 million individuals.[44] According to OPM, the stolen data included personally identifiable information (PII). Hacking tools and techniques used in the OPM breach were similar to the ones used in the Anthem incident, indicating that the motive of the attackers may have been acquiring information for espionage rather than criminal purposes.[45]

(U) The United States depends highly on computer network-based technology. In FY 2014, the Industrial Control Systems-Cyber Emergency Response Team (ICS–CERT) reported 245 cyber-related incidents. As can be seen in the Table, nearly one-third of those incidents targeted the Energy Sector.[46] In comparison, ICS–CERT reported 197 incidents in 2012 and 257 incidents in 2013.[47] According to ICS–CERT, the scope of incidents encompassed a vast range of threats and observed methods for attempting to gain access to both business and control systems infrastructure, including the following: Unauthorized access and exploitation of Internet facing ICS and SCADA devices, exploitation of zero-day vulnerabilities in control system devices and software, malware infections within air-gapped control system networks, Structured Query Language injection and application vulnerability exploitation, network scanning and probing, lateral movement between network zones, targeted spear-phishing campaigns, and strategic Website compromises (a.k.a. watering hole attacks). Note that no incident resulted in any significant outages or damage.

(U) Based on this information, OCIA assesses that the number of cyber-related incidents targeting critical infrastructure will likely increase during the next decade.

[37] (U) National Security Telecommunications Advisory Committee, NSTAC Report to the President on the Internet of Things, Washington, D.C.,, p.1, https://www.dhs.gov/sites/default/files/publications/IoT%20Final%20Draft%20Report%2011-2014.pdf, accessed 29 July 2015.

[38] (U) Castelli, Christopher, "Official: Greatest cyber risks to national security involve handful of sectors," http://www.fortgordonalliance.com/LatestNews/item203, accessed 25 June 2015.

[39] (U) Staff, "Managing cyber risks in an interconnected world-key findings from The Global State of Information Security Survey 2015," https://www.pwc.lu/en/information-risk-management/docs/pwc-irm-managing-cyber-risks-in-an-interconnected-world.pdf, accessed 28 August 2015.

[40] (U) Ibid.

[41] (U) Carin, Matthew, "Cyber Espionage and the Digital Redistribution of Wealth," http://warontherocks.com/2014/10/cyber-espionage-and-the-digital-redistribution-of-wealth/, accessed 31 August 2015.

[42] (U) U.S. Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor, accessed 28 August 2015.

[43] (U) Miller, Jason, "Cyberattack against OPM was 1 of 9 DHS recently discovered targeting 'bulk PII'," http://federalnewsradio.com/technology/2015/06/cyber-attack-against-opm-was-1-of-9-dhs-recently-discovered-targeting-bulk-pii/, accessed 1 July 2015.

[44] (U) Zengerle, Patricia, "Millions more Americans hit by government personnel data hack," http://www.reuters.com/article/us-cybersecurity-usa-idUSKCN0PJ2M420150709, accessed 2 October 2015.

[45] (U) Miller, Jason, "Cyberattack against OPM was 1 of 9 DHS recently discovered targeting 'bulk PII'," http://federalnewsradio.com/technology/2015/06/cyber-attack-against-opm-was-1-of-9-dhs-recently-discovered-targeting-bulk-pii/, accessed 1 July 2015.

[46] (U) ICS–CERT, Year in Review FY 2014, Washington, D.C, 2014 p. 6.

[47] (U) Ibid., 6.

(U) TABLE 1—FY 2014 CYBER INCIDENTS REPORTED BY SECTOR (245 TOTAL)[48]

Sector	Number of Incidents (total percent)
Critical Manufacturing	65 (27%)
Communications	14 (6%)
Commercial Facilities	7 (3%)
Chemical	4 (2%)
Unknown	6 (2%)
Water and Wastewater Systems	14 (6%)
Transportation Systems	12 (5%)
Nuclear Reactors, Materials, and Waste	6 (2%)
Information Technology	5 (2%)
Healthcare and Public Health	15 (6%)
Government Facilities	13 (5%)
Financial Services	3 (1%)
Food and Agriculture	2 (1%)
Energy	79 (32%)

- (U) BlackEnergy: Since 2011, a sophisticated cyber campaign involving BlackEnergy malware has compromised numerous industrial control system environments. Users of Internet-connected human machine interface products, including General Electric Cimplicity, Advantech/Broadwin WebAccess and Siemens WinCC—have been targeted.[49]
- (U) Havex: Malware known as the Havex Trojan contains ICS-specific capabilities, including a payload that finds and gathers information about control system resources within a network by using the Open Platform Communications (OPC) standard. Havex uses multiple vectors for infection, including phishing emails, redirects to compromised web sites and trojanized update installers on ICS vendor web sites.[50]
- (U) Ukraine Power Outage: On December 23, 2015, Ukrainian power companies experienced unscheduled power outages impacting a large number of customers in Ukraine. A U.S. government interagency team deployed to the Ukraine indicated that the outages were caused by external cyber-attackers through remote cyber intrusions at three regional electric power distribution companies. The event impacted approximately 225,000 customers.[51]

(U) According to the Director of National Intelligence, James R. Clapper, U.S. adversaries are also likely to engage in cyber operations focused on data manipulation in the near future.[52] Manipulated data has the potential to affect trades in the stock market, trade secrets, and PII. The use of digital information, more than that of paper hardcopies, is pervasive in the United States. The manipulation of this data will likely erode trust in public and private institutions by U.S. citizens. Widespread adoption of digital information is likely to leave U.S. critical infrastructure vulnerable to data manipulation for the foreseeable future.

(U) AERIAL THREATS: NON-TRADITIONAL AVIATION TECHNOLOGY (NTAT)

(U//FOUO) NTAT are low altitude and slow speed aerial vehicles, including small Unmanned Aircraft Systems (sUAS), ultralights, or gyrocopters that are hard to detect because of their small size, low radar cross section, speed, and operational altitude. They are also adequate in power and size to be weaponized and do not require a license to operate. NTAT present a significant challenge to the security and resilience of critical infrastructure by providing adversaries with the ability to exploit vulnerabilities that do not exist for other threat vectors. Further, this technology can be used to defeat existing protective measures at a number of infrastructure asset classes.

(U) Because of their difficulty in detection, they are capable of circumventing protective measures used to detect more traditional aircraft. Because they are airborne, they can circumvent protective measures designed to prevent ground-based attacks on critical infrastructure. In addition, NTAT provide sufficient range for an adversary to launch an attack from a remote location yet remain in control of the aircraft.

(U) Recent incidents involving NTAT operating in the National Capital Region (NCR) airspace highlights the need for increased awareness and additional research to successfully manage the changing threat landscape as a result of NTAT. For example, in January 2015, a drone crash landed on the White House ellipse, and then again in April 2015, a gyrocopter landed on the grounds of the U.S. Capitol building. These particular incidents identified potential limitations in airspace security operations nationally; in

[48] (U) ICS–CERT, Year in Review FY 2014, Washington, D.C, 2014 p. 6.

[49] ICS-CERT, "Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)", https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B, Alert (ICS-CERT-14-281-01E).

[50] ICS-CERT, "ICS Focused Malware (Update A)", https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A, Alert (ICS-ALERT-14-176-02A).

[51] (U) U.S. Department of Homeland Security, "Cyber-Attack Against Ukrainian Critical Infrastructure", https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01, accessed 3 March 2016.

[52] (U) Ackerman, Spencer, "Newest Cyber Threat will be data manipulation, U.S. intelligence chief says," http://www.theguardian.com/technology/2015/sep/10/cyber-threat-data-manipulation-us-intelligence-chief f, accessed 20 October 2015.

addition, they highlighted airspace security gaps specifically within the NCR. Although few of the incidents within the NCR were malicious or exhibited criminal intent, they posed safety and security challenges to emergency responders, security personnel, infrastructure operators, and the general public. They also illustrate potential vulnerabilities that malicious use of NTAT could exploit.

(U) NTAT's commercial availability, low cost, and ease of operation make them an appealing tool for use by individuals for nefarious purposes. NTAT increases the capabilities of a malicious actor to exploit previously mitigated terrestrial attack vectors (e.g., walls, barriers, and checkpoints). As a result, OCIA assesses that the malicious use of NTAT, especially from terrorist organizations, is likely to increase during the next decade.

(U) Publicly available information highlights Federal Law enforcement involvement in disrupting attack plots that included the use of NTAT, for example:

- (U) Between 2006 and 2007, an al-Qaida-trained operative, Christopher Paul, was arrested by the FBI during the planning phase of a plot to use a remotely controlled helicopter for terrorism purposes.[53]
- (U) In September 2011, the FBI stopped a plot by Rezwan Ferdaus to deploy explosive-laden remotely controlled NTAT against the U.S. Capitol and Pentagon.[54]

(U) International terrorist plots leveraging NTAT date back at least to 1994 when Aum Shinrikyo experimented with the use of remote controlled helicopters for delivery of sarin before their attacks on the Tokyo subway system. [55] More recently, terrorist organizations supported by state sponsors have used military grade UAS for surveillance and kinetic attacks.[56] In one example, the Israeli Air Force interdicted three Iranian-built Ababil drones carrying 40–50 kg warheads.[57] The Islamic State of Iraq and the Levant (ISIL) and other groups have used commercially available sUAS for reconnaissance and since August and September 2015 for ground attacks.[58]

(U//FOUO) A "swarm" scenario in which multiple NTAT systems are simultaneously used in an attack may be of particular concern as these scenarios increases the likelihood of an attack's success and can increase the consequences of an attack. A 2015 report published by the U.S. Army War College Strategic Institute claimed that "UAS swarm" threat scenarios involving non-state actors are years, if not decades, away from becoming realistic terrorist capability. However, simple swarming approaches are already technically feasible with commercially available systems (e.g., one operator directing up to four UAS via one control interface).[59]

(U) The use of NTAT for recreation and commerce is likely to continue to grow within an evolving regulatory framework. As the number of platforms in the sky increases, the number of accidents is likely to increase causing injuries and property damage—intentional or not. The most significant of these is the possibility of an accidental collision between UAS and commercial, private, or government aircraft. Events of highest potential consequence involve commercial passenger aircraft either landing or taking off, when they are flying at altitudes most likely to contain errant NTAT and are at greatest risk to engine or airframe compromise. Events of greatest likelihood include other aircraft (e.g., government, private, and civil aircraft) that routinely fly at low altitudes where encounters with NTAT are most likely to occur.

(U//FOUO) Note as of the end of 2015, no attempt to purposely collide an NTAT with a manned aircraft has been reported domestically. Worldwide, several incidents have occurred in recent years involving the accidental collision of UAS and manned aircraft. None resulted in fatalities or involved the jet engine ingestion of an NTAT. OCIA assesses that the rate of accidental collisions can be expected to increase as the number of UAS platforms in use increases.

(U) The capabilities of NTAT technologies are likely to increase in the near term because of commercial demand and interest from the general public. As NTAT become more prevalent, the price is likely to decrease, increasing accessibility of systems. Projections from early 2015 suggest substantial growth in the commercial NTAT industry during 2015–2025. The primary driver for this growth will be for commercial applications in media, agriculture, energy, minerals exploration, construction, and disaster response.[60,61,62]

[53] (U) U.S. Department of Justice, "Ohio Man Indicated and Arrested for Conspiring to Provide Material Support to Terrorists," https://www.justice.gov/archive/opa/pr/2007/April/07_nsd_240.html, accessed 9 March 2016 November 2015.

[54] (U) U.S Department of Justice, "Ashland Man Agrees to Plead Guilty to Plotting Attack on Pentagon and U.S. Capitol and Attempting to Provide Materiel Support to Terrorists," http://www.justice.gov/archive/usao/ma/news/2012/July/FerdausRezwanPlea.html, accessed 19 October 2015.

[55] (U) Eric A Croddy, et al., Weapons of Mass Destruction: An Encyclopedia of Worldwide Policy, Technology and History, Santa Barbara, CA, ABC Clio, 2005, p. 32.

[56] (U) Robert J. Bunker, "Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Implications" , Carlisle Barracks, PA U.S. Army War College Press,August 2015: p.x.

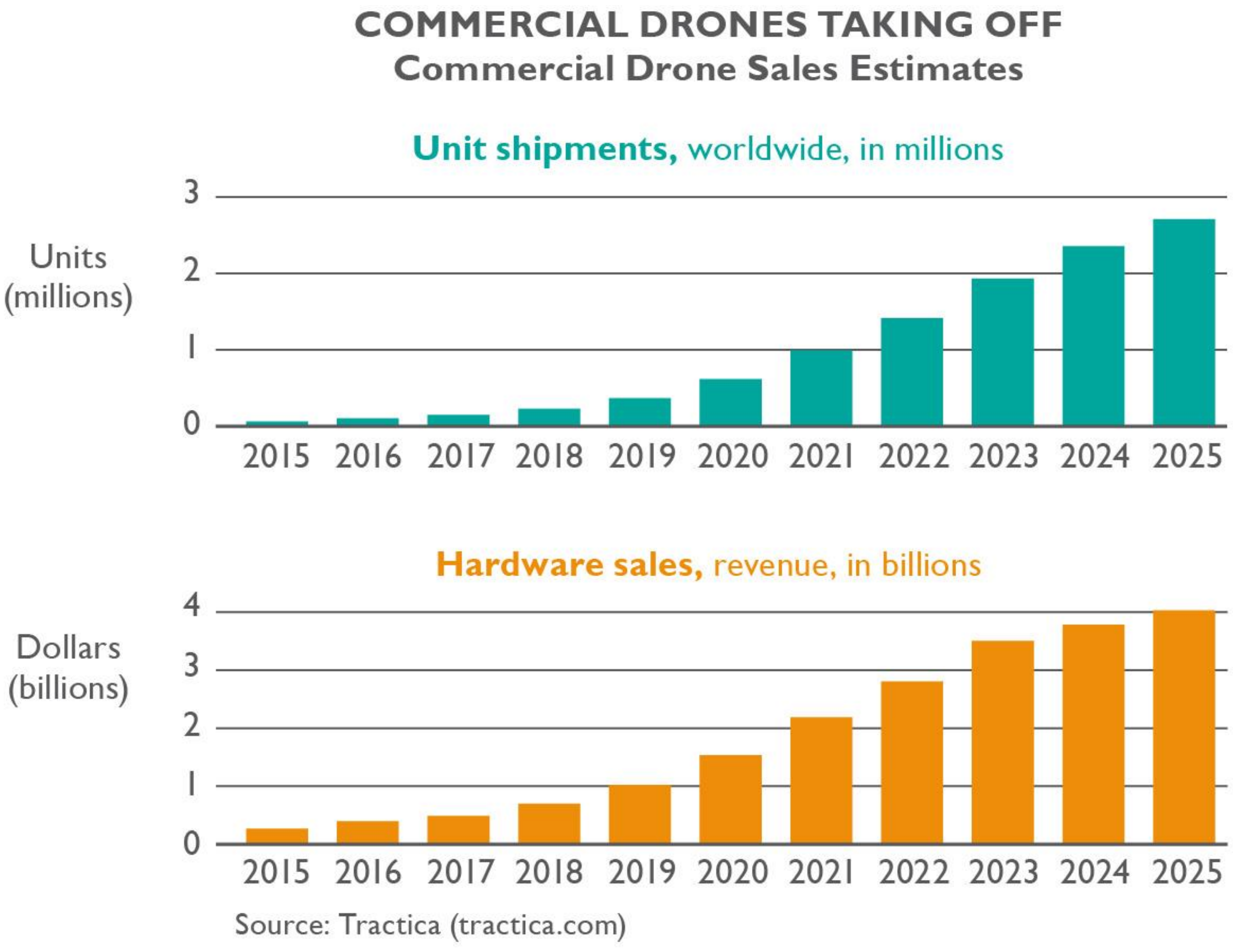
[57] (U) Defense Update, "Israel Intercept Two Attack UAV Launched by Hezbollah", http://defense-update.com/2006/08/israel-intercept-two-attack-uav.html, accessed 14 August 2006.

[58] (U) CNN News, "Now ISIS has drones"?, http://www.cnn.com/2014/08/24/opinion/Bergen-schneider-drones-isis/, accessed 9 March 2016.

[59] (U) Bunker, R.J., "Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Implications," Carlisle Barracks, PA, U.S. Army War Press, 2015:p.x,.

[60] (U) Business Insider (2015), "The Drones Report; Market forecasts, regulatory barriers, top vendors, and leading commercial applications," http://www.businessinsider.com/uav-or-commercial-drone-market-forecast-2015-2, accessed 16 December 2015.

(U) In addition to commercial applications, NTAT are growing in popularity among aviation hobbyists who have propelled sales of commercial-off-the-shelf platforms past traditional radio-controlled model aircraft.[63] The Federal Aviation Administration has estimated that U.S. sales of recreational NTAT systems will be approximately 1.6 million in 2015, and that another 600,000 will be sold for commercial purposes in 2016. Figure 1 shows the expected worldwide growth in units and sales for commercial UAS.[64]



Source: Tractica (tractica.com)

(U) FIGURE 1—COMMERCIAL DRONE SALES PROJECTIONS

[61] (U) Investor's Business Daily (2015)m "Commercial Drone Sales Set to Soar", http://news.investors.com/technology/072215-762954-drone-sales-forecast-2015-to-2025-from-tractica.html.

[62] (U) MarketWatch (2015), "Small Unmanned Aerial Vehicle (UAV) Market Forecast 2015–2025," http://www.marketwatch.com/story/small-unmanned -aerial-vehicle-uav-market-forecast-2015-2025-2015-05-13-9203241), accessed 16 December 2015.

[63] (U) Forbes, "Drone Sales Soar Past $16 Million on Ebay," http://www.forbes.com/sites/frankbi/2015/01/28/drone-sales-soar-past-16-million-on-ebay, 2015, accessed 16 December 2015.

[64] (U) Tractica, "Drones for Commercial Applications in Investor's Business Daily", http://news.investors.com/technology/072215-762954-drones-sales-forecast-2015-to-2025-from-tractica.htm, 2015, accessed 16 December 2015.

(U//FOUO) Market demand will continue to drive innovation in NTAT and result in wide retail access to easier-to-use, highly capable, highly automated systems. Commercially available NTAT already allow for beyond-line-of-sight operations, and the most advanced systems are equipped with geo-fencing capabilities and waypoint navigation. Moreover, innovation among operators, emerging technologies for producing custom parts, and the flexibility of commercial systems for carrying payloads suggest an infinite number of potential applications, whether useful or nefarious.

(U//FOUO) The added dimension of NTAT technology as a delivery platform necessitates a reevaluation of physical and operational vulnerabilities to determine whether the risk profile for critical infrastructure changes. With ever-increasing technical capabilities and ever-widening availability, one can expect the likelihood for malicious use of NTAT to steadily increase over time. OCIA assesses that adversaries are likely to continue employing legitimate, commercially available, NTAT—in particular sUAS—to advance terrorist and criminal activities.

(U) EVOLVING TERRORIST THREAT

(U) Terrorist organizations are increasingly expanding their use of Internet communication methods, such as social media platforms and email, to extend their reach and influence all over the globe. Social media, in particular, is a pivotal component in not only the recruitment of individuals and the dissemination of propaganda, but also a path for individuals to self-radicalize and potentially commit acts of terror.[65] In addition, terrorist organizations have expressed interest in conducting cyber warfare to inflict damage on critical infrastructure. OCIA assesses that terrorist organizations and individual homegrown violent extremists (HVEs) are likely to increasingly use the cyber domain in evolving and dangerous ways during the next decade.

(U) Radicalizing material is easily accessible over the Internet. The Internet is increasingly used by terrorist entities to emphasize and illustrate their ideological message.[66] Terrorist organizations such as Al-Qaeda in the Arabian Peninsula (AQAP) and ISIL continually use online Websites and social media platforms for recruitment, dissemination of propaganda, and in the case of AQAP, training material.[67,68]

- (U) ISIL Online Magazine: ISIL produces an English-language online magazine called “Dabiq.” The magazine includes photo reports, current events, and articles related to the Islamic State.[69]
- (U) Inspire: In 2010, AQAP introduced its English online magazine “Inspire.” The purpose of Inspire magazine is to reach out to Western sympathizers and recruits. Further, previous editions of the magazine explained how to support the organization, provided instructions on building homemade bombs, and called for individual attacks in the United States.[70]

(U) Social media platforms such as Facebook, Twitter, and YouTube benefit terrorist organizations and HVEs. These platforms create an “echo chamber” where extremist discourse and propaganda is continually shared and reposted across multiple platforms and mediums (e.g., video, photo, and text).[71] This information can be pushed to individuals where they can, in turn, pass the information on to other individuals by simply sharing. In addition, the Internet enables individuals with like-minded views to network and integrate into formal entities or organizations.[72] The FBI estimates that thousands of Americans are exposed to and consume ISIL propaganda online, creating an echo chamber, where active supporters and passive sympathizers reshare and post radical material on the Internet and various social media platforms.[73] The National Counterterrorism Center states that the Internet and social media platforms will continue to be used for extremist propaganda and discourse, enabling the radicalization process and helping mobilize individuals.[74]

[65] (U) Vidino, Lorenzo, and Seamus Hughes, “ISIS in America – From Retweets to Raqqa,” https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/ISIS%20in%20America%20-%20Full%20Report.pdf, accessed 12 February 2016.

[66] (U) Tim Stevens and Peter R. Neumann, “Countering Online Radicalisation: A Strategy for Action,” https://cst.org.uk/docs/countering_online_radicalisation1.pdf. accessed 12 February 2016

[67] (U) Purdy, Walter, Radicalization: Social Media and the Rise of Terrorism, Testimony presented before the House Committee on Oversight and Government Reform’s Subcommittee on National Security, https://oversight.house.gov/wp-content/uploads/2015/10/10-28-2015-Natl-Security-Subcommittee-Hearing-on-Radicalization-Purdy-TRC-Testimony.pdf, accessed 15 February 2016.

[68] (U) Counter Extremism Project, “Al-Qaeda in the Arabian Peninsula (AQAP),” http://www.counterextremism.com/threat/al-qaeda-arabian-peninsula-aqap, accessed 14 February 2016.

[69] (U) Clarion Project, “The Islamic State’s (ISIS, ISIL) Magazine”,: http://www.clarionproject.org/news/islamic-state-isis-isil-propaganda-magazine-dabiq, Clarion Project,; accessed 15 December 2015.

[70] (U) Counter Extremism Project, “Al-Qaeda in the Arabian Peninsula (AQAP),” http://www.counterextremism.com/threat/al-qaeda-arabian-peninsula-aqap, accessed 15 February 2016.

[71] (U) Vidino, Lorenzo, and Seamus Hughes, “ISIS in America – From Retweets to Raqqa,” https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/ISIS%20in%20America%20-%20Full%20Report.pdf, accessed 12 February 2016.

[72] (U) Tim Stevens and Peter R. Neumann, “Countering Online Radicalisation: A Strategy for Action,” https://cst.org.uk/docs/countering_online_radicalisation1.pdf, accessed 12 February 2016.

[73] (U) Pierre Thomas, Mike Levine, Jack Date and Jack Cloherty, “ISIS: Potentially ‘Thousands’ of Online Followers Inside US Homeland, FBI Chief Warns,” http://abcnews.go.com/International/thousands-online-isis-followers-inside-us-homeland-fbi/story?id=30882077, accessed February 2016.

[74] (U) Vidino, Lorenzo, and Seamus Hughes, “ISIS in America – From Retweets to Raqqa,” https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/ISIS%20in%20America%20-%20Full%20Report.pdf, accessed 12 February 2016.

- (U) San Bernardino: In December 2015, husband and wife Tashfeen Malik and Syed Rizwan Farook shot and killed 14 people in San Bernardino, CA. FBI Director James B. Comey indicated that the individuals were "consuming poison on the Internet" and became radicalized over a time.[75]

(U) Further, social media allows for varying levels of participation. Individuals can choose to actively create new content, passively repost recycled material, or promote newly created accounts of once suspended users. Active participation creates interactions among like-minded individuals. The result of these interactions may gradually push individuals toward self-radicalization, during which their level of participation begins to change.[76] Eventually, some of these "keyboard warriors" are likely to transition to taking physical action, evolving into HVEs.[77] DHS defines an HVE as a person of any citizenship who has lived or operated primarily in the United States or its territories who advocates, is engaged in, or is preparing to engage in ideologically motivated terrorist activities, including providing material support to terrorism, in furtherance of political or social objectives promoted by a terrorist organization, but who is acting independently of direction by a terrorist organization.

- (U) Congressional Research Service (CRS): According to CRS, approximately 63 HVE plots or attacks have occurred in the United States since September 11, 2001.[78,79]
- (U) Georgetown National Security Critical Issue Task Force Report: Of the 198 lone wolf attacks conducted between 1968 and 2010 in the United States and 14 western countries, 113 occurred in the United States.[80]

(U) The Internet and social media platforms "virtually" remove geographical barriers that once restricted an individual's participation in terrorist activities. An individual does not need to be physically present to attend terrorist training camps or organizational meetings; they can find, relatively easily, information and guidebooks on tactics, techniques, and procedures online.[81] Instant access to these resources narrows the skills gap between terrorist actors overseas and HVEs. Further, terrorist organizations and HVEs can use the Internet to gather intelligence on potential targets, provide training, raise and transfer funds, and communicate operational direction.[82] The result is the expansion of operational capabilities by both terrorist organizations and HVEs. OCIA assesses that terrorist organizations and HVEs are likely to continue executing operations aimed at the recruitment of individuals, dissemination of propaganda and information, and physical attacks on U.S. soil. The result of these operations will likely affect U.S. critical infrastructure to varying degrees.

(U) Terrorist organizations will continue to use the Internet and social media for recruitment, training, and dissemination of extremist propaganda and information for the foreseeable future. To date, cyber terrorists lack the advanced technical skills to launch a large-scale cyber attack; however, individual terrorists and small affiliated hacker groups have successfully carried out cyber attacks against the U.S. Government and the private sector.[83] The majority of these attacks had moderate impacts that resulted primarily in data loss and exposure.[84] For this assessment, OCIA defines cyberterrorism as politically motivated use of ICT with the intent to influence government policies; coerce civilian populations; sabotage infrastructure; effect economic decisions; or otherwise intimidate commercial, public, or government entities.

(U) Cyber attacks conducted by terrorist groups or individuals are becoming a regular and appealing method of advancing extremist ideology as these attacks have a more profound impact psychologically and economically. The activities of some terrorist hackers demonstrate a gradual sophistication of attack modes and intended impacts.[85]

- (U) Junaid Hussain: In January 2015, ISIL hacker Junaid Hussain hacked the Twitter and YouTube accounts for US Central Command. Hussain used the social media platforms to spread ISIL propaganda.[86] In April 2012, British authorities convicted Hussain for illegally accessing and publishing the address book of former British Prime Minister Tony Blair.[87]
- (U) Oxmar: In January 2012, a Saudi hacker, using the moniker "Oxmar," conducted a Distributed

[75] (U) Perez, Eva, Dana Ford,, "FBI: San Bernardino shooters pledged jihad over direct messages", http://www.cnn.com/2015/12/16/us/san-bernardino-shooting/ ," ,accessed February 2016.

[76] (U) Bjelopera, Jerome P., "American Jihadist Terrorism: Combating a Complex Threat," http://www.fas.org/sgp/crs/terror/R41416.pdf, accessed 18 February 2016.

[77] (U) Bjelopera, Jerome P., "American Jihadist Terrorism: Combating a Complex Threat," http://www.fas.org/sgp/crs/terror/R41416.pdf, accessed 18 February 2016.

[78] (U) Ibid.

[79] (U) CRS defines jihadists as radicalized individuals using Islam as an ideological or religious justification for their belief in the establishment of a global caliphate, or jurisdiction governed by a Muslim civil and religious leader known as a caliph.

[80] (U) Alfaro-Gonzalez, Lydia, et al., Report: Lone Wolf Terrorism, Georgetown University Security Studies Program, http://georgetownsecuritystudiesreview.org/wp-content/uploads/2015/08/NCITF-Final-Paper.pdf ,accessed 9 December 2015.

[81] (U) Bjelopera, Jerome P., "American Jihadist Terrorism: Combating a Complex Threat," http://www.fas.org/sgp/crs/terror/R41416.pdf, accessed 18 February 2016.

[82] (U) Bjelopera, Jerome P., "American Jihadist Terrorism: Combating a Complex Threat," http://www.fas.org/sgp/crs/terror/R41416.pdf, accessed 18 February 2016..

[83] (U) Heffelfinger, Christopher, "The Risks Posed by Jihadist Hackers," https://www.ctc.usma.edu/posts/the-risks-posed-by-jihadist-hackers, accessed 12 February 2016.

[84] (U) Ibid.

[85] (U) Ibid.

[86] (U) Ackerman, Spencer, "US Central Command Twitter account hacked to read 'I love you ISIS,'", http://www.theguardian.com/us-news/2015/jan/12/us-central-command-twitter-account-hacked-isis-cyber-attack, accessed 12 February 2016.

[87] (U) Ackerman, Spencer, "Junaid Hussain: British hacker for ISIS believed killed in US air strike,", http://www.theguardian.com/world/2015/aug/27/junaid-hussain-british-hacker-for-isis-believed-killed-in-us-airstrike, accessed 12 February 2016.

Denial of Service (DDoS) attack on the Websites of Israeli national airline El Al, Tel Aviv Stock Exchange, and three Israeli banks.[88]

(U) OCIA assesses that cyberterrorism activities designed to disrupt critical infrastructure cyber-dependent assets will gradually increase by 2025. Cyberterrorists have the greatest chance of successfully disrupting U.S. critical infrastructure either by a Denial of Service or a Distributed Denial of Service Attack, resulting in disruption to operations. These methods of attack are simplistic and do not demonstrate a high level of sophistication. OCIA assesses that although cyberterrorists will not have the capabilities to launch a nationwide cyber attack this coming decade, they do possess the means to execute low to moderate level attacks focused on data loss and exposure for the foreseeable future.[89]

- (U) Syrian Electronic Army Hacks Associated Press Twitter Account: In late April 2013, members of the Syrian Electronic Army hacked into the Twitter account of the Associated Press. Once the individuals gained control of the account, they published bogus messages concerning explosions at the White House and the U.S. President being injured. The bogus claim may have contributed to a temporary $136.5 billion loss for the S&P 500 index, although it later recovered.[90]

(U) Although the capability of attack methods remains low to moderate in terms of sophistication, cyber terrorists have repeatedly called for attacks on critical infrastructure targets.[91] As terrorist organizations, such as ISIL, become more aggressive in their recruitment of technical experience, it is likely that their cyber capabilities will improve.[92] Incidents of cyberterrorism will increase in the next decade as terrorist organizations augment their capabilities with information warfare techniques. Cyberterrorism is an unavoidable threat because the Nation's critical infrastructure sectors increasingly rely on computer networks, leaving them vulnerable to enhanced cyberterrorism techniques.[93]

(U) OCIA assesses that terrorist organizations will increasingly use the cyber domain in more efficient ways in the coming decade. The threat of a terrorist attack on critical infrastructure by HVEs or lone wolf attackers in the United States remains a threat that can result in harsh socioeconomic consequences.[94,95] In addition, terrorist organizations are likely to gradually improve their overall technical capabilities in conducting cyberterrorism operations.

- (U) University of Maryland Global Terrorism Database: According to the University of Maryland's Global Terrorism Database, between January 2001 and April 2013, more than 200 terrorism-related incidents occurred in the United States.[96.97]

(U) FACING THE INEVITABLE: THE STATE OF U.S. INFRASTRUCTURE

(U) Infrastructure failures occur almost daily throughout the United States. Incidents often do not make news nationally, but can have serious local and regional effects. Train derailments, water main breaks, chemical leaks, pipeline ruptures, and power outages are just a few examples of infrastructure failures that can have costly human health, economic, and national security consequences. In the United States, a considerable number of infrastructure assets, particularly those in the Transportation Systems, Dams, Water and Wastewater Systems, and Energy Sectors, are nearing the end of their lifespans and pose a significant risk to public health and safety.[98] The risks posed by and associated with aging and failing infrastructure are likely to increase in the coming decade. In a 2013 report, the American Society of Civil Engineers evaluated 16 critical infrastructure categories and assigned grades to each based on eight criteria: capacity, condition, funding, future need, operation and maintenance, public safety, resilience, and innovation.[99] Ten out of 16 categories were given a D grade and rated "Poor: At Risk."[100,101]

[88] (U) Heffelfinger, Christopher, "The Risks Posed by Jihadist Hackers," https://www.ctc.usma.edu/posts/the-risks-posed-by-jihadist-hackers, accessed 12 February 2016.

[89] (U) Heffelfinger, Christopher, "The Risks Posed by Jihadist Hackers," https://www.ctc.usma.edu/posts/the-risks-posed-by-jihadist-hackers, accessed 12 February 2016.

[90] (U) Foster, Peter, "Bogus AP Tweet about explosion at the White House wipes billions off U.S. markets," http://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html, accessed 21 July 2015.

[91] (U) Heffelfinger, Christopher, "The Risks Posed by Jihadist Hackers," https://www.ctc.usma.edu/posts/the-risks-posed-by-jihadist-hackers, accessed 12 February 2016.

[92] (U) Ibid.

[93] (U) Oliveria, Daniela, "Cyber-Terrorism and Critical Energy Infrastructure Vulnerability to Cyber-Attacks," http://www.law.uh.edu/eelpj/publications/5-2/RD2-Oliveira.pdf, accessed 17 July 2015.

[94] (U) Bjelopera, Jerome P., "American Jihadist Terrorism: Combating a Complex" Threat, Congressional Research Service, http://www.fas.org/sgp/crs/terror/R41416.pdf, accessed 18 February 2016.

[95] (U) Office of the Director of National Intelligence, Worldwide Threat Assessment of the US Intelligence Community http://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf, accessed 6 January 2016.

[96] (U) National Consortium for the Study of Terrorism and Responses to Terrorism (START), (2013), Global Terrorism Database, http://www.start.umd.edu/gtd accessed 31 December 2015.

[97] (U) Vidino, Lorenzo, and Seamus Hughes, "ISIS in America – From Retweets to Raqqa," https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/ISIS%20in%20America%20-%20Full%20Report.pdf, accessed 12 February 2016.

[98] (U) Office of Cyber and Infrastructure Analysis, National Risk Estimate on Aging and Failing Critical Infrastructure Systems, Washington, DC: Department of Homeland Security, December, 2014. p.10

[99] (U) American Society of Civil Engineers, 2013 Report Card for America's Infrastructure, http://www.infrastructurereportcard.org/, accessed 17 June 2015.

[100] (U) Ibid.,

[101] (U) According to the ASCE, infrastructure earning a D is "in poor to fair condition and mostly below standard, with many elements approaching the end of their service

(U) VULNERABILITIES OF PHYSICAL INFRASTRUCTURE ASSETS

(U) OCIA assesses that infrastructure does not fail simply because of advanced age; common failure mechanisms put older infrastructure at increased risk of failure. To better assess likelihood of failure, other indicators must be considered in addition to age.

(U) COMMON CAUSES OF INFRASTRUCTURE FAILURE

(U) Although each type of infrastructure has unique characteristics, all infrastructure assets will continue to be affected by common failure mechanisms including material fatigue, corrosion, erosion, extreme weather and natural disasters, and human error during the next decade.[102] For a more detailed explanation of common causes of infrastructure failure, please see the Appendix.

- (U) Seattle, Washington: The Interstate 5 Bridge over the Skagit River (an hour north of Seattle) was 58 years old on May 23, 2013, when a truck with an excessively large load struck one of its steel girders, causing a 160-foot section of the bridge to collapse into the Skagit River.[103] The Washington State Department of Transportation reported that the cost of repairing and replacing the bridge amounted to nearly $20 million.[104]
- (U) Lake Delhi, Iowa: The Delhi Dam's 2010 failure resulted in an estimated $50 million in damages and $120 million in economic losses.[105] An independent panel of engineers found the probable causes of the dam's failure were design flaws, construction issues, and a faulty floodgate that allowed rising floodwater from days of torrential rain to flow from the dam and into the Maquoketa River 45 feet below.[106] The dam failure drained all the water from Lake Delhi, negatively affecting area homeowners and businesses.[107] Reconstruction of the Lake Delhi Dam did not begin until April 2014. The lake remained empty for years, adversely affecting the surrounding communities.[108]
- (U) Kauai, Hawaii: The Kaloko Dam was 124 years old when it collapsed on March 14, 2006, releasing a 70-foot-high, 200-foot-wide, 1.6-million-ton wave.[109] The dam failure swept away 16 cars, hundreds of trees, and a cluster of homes, drowning all seven of the homes' occupants.[110] Despite Hawaiian law requiring dam inspections every 5 years, Kaloko was never inspected.[111]

(U) INDICATORS OF FAILURE

(U) No single factor indicates an increased likelihood of infrastructure failure; many factors must be considered. Each sector, subsector, and asset type has different indicators, but some general indicators support risk assessments for most infrastructure types. All infrastructure sector vulnerabilities will continue to depend on the following attributes in the next 10 years: age, structural material, asset design, construction techniques, amount of use, and geographic location.[112] For a more detailed explanation of indicators of failure, see the Appendix.

- (U) Brockton, Massachusetts: In May 2015, tens of thousands of citizens in Brockton and other neighboring towns were left without drinking water when a water main ruptured, prompting Brockton officials to declare a state of emergency.[113,114] The water main failure was a result of a break in a 100-year-old pipe in the town of East Bridgewater.[115,116] The water main break closed schools, canceled city events, postponed non-elective surgeries at a city hospital, and forced tens

life. A large portion of the system exhibits significant deterioration. Condition and capacity are of significant concern with strong risk of failure."

[102] (U) U.S. Department of Homeland Security/Office of Cyber and Infrastructure Analysis, National Risk Estimate on Aging and Failing Critical Infrastructure Systems, Washington, D.C., December 2014, p. 11.

[103] (U) Johnson, Kirk, "Washington State Bridge Collapse Could Echo Far Beyond Interstate," http://www.nytimes.com/2013/05/25/us/washington-state-bridge-collapse-highlights-infrastructure-needs.html?_r=0, accessed 3 July 2015.

[104] (U) Washington State Department of Transportation, "I-5 - Skagit River Bridge Replacement - Completed July 2014," http://www.wsdot.wa.gov/projects/i5/skagitriverbridgereplacement/, accessed 3 July 2015.

[105] (U) McGreal, Chris, "Accident Waiting to Happen: the Ohio Village Built on a Crumbling Dam," T http://www.theguardian.com/us-news/2015/aug/03/buckeye-lake-dam-accident-waiting-to-happen, accessed 11 August 2015.

[106] (U) Crumb, Michael, "Report: Flood of Problems Led to Iowa's Lake Delhi Dam Breach," http://www.insurancejournal.com/news/midwest/2010/12/03/115391.htm, accessed 11 August 2015.

[107] (U) Danielson, Dar, "Lake Delhi Getting Closer to a Refill," http://www.radioiowa.com/2015/01/30/lake-delhi-getting-closer-to-a-refill/, accessed 11 August 2015.

[108] (U) HydroWorld, "Reconstruction of Iowa's Delhi Dam Could Begin Soon," http://www.hydroworld.com/articles/2014/02/reconstruction-of-iowa-s-dehli-dam-could-begin-soon.html, accessed 11 August 2015.

[109] (U) Leslie, Jacques, "Before the Flood," http://www.nytimes.com/2007/01/22/opinion/22leslie.2.html, accessed 13 July 2015.

[110] (U) Ibid.

[111] (U) Ibid.

[112] (U) U.S. Department of Homeland Security/Office of Cyber and Infrastructure Analysis, National Risk Estimate on Aging and Failing Critical Infrastructure Systems, , Washington, D.C., December 2014: p. 12

[113] (U) Staff, "Brockton to Investigate Water Main Infrastructure after Pipe Break," http://www.enterprisenews.com/article/20150706/NEWS/150707996/?Start=1, accessed 13 July 2015.

[114] (U) Ransom, Jan and Travis Andersen, "After Water Main Break, Brockton Declares State of Emergency," https://www.bostonglobe.com/metro/2015/05/27/water-service-disrupted-brockton-and-towns-after-water-main-break/Q9uEuQYp0EYqGSei6DOmkK/story.html, accessed 31 July 2015.

[115] (U) WCVB, "State of Emergency Remains in Effect after Major Water Main Break," http://www.wcvb.com/news/brockton-other-towns-without-water-after-main-break/33239270, accessed 13 July 2015.

[116] (U) Paulin, Benjamin and Joseph Markman, "Broken Main Cuts Water to Brockton," http://www.southcoasttoday.com/article/20150527/news/150529412, accessed 13 July 2015.

of thousands of people to boil their cleaning and drinking water.[117]

- (U) Kilmore East, Australia: The most deadly fire on a day known as Black Saturday in Australia in 2009 occurred because of electrical arcing from a broken 43-year-old conductor.[118] The Kilmore East fire killed 119 people, destroyed more than 1,000 homes, and affected more than 125,000 hectares of land, destroying critical infrastructure assets including police stations, water treatment plants, power substations, communication towers, government facilities, schools, and businesses.[119] The fire is estimated to have caused more than $1 billion in damages.[120]
- (U) Toronto, Canada: The Toronto Transit Commission (TTC) was blamed when one of its busiest lines was shut down because of equipment failure during rush hour on the morning of February 23, 2015. The 3-hour shutdown forced commuters to resort to alternative outdoor modes of transportation including buses and streetcars on that day of record-breaking cold.[121,122] TTC employees admitted that its system's 60-year-old age was to blame for the shutdown.[123]

(U) BARRIERS TO MITIGATING AGING AND FAILING INFRASTRUCTURE

(U) OCIA assesses that lack of funding is one of the primary factors affecting owners' ability to adequately maintain critical infrastructure.[124] Although state and local governments and private industry are using innovative funding mechanisms, such as public-private partnerships (PPPs), to decrease the funding gap, current funding by both private and public partners is insufficient to meet current and future funding needs. PPPs increase the participation of private investors in the development and operations of public infrastructure projects. Private responsibilities can range from simply managing the project to designing, building, financing, operating, and maintaining the infrastructure.[125] Budget cuts, population shifts, and decreased usage lead to decreased revenues; no tax increases account for inflation.[126] In the next 10 years, owners and operators will take the following factors into account when deciding when and how to invest in infrastructure maintenance, repairs, and replacements: upfront costs, replacement duration and service interruption, repair and replacement versus maintenance and mitigation, new legislation and regulations, short-term funding plans, and externalities.[127]

(U) In addition, rapid increases in urban populations are likely to increase demand for improved services, increase infrastructure use, expand seasons of consumption, or decrease available "down time" for maintenance and repairs. These factors are likely to increase system stress and may increase the likelihood of critical infrastructure failures. Rapid population growth comes with demand for new or expanded infrastructure systems, including energy supplies and connections, roads and bridges, and water and wastewater systems.

(U) EFFECT OF FAILING INFRASTRUCTURE

(U) According to the American Society of Civil Engineers (ASCE), roughly $3.6 trillion in total investment is needed by 2020 to return the Nation's critical infrastructure facilities to good repair, defined by the organization as safe and reliable with minimal capacity issues and minimal risk.[128] The funding gap for all critical infrastructure areas is estimated to be approximately $1.6 trillion; closing the funding gap would require spending an additional $201 billion a year until 2020.[129]

(U) The consequences of failure to properly mitigate risks to critical infrastructure through adequate funding, maintenance, and repair in the next 10 years will be severe. OCIA assesses that critical infrastructure failures and funding deficiencies will have cascading effects on the U.S. economy by lowering business productivity, gross domestic product (GDP), employment, personal income, and international

[117] (U) Markman, Joseph, "Brockton Continues to Come Clean after Emergency," http://www.enterprisenews.com/article/20150527/NEWS/150527106, accessed 13 July 2015.

[118] (U) Australian Information Warfare and Security Conference, "Australian Critical Infrastructure Protection: A Case of Two Tales," http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1035&context=isw, accessed 11 August 2015.

[119] (U) 2009 Victorian Bushfires Royal Commission, "The Kilmore East Fire," http://www.royalcommission.vic.gov.au/Finaldocuments/volume-1/PF/VBRC_Vol1_Chapter05_PF.pdf, accessed 11 August 2015.

[120] (U) Bowden, Ebony, "Bushfire Class Action: What It Means for Victims and the Power Company," http://thenewdaily.com.au/news/2014/07/15/explainer-black-saturday-class-action/, accessed 11 August 2015.

[121] (U) Westwood, Rosemary, "TTC Delays Amid Cold Weather Blamed on Aging Infrastructure," http://www.metronews.ca/news/toronto/2015/02/23/ttc-transit-troubles-blamed-on-age.html, accessed 2 July 2015.

[122] (U) Fox, Chris, "Subway Service Resumes between Union and Bloor-Yonge Stations," http://www.cp24.com/news/subway-service-resumes-between-union-and-bloor-yonge-stations-1.2248768, accessed 2 July 2015.

[123] (U) Westwood, Rosemary, "TTC Delays Amid Cold Weather Blamed on Aging Infrastructure," http://www.metronews.ca/news/toronto/2015/02/23/ttc-transit-troubles-blamed-on-age.html, accessed 2 July 2015,.

[124] (U) U.S. Department of Homeland Security/Office of Cyber and Infrastructure Analysis, National Risk Estimate on Aging and Failing Critical Infrastructure Systems, , Washington, D.C. December 2014: p. 2

[125] (U) U.S. Department of Homeland Security/Office of Cyber and Infrastructure Analysis, National Risk Estimate on Aging and Failing Critical Infrastructure Systems, , Washington, D.C. December 2014: p. 16

[126] (U) Ibid., 3.

[127] (U) Ibid., 18.

[128] (U) Sanders, Bernie, "Repairing Our Infrastructure," Senate Budget Committee, http://www.budget.senate.gov/democratic/public/index.cfm/repairing-our-infrastructure, accessed 2 July 2015.

[129] (U) Mitchell, Anthea, "Highway to Hell: American Infrastructure in Desperate Need of Reform," http://www.cheatsheet.com/politics/highway-to-hell-american-infrastructure-in-desperate-need-of-reform.html/?a=viewall, accessed 7 July 2015.

competitiveness.[130] According to the ASCE, from 2012 to 2020, the U.S. economy is likely to lose more than $3.1 trillion in GDP and $1.1 trillion in total trade.[131] The U.S. economy could lose almost $1 trillion in business sales through 2020, resulting in a loss of 3.5 million jobs.[132] In addition, OCIA assesses that a predicted labor force shortage in the coming decades could hamper efforts aimed at implementing and maintaining aging infrastructure upgrades. In the next 10 years, one-quarter of all infrastructure workers (more than 2.7 million) in the United States will need to be replaced.[133]

(U) Critical infrastructure failures will occur more frequently in the coming decade if risks are not appropriately mitigated, leading to increasingly negative effects on the Nation's health, public safety, economic well-being, and national security.[134]

(U) EXTREME WEATHER: A GLOOMY FORECAST

(U) Extreme weather poses a significant challenge to the resiliency and sustainability of critical infrastructure. The risk of these disasters is exacerbated by the current state of our aging and failing infrastructure, increasing population density in high-risk areas, and—in the case of droughts, floods, and hurricanes—by trends associated with climate change.[135] OCIA assesses that extreme weather is highly likely to increase in frequency and intensity during the next 10 years. As extreme weather becomes more frequent and intense, risk to critical infrastructure grows. Extreme weather, intensified by the effects of climate change, is expected to cost the United States approximately 100,000 jobs and $15 billion in GDP by 2025.[136]

- (U) California: Experts at the University of California, Davis, estimate that the 2015 California drought will cost the state a total of $2.7 billion in statewide economic losses and approximately 21,000 jobs.[137]

(U) An interagency Quadrennial Energy Review Task Force determined that extreme weather occurrences have been increasing during the past decade, and this trend is expected to intensify under continuing climate change.[138] Extreme weather events projected to increase during the coming decade include more frequent heavy precipitation events, longer and more intense drought, heat waves, and wildfires.[139]

(U) The potential for flash floods, urban floods, and coastal floods is expected to increase as a result of more frequent heavy precipitation events.[140]

(U) Higher temperatures are projected to increase hurricane-associated storm intensity and rainfall rates, both of which can lead to severe damage to critical infrastructure.[141,142] Categories 4 and 5 hurricanes in the Atlantic are expected to occur more frequently, and the resulting flooding and strong winds can damage or destroy critical infrastructure.[143] Heavy precipitation-related extreme weather events can have a significant, and in some areas of the country devastating, effect on the Water and Wastewater Systems, Energy, Transportation Systems, and Communications Sectors.[144]

(U) Short-term (seasonal or shorter) droughts are expected to intensify in most U.S. regions, whereas long-term (multi-seasonal) droughts are expected to intensify in large areas of the Southwest, southern Great Plains, and Southeast.[145] Longer periods of dry weather and more extreme heat are projected to intensify summer droughts almost everywhere in the continental United States.[146] Drier conditions and droughts can exacerbate conditions that fuel

[130] (U) American Society of Civil Engineers, "Failure to Act: The Impact of Current Infrastructure Investment on America's Economic Future", http://www.asce.org/uploadedFiles/Issues_and_Advocacy/Our_Initiatives/Infrastructure/Content_Pieces/failure-to-act-economic-impact-summary-report.pdf, accessed 17 June 15.

[131] (U) Ibid., 5.

[132] (U) Sanders, Bernie, "Repairing Our Infrastructure," Senate Budget Committee, http://www.budget.senate.gov/democratic/public/index.cfm/repairing-our-infrastructure, accessed 2 July 2015.

[133] (U) Brookings Institution, "Beyond Shovel Ready: The Extent and Impact of U.S. Infrastructure Jobs" http://www.brookings.edu/research/interactives/2014/infrastructure-jobs#/M10420, accessed 17 June 2015.

[134] (U) U.S. Department of Homeland Security, "What is Critical Infrastructure?" http://www.dhs.gov/what-critical-infrastructure, accessed 13 July 2015.

[135] (U) U.S. Department of Homeland Security, "The 2014 Quadrennial Homeland Security Review," https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pd,f, accessed 14 October 2015.

[136] (U) Sandia National Laboratories, Assessing the Near-Term Risk of Climate Uncertainty: Interdependencies among the U.S. States, Albuquerque, New Mexico, May 2010 pp. 18 and 19.

[137] (U) University of California, Davis, Economic Analysis of the 2015 Drought for California Agriculture, https://watershed.ucdavis.edu/files/biblio/Final_Drought%20Report_08182015_Full_Report_WithAppendices.pdf, accessed 15 July 2015.

[138] (U) Quadrennial Energy Review Task Force, Quadrennial Energy Review: Energy Transmission, Storage, and Distribution Infrastructure http://energy.gov/sites/prod/files/2015/04/f22/QER-ALL%20FINAL_0.pdf, accessed 9 July 2015.

[139] (U) U.S. Global Change Research Program, Climate Change Impacts in the United States: The Third National Climate Assessment Ch. 4: Energy Supply and Use, p. 115.

[140] (U) U.S. Global Change Research Program, Climate Change Impacts in the United States: The Third National Climate Assessment Ch. 3: Water Resources, p. 75.

[141] (U) U.S. Global Change Research Program, Climate Change Impacts in the United States: The Third National Climate Assessment Ch. 2: Our Changing Climate, p. 20.

[142] (U) Ibid., 43.

[143] (U) U.S. Global Change Research Program, Climate Change Impacts in the United States: The Third National Climate Assessment Ch. 5: Transportation, p. 135.

[144] (U) Ibid., 86.

[145] (U) Ibid., 70.

[146] (U) Ibid., 75.

wildfires, primarily in the western United States.[147] In addition, droughts and drier conditions can negatively affect the Water and Wastewater Systems, Energy, and Transportation Systems Sectors, in particular.

(U) EXTREME WEATHER AND ITS EFFECT ON CRITICAL INFRASTRUCTURE SECTORS

(U) By the year 2025, extreme weather will have significant effects on the Water and Wastewater Systems, Energy, Transportation Systems, Food and Agriculture, and Healthcare and Public Health Sectors. Effects to these Sectors will result in cascading consequences across all critical infrastructure Sectors.

(U) Water and Wastewater Systems: Extreme weather is projected to exacerbate water shortages by reducing water availability and increasing water demand.[148] The entire United States will face challenges balancing water supply and demand, but the Southeast and Southwest regions are especially vulnerable.[149] Sandia National Laboratories assesses that the industries most directly affected by reduced water availability are agriculture and farming, food, beverage, paper, petroleum and coal, chemical, primary metal, mining, thermoelectric power generation, hydropower, and municipal water utilities.[150]

(U) More intense precipitation and floods will negatively affect wastewater treatment by increasing the likelihood of combined sewer overflows and contaminated overland flow.[151] Wastewater utility infrastructure may be damaged and become less efficient because of more frequent coastal flooding.[152]

(U) Impacts to the Water and Wastewater Systems Sector can cascade across all dependent critical infrastructure Sectors including Energy, Food and Agriculture, Transportation Systems, Emergency Services, and Healthcare and Public Health.[153]

- (U) California: Mandated statewide water conservation measures are expected to reduce water agencies' revenue by $1 billion in 2015.[154] Consequently, customers are likely to see higher water bills. In San Francisco, for example, the Bay Area's largest water wholesaler increased prices by 28 percent to make up for reduced sales.[155]

(U) Energy: The Quadrennial Energy Review Task Force assessed that energy transmission, storage, and distribution infrastructure will become more vulnerable as occurrences of extreme weather increase.[156] Extreme weather is one of the primary sources of electrical grid disturbances in the United States, and this risk is projected to grow.[157] High temperature extremes and a rise in average temperatures are projected to increase the demand for electricity needed for cooling in all U.S. regions. This will likely lead to increased use of transmission and distribution systems during peak demand.[158,159] More fuel and energy are required to generate and deliver electricity in hotter temperatures; consequently, increases in electricity demand can raise costs for producers and consumers.[160]

(U) Thermoelectric power plants—coal, nuclear, natural gas, and oil—produce 90 percent of electrical energy in the United States making power plant cooling a critical national water use.[161,162] Reduced efficiency in power plant cooling increases the risk of partial or full shutdowns of electricity generation facilities.[163]

[147] (U) National Wildlife Federation, "Global Warming and Wildfires," http://www.nwf.org/Wildlife/Threats-to-Wildlife/Global-Warming/Global-Warming-is-Causing-Extreme-Weather/Wildfires.aspx, accessed 9 July 2015.

[148] (U) U.S. Global Change Research Program, Climate Change Impacts in the United States: The Third National Climate Assessment Ch. 3: Water Resources, 87.

[149] (U) Ibid.

[150] (U) Sandia National Laboratories, Assessing the Near-Term Risk of Climate Uncertainty: Interdependencies among the U.S. States, p. 110.

[151] (U) U.S. Global Change Research Program, Climate Change Impacts in the United States: The Third National Climate Assessment Ch. 3: Water Resources, 85.

[152] (U) U.S. Global Change Research Program, Climate Change Impacts in the United States: The Third National Climate Assessment Ch. 3: Water Resources, 86.

[153] (U) U.S. Department of Homeland Security, "Water and Wastewater Systems Sector: Sector Overview," http://www.dhs.gov/water-and-wastewater-systems-sector, accessed 10 July 2015.

[154] (U) NBC Los Angeles, "California Water Rates Rise as Cities Lose Money in Drought," http://www.nbclosangeles.com/news/california/Saving-Water-Rising-Costs-Drought-311680531.html, accessed 15 July 2015.

[155] (U) Ibid.

[156] (U) Quadrennial Energy Review Task Force, "Quadrennial Energy Review: Energy Transmission, Storage, and Distribution Infrastructure," http://energy.gov/sites/prod/files/2015/04/f22/QER-ALL%20FINAL_0.pdf, accessed 9 July 2015.

[157] (U) Quadrennial Energy Review Task Force, Quadrennial Energy Review: Energy Transmission, Storage, and Distribution Infrastructure http://energy.gov/sites/prod/files/2015/04/f22/QER-ALL%20FINAL_0.pdf, accessed 9 July 2015.

[158] (U) U.S. Global Change Research Program, Climate Change Impacts in the United States: The Third National Climate Assessment Ch. 4: Energy Supply and Use, 116.

[159] (U) Quadrennial Energy Review Task Force, Quadrennial Energy Review: Energy Transmission, Storage, and Distribution Infrastructure http://energy.gov/sites/prod/files/2015/04/f22/QER-ALL%20FINAL_0.pdf, accessed 9 July 2015.

[160] (U) U.S. Global Change Research Program, Climate Change Impacts in the United States: The Third National Climate Assessment Ch. 4: Energy Supply and Use, 116.

[161] (U) U.S. Global Change Research Program, Climate Change Impacts in the United States: The Third National Climate Assessment Ch. 3: Water Resources, 109.

[162] (U) Union of Concerned Scientists, "How it Works: Water for Power Plant Cooling," http://www.ucsusa.org/clean_energy/our-energy-choices/energy-and-water-use/water-energy-electricity-cooling-power-plant.html, accessed 10 July 2015.

[163] (U) Quadrennial Energy Review Task Force, Quadrennial Energy Review: Energy Transmission, Storage, and Distribution Infrastructure http://energy.gov/sites/prod/files/2015/04/f22/QER-ALL%20FINAL_0.pdf, accessed 9 July 2015.

(U) Effects to the Energy Sector can affect all critical infrastructure Sectors, because all industries require electric power and fuel to function.[164]

- (U) California: The 2013 Yosemite Rim Fire forced two hydroelectric power plants offline, requiring San Francisco to spend $600,000 to make up for energy losses.[165,166]

(U) Transportation Systems: Extreme weather will affect transportation systems directly through damage to infrastructure and indirectly through shifts in trade flows, agriculture, energy use, and settlement patterns.[167] Changing climatic conditions may reduce the reliability and capacity of transportation systems that were not designed to withstand unanticipated extreme weather.[168] Increasing temperatures, more instances of extreme weather, and changes in precipitation can affect all regions and transportation systems.[169] Severe storms are capable of causing disruptions to almost all types of transportation systems through delays.[170]

- (U) Texas: The Blanco River in Central Texas flooded after a record-high rainfall during 2015.[171,172] The Hays County Emergency Management office estimated that replacing flood-damaged infrastructure and cleaning up debris will cost more than $5 million for roads and $4.1 million for bridges.[173] During the weekend storms, more than 200 flights at airports in Houston and Dallas were canceled because of the heavy rain.[174]

(U) Extreme heat will accelerate asphalt deterioration, cause buckling of pavements and rail lines, stress expansion joints on bridges and highways, and reduce aircraft operational efficiency.[175] Drought can negatively affect the Transportation Systems and Dams Sectors by affecting ports and inland navigation channels through low water levels. Flooding can affect inland marine transportation infrastructure, railroads, seaports, airports, roads, and bridges.[176,177] Floods and droughts can create unscheduled lock outages that affect inland waterway availability.[178,179] Critical infrastructure sectors that rely on the transportation system for operational success will potentially be adversely affected by extreme weather effects on the Transportation Systems Sector.

(U) Food and Agriculture: Extreme weather disruptions to agricultural production have increased during the past four decades and are projected to continue to increase throughout the next decade.[180] OCIA assesses that extreme weather, including heat waves, dry spells, and sustained droughts, will have a major effect on crops and livestock.[181]

(U) According to 2010 U.S. Geological Survey data, approximately 32 percent of water is used for U.S. irrigation.[182] Extreme weather, specifically long-term droughts, is likely to affect crop-water requirements and crop-water availability, both of which affect crop productivity and costs of water access.[183] Projected increased exposure to temperatures and soil water conditions outside plants' and animals' various biological ranges because of more extreme weather can cause stress and reduce production.[184] Projected increases in the number of consecutive dry days (especially in the southern and western United States) and the number of hot nights (in all regions of the United States) are expected to negatively affect crop and animal production.[185] Extreme weather can alter agricultural yields, food- and water-borne disease distribution, and food trade and distribution; consequently, food security and public health might be adversely affected.[186] The Food and Agriculture Sector has particularly critical dependencies with the Water and Wastewater Systems, Transportation Systems, Energy, Financial Services, Chemical, and Dams Sectors.[187]

[164] (U) U.S. Department of Homeland Security, "Energy Sector: Sector Overview," http://www.dhs.gov/energy-sector, accessed 10 July 2015.

[165] (U) Francis, Monte and Lori Preuitt, "Yosemite Rim Fire Chars 225 Square Miles, Destroys Berkeley Tuolumne Camp," http://www.nbcbayarea.com/news/local/Rim-Firestorm-Chars-200-Square-Miles-220964981.html, accessed 15 July 2015.

[166] (U) Wilkey, Robin, "Yosemite Fire Threatens San Francisco Water and Power," http://www.huffingtonpost.com/2013/08/27/yosemite-fire-san-francisco_n_3819962.html, accessed 15 July 2015.

[167] (U) U.S. Global Change Research Program, Climate Change Impacts in the United States: The Third National Climate Assessment Ch. 5: Transportation, 131.

[168] (U) Ibid., 131.

[169] (U) Ibid., 131.

[170] (U) Ibid., 135.

[171] (U) McClure, Charles, "Residents Regroup in Face of Adversity," Blanco County News, June 19, 2015, http://www.blanconews.com/946-residents-regroup-in-face-of-adversity, accessed 14 July 2015.

[172] (U) Fritz, Angela, "Record-Breaking Rainfall Forces Critical Flash Flooding in Oklahoma, Texas," https://www.washingtonpost.com/news/capital-weather-gang/wp/2015/05/24/record-breaking-rainfall-forces-critical-flash-flooding-in-saturated-oklahoma-texas/, accessed 14 July 2015.

[173] (U) Rollins, Brad, "Hays County Hopes to Temporarily Bridge Blanco River with Railroad Cars," http://smmercury.com/2015/06/25/hays-county-hopes-to-temporarily-bridge-blanco-river-with-railroad-cars/, accessed 14 July 2015.

[174] (U) Hays, Kristen and Amanda Orr, "UPDATE 10-Storms Kill 17 in Texas, Oklahoma; Houston Flooded," http://www.reuters.com/article/usa-storms-idUSL1N0YH0VF20150527, accessed 14 July 2015.

[175] (U) Ibid..

[176] (U) Quadrennial Energy Review Task Force, Quadrennial Energy Review: Energy Transmission, Storage, and Distribution Infrastructure http://energy.gov/sites/prod/files/2015/04/f22/QER-ALL%20FINAL_0.pdf, accessed 9 July 2015.

[177] (U) U.S. Global Change Research Program, Climate Change Impacts in the United States: The Third National Climate Assessment Ch. 5: Transportation, 138.

[178] (U) Quadrennial Energy Review Task Force, Quadrennial Energy Review: Energy Transmission, Storage, and Distribution Infrastructure http://energy.gov/sites/prod/files/2015/04/f22/QER-ALL%20FINAL_0.pdf, accessed 9 July 2015.

[179] (U) Ibid.

[180] (U) U.S. Global Change Research Program, Climate Change Impacts in the United States: The Third National Climate Assessment Ch. 6: Agriculture, 152.

[181] (U) Ibid., 161.

[182] (U) USGS, Summary of Estimated Water Use in the United States.

[183] (U) U.S. Global Change Research Program, Climate Change Impacts in the United States: The Third National Climate Assessment Ch. 6: Agriculture, 160.

[184] (U) Ibid., 173.

[185] (U) Ibid., 155.

[186] (U) Ibid., 162,163.

[187] (U) U.S. Department of Homeland Security, "Food and Agriculture Sector: Sector Overview," http://www.dhs.gov/food-and-agriculture-sector, accessed 14 July 2015.

- (U) Brazil: An agro-climatologist estimates that Brazil could lose approximately 10 percent of its coffee crop and 20-22 percent of its soybean crop by 2020. Brazil is the world's biggest coffee producer and second-biggest soybean producer.[188,189]

(U) Healthcare and Public Health: In both inland and coastal areas, flooding will negatively affect the Healthcare and Public Health Sector by exacerbating human health risks associated with critical infrastructure failures including waterborne diseases, decreased sanitary conditions, and airborne diseases.[190]

(U) Extreme weather, propelled by climate change, is likely to disrupt physical, biological, and ecological systems. The result will likely be an effect to public health through increased respiratory and cardiovascular disease, injuries and premature deaths related to extreme weather, and threats to mental health.[191]

(U) The Healthcare and Public Health Sector depends on numerous other critical infrastructure Sectors including the Communications, Emergency Services, Energy, Food and Agriculture, Information Technology, Transportation Systems, and Water and Wastewater Systems Sectors.[192]

(U) ECONOMIC CONSEQUENCES OF EXTREME WEATHER EVENTS

(U) The increase in frequency of extreme weather events (e.g., hurricanes, blizzards, and flooding) will likely lead to higher costs in preparing for, responding to, and recovering from such events.[193] This is because these events are anticipated to become more severe and damaging. According to NOAA, during 2014, eight weather and climate disaster events occurred with losses exceeding $1 billion each across the United States. These events included a drought, a flood, five severe storms, and a winter storm overall. NOAA states that between 1980 and 2014, the United States has experienced 178 weather and climate disasters; the total costs reaching or exceeding $1 billion per event. The total cost of those 178 events exceeds $1 trillion.[194] Figure 2 shows a rise in number of billion-dollar damage events caused by extreme weather per year and an increase in total cost of billion-dollar damage events per year between 1980 and 2012. The cost of extreme weather will continue to rise for the foreseeable future; consequently, stakeholders will need to consider investing in resiliency measures to mitigate disruptions to critical infrastructure.

(U) NEXT PANDEMIC: EMERGENCE AND OUTBREAK

(U) Although the likelihood and consequence of pandemics are low in probability, OCIA anticipates the high impact of these events to increase during the next decade. The likelihood is driven in large part by increasing opportunities for infectious diseases to emerge and quickly diffuse because of our highly globalized society.[195] Trends in severe weather patterns, a continuously globalizing world in which barriers to trade, tourism, and migration are less restrictive, and an increase in global urbanization all contribute to the potentiality of the next pandemic. The outbreak of a pandemic could affect multiple critical infrastructure sectors in the United States, as well as economic and political systems.[196]

(U) OCIA assesses that the critical infrastructure Sectors most likely to be affected by a pandemic are Healthcare and Public Health, Emergency Services, Transportation Systems, Water and Wastewater Systems, and Energy (Electrical Power).

(U) The effects of a pandemic on a population and critical infrastructure can vary based on the transmissibility and severity of the disease, with higher rates of sickness (morbidity) and mortality having a greater impact. In addition, the effect can vary based not only on the virus' characteristics, but also on the demographic information of critical infrastructure personnel, behavior of personnel once a pandemic occurs, and the capability of the Healthcare and Public Health Sector to provide adequate care to the sick.[197] Pandemics such as influenza and plague vary widely in their characteristics, creating challenges to pandemic planning and mitigation strategies.[198]

[188] (U) Rapoza, Kenneth, "Brazil Loses Billions as Crops Reduced by Wacky Weather," Forbes, http://www.forbes.com/sites/kenrapoza/2014/03/03/brazil-loses-billions-as-crop-losses-mount-from-wacky-weather/#2f0ddd551c5a, accessed 16 July 2015.

[189] (U) Garcia-Navarro, Lourdes, "Drought Could Drain More Than Brazil's Coffee Crop," http://www.npr.org/2014/02/23/280770928/drought-could-drain-more-than-brazils-coffee-crop, accessed 16 July 2015.

[190] (U) U.S. Global Change Research Program, Climate Change Impacts in the United States: The Third National Climate Assessment Ch. 3: Water Resources, 87.

[191] (U) U.S. Global Change Research Program, Climate Change Impacts in the United States: The Third National Climate Assessment Ch. 9: Human Health, 221.

[192] (U) U.S. Department of Homeland Security, "Healthcare and Public Health Sector: Sector Overview," http://www.dhs.gov/healthcare-and-public-health-sector, accessed 14 July 2015.

[193] (U) U.S. Department of Homeland Security, "The 2014 Quadrennial Homeland Security Review," https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pd,f, accessed 14 October 2015.

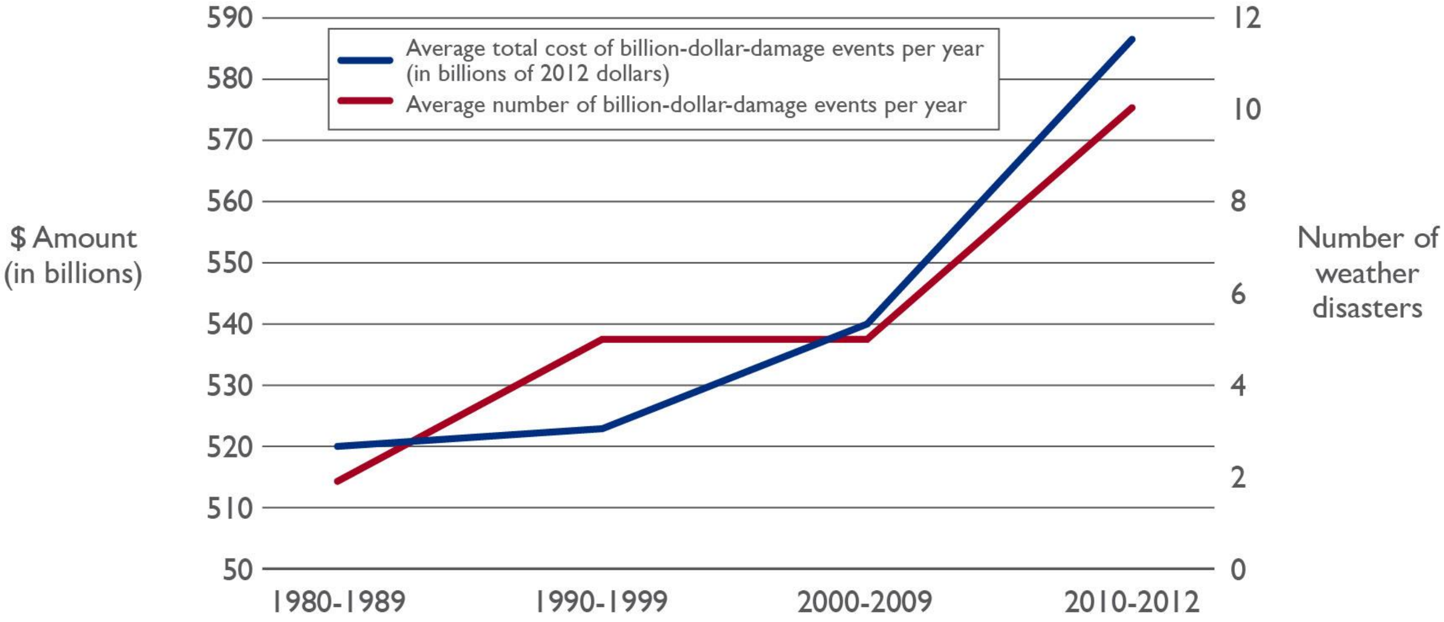
[194] (U) NOAA, Billion-Dollar Weather and Climate Disasters: Overview, https://www.ncdc.noaa.gov/billions/, accessed 14 October 2015.

[195] (U) U.S. Department of Homeland Security, "The 2014 Quadrennial Homeland Security Review," https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pd,f, accessed 14 October 2015.

[196] (U) Fonkwo, Peter Nbedoc, "Pricing Infectious Disease," http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3327542/pdf/embor200811 0.pdf, accessed 7 July 2015.

[197] (U) Ibid.

[198] (U) Office of Cyber and Infrastructure Analysis, Pandemic Impacts To Lifeline Critical Infrastructure, Washington, D.C.: U.S. Department of Homeland Security, July 2015, p. 2.



(U) FIGURE 2—AVERAGE NUMBER AND TOTAL COST OF BILLION-DOLLAR U.S. WEATHER DISASTERS, 1980–2012

(U) A pandemic's effect on critical infrastructure arises not from the disease itself, but from the effect the pandemic has on personnel required to maintain and operate critical infrastructure and to sustain domestic and global supply chains, including medical supplies and food. Critical infrastructure sectors can even exacerbate the transmission of a pandemic regionally and nationally. The Transportation Systems Sector, for example, can act as a vector for spreading a pandemic across state and national borders from trade and tourism. Trade and travel across state and national borders create numerous opportunities for the spread of infection to multiple individuals.[199] Packed train cars, international flights, and poor living conditions can all contribute to the dissemination of a disease.

- (U) Severe Acute Respiratory Syndrome (SARS) November 2002: Originally believed to be an abnormal amount of atypical pneumonia cases, SARS emerged in China's Guangdong Province in the fall of 2002. Later in February 2003, a Chinese physician treating patients in China, who became infected with the virus, traveled to Hong Kong. Some Individuals staying at the same hotel as the physician became infected and subsequently traveled to Vietnam, Singapore, and Canada. By the spring of 2003, the outbreak spread to 26 countries.[200]

(U) The United States experienced three pandemic outbreaks in the 20th century. The impact of each varied depending on the virulence of the pandemic, but all resulted in a tragic number of deaths totaling approximately 500,000 in 1918, 70,000 in 1958, and 34,000 in 1968.[201]

(U) PANDEMIC DRIVERS

(U) The lack of universal health-monitoring and emergency planning in underdeveloped and developing countries increases the likelihood that a new pandemic will emerge.[202] An inadequate health response to the initial onset of a pathogen could intensify its outbreak.[203] Compounded by a globalized society in which barriers to travel and movement of goods are fading, the potential for an infectious disease to spread across national borders is high.[204,205]

[199] (U) Kimball M.D., Ann Marie, "Infectious Disease Movement in a Borderless World," http://www.nap.edu/read/12758/chapter/4#110, accessed 11 December 2015.

[200] (U) United States General Accounting Office, "Emerging Infectious Disease: Asian SARS Outbreak Challenged International and National Responses", http://www.gao.gov/new.items/d04564.pdf, accessed 11 December 2015.

[201] (U) U.S. Department of Homeland Security, "National Population, Economic, and Infrastructure Impacts of Pandemic Influenza with Strategic Recommendations,"Washington, D.C.,, , October 2007,. p. 11

[202] (U) Weber, Carol J., "Update on Global Climate Change," Urologic Nursing Journal, 2010, p. 83.

[203] (U) Global Trends 2025: A Transformed World, www.dni.gov/nic/NIC_2025_project.html, p. 75, November 2008, accessed 10 July 2015.

[204] (U) Weber, Carol J., "Update on Global Climate Change," Urologic Nursing Journal, 2010,p. 83.

[205] (U) Gushulak M.D., Brian D., MacPherson M.D., Dougles W., "Infectious Disease Movement in a Borderless World," http://www.nap.edu/read/12758/chapter/3#52, accessed 11 December 2015.

(U) AFFECTED SECTORS

(U) OCIA judges that the Sectors most likely to be affected by a pandemic are Healthcare and Public Health, Emergency Services, Transportation Systems, Water and Wastewater Systems, and Energy (Electrical Power). All other critical infrastructure sectors will be affected to some degree by the availability of personnel needed to maintain operations.[206]

(U) Illness, the need to care for sick family members, community protection strategies, and voluntary self-isolation could significantly increase worker absenteeism across all sectors during a pandemic, affecting infrastructure operations and the economy.[207] The two potential effects of concern are service supply reductions and increased demand because of behavior or health status changes.

(U) Critical infrastructure sectors with relatively large percentages of critical workers are most vulnerable to disruption when high levels of absenteeism occur.[208] Although the total workforce population for critical infrastructure sectors varies, the top four Sectors most vulnerable to worker absenteeism are Water and Wastewater Systems, Healthcare and Public Health, and Emergency Services.

- (U) 2009 H1N1 Pandemic: In April 2009, a strain of H1N1 emerged in North America and rapidly spread around the world.[209] Two months later, H1N1 would be officially declared a pandemic, lasting until August 2010.[210,211] A study published by the National Institutes of Health found that the NCR experienced an estimated $6.7 billion economic loss because of workforce absenteeism and inoperability during the pandemic.[212]

(U) The economic impact of a pandemic will depend greatly upon the severity of the pandemic and mitigation efforts taken by the federal, state, and local governments and the public. Estimates for loss in GDP during the first year of a pandemic could range from less than 1 percent in a mild pandemic to up to 4.25 percent during a severe pandemic.[213] Once the pandemic has passed, the longer term economic losses will be due primarily to the number of deaths caused by the disease.

(U) Healthcare and Public Health Sector: The National Infrastructure Advisory Council surveyed critical infrastructure sectors and found that 51.8 percent of Healthcare and Public Health Sector workers were deemed "Tier 1" critical workers essential to maintaining operations during a pandemic. Because of their frequent direct contact with infected patients, these critical personnel are at an increased risk of becoming ill, resulting in a greater strain upon the Sector. In addition to personnel shortages, the Healthcare and Public Health Sector will have to prioritize limited resources to treat pandemic victims in addition to their usual patient load.[214]

(U) The health care systems in urban areas will be highly stressed during a pandemic; seriously ill people will be forced to rely on alternative care strategies if the patient load generated by a severe pandemic is similar to patient loads experienced during the worst pandemics in the past.[215] The health care costs related to implementing mitigation strategies during a pandemic are predicted to be up to $80 billion depending on the success of the interventions, and the predicted GDP losses could be up to $100 billion in the first year.[216]

(U) Emergency Services Sector: Much like the Healthcare and Public Health Sector, the workers in the Emergency Services Sector, and especially those in the Emergency Medical Services Subsector, are at an increased risk because of the likelihood of contact with infected people. The 2007 National Infrastructure Advisory Council survey on critical infrastructure stated that the Emergency Services Sector considered more than 87 percent of its workers Tier 1 critical, and it is likely that many emergency services agencies have a rate of Tier 1 workers above 87 percent. With such a high percentage of workers deemed critical, even a small number of absent workers can have an effect on the Emergency Services Sector and the sectors that rely on them, especially the Healthcare and Public Health Sector. Supply chain disruptions could also significantly hamper the effectiveness of the Sector's workforce during a pandemic.[217]

[206] (U) Office of Cyber and Infrastructure Analysis, Pandemic Impacts on Lifeline Critical Infrastructure, Washington, D.C.:, July 2015.p.1

[207] (U) U.S. Department of Homeland Security, "National Population, Economic, and Infrastructure Impacts of Pandemic Influenza with Strategic Recommendations,"Washington, D.C., , , October 2007, p. 16, accessed 14 July 2015.

[208] (U) Ibid., 25.

[209] (U) Santos, Joost R., et al., "Risk-Based Input-Output Analysis of Influenza Epidemic Consequences on Interdependent Workforce Sectors," http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3640689/pdf/nihms423932.pdf, accessed 17 July 2015.

[210] (U) Ibid., 2.

[211] (U) The virus continues to circulate around the world.

[212] (U) Santos, Joost R., et al., "Risk-Based Input-Output Analysis of Influenza Epidemic Consequences on Interdependent Workforce Sectors," http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3640689/pdf/nihms423932.pdf, accessed 17 July 2015.

[213] (U) Office of Cyber and Infrastructure Analysis, Pandemic Impacts To Lifeline Critical Infrastructure, Washington, DC: U.S. Department of Homeland Security, July 2015, p. 8.

[214] (U) Office of Cyber and Infrastructure Analysis, "Pandemic Impacts on Lifeline Critical Infrastructure,", Washington, D.C.: U.S. Department of Homeland Security, July 2015, p. 4.

[215] (U) U.S. Department of Homeland Security, "National Population, Economic, and Infrastructure Impacts of Pandemic Influenza with Strategic Recommendations," Washington, D.C.p. 7, , October 2007,, p.7.

[216] (U) U.S. Department of Homeland Security, "National Population, Economic, and Infrastructure Impacts of Pandemic Influenza with Strategic Recommendations,"Washington D.C. , , October 2007,. p. 7.

[217] (U) Office of Cyber and Infrastructure Analysis, "Pandemic Impacts on Lifeline Critical Infrastructure,", Washington, DC: Department of Homeland Security, July 2015. p. 5.

(U) Transportation Systems Sector: OCIA assesses that a significant risk to the Transportation Systems Sector during a pandemic is in the movement of freight by rail. The loss of critical employees to illness or absenteeism could create significant delays moving cargo in and out of rail yards.[218] Any loss in rail capacity could result in cascading effects on critical infrastructure sectors, leading to lengthy delays in the delivery of goods and potential increases in cost because of the need to use other transportation modes. A number of critical infrastructure sectors, including the Energy, Chemical, and Food and Agriculture Sectors, rely heavily on the Rail Subsector for the movement of goods and commodities. In 2014, Class I Railroads moved more than1.8 billion tons of freight. Coal, chemicals, non-metallic minerals, farm products, food, and kindred products accounted for more than 70 percent of tonnage carried by Class I Railroads.[219]

(U) Truck drivers, because of their consistent contact with persons at warehouses, ports, rest stops, and other locations, face a significant risk of becoming ill. Nearly every industry relies on trucks to carry cargo at some point in the shipping chain.[220]

(U) Water and Wastewater Systems Sector: The greatest risk to the Water and Wastewater Systems Sector comes from the loss of available operators and support staff because of illness or absenteeism. Highly specialized personnel, such as plant operators, might be difficult to replace, and their absence could result in disruptions of water and wastewater systems during the pandemic. The effect of the pandemic will vary locally, depending on the number of critical personnel in each locality who are ill or absent.[221]

(U) Energy Sector (Electrical Power): A pandemic alone is unlikely to cause disruptions to the electrical grid, but the greatest risk to the Electric Power Subsector is a significant incident occurring at the same time as a pandemic, which can result in longer lasting power outages that could have cascading effects on other critical infrastructure in the area.[222]

(U) Pandemics and even smaller scale epidemics will result in deliberation over the value of closing borders, restricting travel from certain regions, or even implementing economic restrictions on trade.[223] These government decisions may have a significant effect on the supply chains for the Nation's economy. In addition, research that focuses on manipulating these viruses to study their properties may increase their deadliness. In June 2012, a paper was published identifying mutations to make the bird flu spread easily among ferrets whose immune systems closely model those of humans.[224] Such research helps combat disease but has inherent risks including accidental release or research duplication by malicious actors.[225]

- (U) University of Wisconsin: A professor at the University of Wisconsin-Madison genetically manipulated the 2009 H1N1 virus to study its genetic changes. The experiment resulted in a more lethal strain of the virus against which the human population is considered defenseless.
- (U) Ebola Epidemic in West Africa: As of November 2014, 5,000 recorded deaths are related to Ebola.[226] Countries such as Liberia and Senegal temporarily closed their borders to Guinea as a preventive measure to contain the spread of the deadly virus.[227,228] A report by the World Bank Group estimated a $2.2–$7.4 billion economic loss in 2014 for West Africa because of Ebola.[229]

[218] (U) Ibid., 5.
[219] (U) Ibid., 6.
[220] (U) Ibid., 6.
[221] (U) Office of Cyber and Infrastructure Analysis, "Pandemic Impacts on Lifeline Critical Infrastructure,", Washington, D.C.: U.S. Department of Homeland Security, July 2015. p. 7.
[222] (U) Ibid.
[223] (U) U.S. Department of Homeland Security," The Homeland Security Environment 2014–2019", , accessed 13 May 2015.
[224] (U) Herfst, Sander, et al., "Airborne Transmission of Influenza A/H5N1 Virus Between Ferrets," *Science*, 336, 2012, p. 1534–1541.
[225] (U) NcNeil Jr., Donald G., "Bird Flu Paper Is Published After Debate," *New York Times*, http://www.nytimes.com/2012/06/22/health/h5n1-bird-flu-research-that-stoked-fears-is-published.html?_r=0, accessed 10 December 2012.
[226] (U) The World Bank Group, "The Economic Impact of the 2014 Ebola Epidemic," http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2014/10/07/000456286_20141007140300/Rendered/PDF/912190WP0see0a00070385314B00PUBLIC0.pdf, accessed 17 July 2015.
[227] (U) Flynn, Daniel and Saliou Samb, "Senegal shuts land border with Guinea to prevent Ebola spreading," http://www.reuters.com/article/us-guinea-ebola-idUSBREA2S0JA20140329, accessed 17 July 2015.
[228] (U) Staff, "UN Mission for Ebola Emergency Response (UNMEER) External Situation Report", https://ebolaresponse.un.org/sites/default/files/150223-_unmeer_external_situation_report.pdf, accessed 17 July 2015.
[229] (U)) The World Bank Group, "The Economic Impact of the 2014 Ebola Epidemic," http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2014/10/07/000456286_20141007140300/Rendered/PDF/912190WP0see0a00070385314B00PUBLIC0.pdf, accessed 17 July 2015.

(U) APPENDIX: GLOSSARY

(U) COMMON CAUSES OF INFRASTRUCTURE FAILURE

Corrosion	Corrosion occurs when a material degrades over time as a result of a reaction with its environment. Corrosion becomes more of a danger to infrastructure with the passage of time because the effects cannot be reversed, and in some cases cannot be repaired without replacing the entire asset. Assets composed primarily of metal and exposed to extreme weather or specific soil characteristics are most at risk from corrosion.
Erosion	Erosion is the gradual destruction of something by natural forces (such as water, wind, or ice) that can wear away the surface of a material. Erosion that occurs at the base of bridges near waterways is called "scour" and can lead to washout of an entire structure if left unrepaired.
Extreme Weather and Natural Disasters	Natural disasters such as heat waves, hurricanes, floods, droughts, earthquakes, and tornados endanger infrastructure and can increase the likelihood of failure.
Human Error	All types of infrastructure are susceptible to failure from human error, including design characteristics or improper operation.
Material Fatigue	Constant loading and unloading—cycling a component between compression and tension—can cause material fatigue. Material fatigue is directly related to load and usage. Like bending a paperclip until it snaps, material fatigue typically occurs in structures that undergo heavy use.
System Stress	Logistic failures can occur when an infrastructure system is overloaded by demand. System stress can also lead to physical failures. The Electric Power Subsector, natural gas and hazardous liquid pipelines, and commercial airlines are especially susceptible to system stress.

(U) INDICATORS OF FAILURE

Age	Infrastructure does not fail simply because of advanced age, but some failure mechanisms are directly age-related. Material fatigue, corrosion, and erosion occur with use and over time, and therefore, infrastructure assets susceptible to these failure mechanisms may have an increased likelihood of failure.
Amount of Use	Population shifts are constantly occurring based on economic, climatic, technological, and sociological factors. Both increases and decreases in population, and resulting fluctuations in infrastructure use can increase the risk of failure.
Asset Design	Asset designs depend on the location, cost, and level of acceptable risk. Decreased risk of failure often comes with increased cost. In some cases, older designs may be more resilient than newer designs. Older infrastructure may have been over-engineered—varying material quality, insufficient information regarding failures, and other factors lead engineers to use conservative designs to ensure safety. New infrastructure may meet only the minimum safety standards, lowering cost but increasing risk.
Construction Techniques	Like asset designs, construction techniques have improved over time. Older techniques, such as certain methods of welding, have been found to have an increased likelihood of failure.
Geographic Location	Infrastructure built in regions prone to extreme weather and natural disasters may have a higher likelihood of failure, especially if an asset's design does not account for these hazards. Soil conditions, temperatures, water characteristics, snow, rain, and other factors related to location may also increase the likelihood of failure.

Structural Material	The materials used to build an asset can greatly affect its likelihood of failure. New materials with enhanced properties—including strength, corrosion resistance, and ductility—are always being developed, and older materials become cheaper and more cost-effective as production techniques and capabilities improve.

(U) BARRIERS TO MITIGATING AGING AND FAILING INFRASTRUCTURE

Externalities	The materials used to build an asset can greatly affect its likelihood of failure. New materials with enhanced properties—including strength, corrosion resistance, and ductility—are always being developed, and older materials become cheaper and more cost-effective as production techniques and capabilities improve.
New Legislation and Regulations	Legislation and regulations can be introduced that require owners and operators to invest significant amounts of money to meet new standards, requiring the deferral of other critical needs. New regulations often require infrastructure to meet new specifications, but older infrastructure can be "grandfathered in" and not meet new standards.
Repair and Replacement Versus Maintenance and Mitigation	It is generally less expensive to keep infrastructure well maintained and mitigate against the risk of failure than it is to repair and replace infrastructure following a failure; however, cheaper designs and materials are often chosen to decrease the upfront costs, even though they may result in significantly greater costs in later years.
Replacement Duration and Service Interruption	Owners, operators, and regulators must balance the need to replace infrastructure with the direct costs of replacement and the indirect costs to the public resulting from disruptions.
Short-Term Funding Plans	Short-term funding plans can be an issue for infrastructure owners and operators, because it is difficult to plan for the future when uncertainty exists concerning funding availability. Experts say that stopgap funding prevents investment in important infrastructure projects.
Upfront Costs	Infrastructure projects often require extremely high initial investments. Bridges, dams, navigation locks, and power plants can cost hundreds of millions, if not billions of dollars, to design and build. As a result, it takes a long time for owners to see a return on their investment, even if the infrastructure offers a steady revenue stream. Therefore, both private and public owners can hesitate to invest in new infrastructure. In some cases, owners may simply not have the money available to make a large investment.

(U) DHS POINT OF CONTACT

National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis
U.S. Department of Homeland Security
OCIA@hq.dhs.gov
(U) For more information about the OCIA, visit www.dhs.gov/office-cyber-infrastructure-analysis.

OMB Control No.: 1670-0027
Expiration Date: 10/31/2017

UNCLASSIFIED

Homeland Security

National Protection and Programs Directorate

NPPD Customer Feedback Survey

Product Title:

1. Please select the partner type that best describes your organization. Select One

2. Overall, how satisfied are you with the usefulness of this product?

○ **Very Satisfied** ○ **Somewhat Satisfied** ○ **Neither Satisfied Nor Dissatisfied** ○ **Somewhat Dissatisfied** ○ **Very Dissatisfied**

3. How did you use this product in support of your mission?

□ Integrated into one of my own organization's information or analytic products

□ Used contents to improve my own organization's security or resiliency efforts or plans

If so, which efforts?

□ Shared contents with government partners

If so, which partners?

□ Shared contents with private sector partners

If so, which partners?

□ Other (please specify)

4. Please rank this product's relevance to your mission. ***(Please portion mark comments.)***

○ Critical

○ Very Important

○ Somewhat Important

○ Not Important

○ N/A

5. Please rate your satisfaction with each of the following:

	Very Satisfied	**Somewhat Satisfied**	**Somewhat Dissatisfied**	**Very Dissatisfied**	**N/A**
Timeliness of product or support	○	○	○	○	○
Relevance to your information needs	○	○	○	○	○

6. How could this product or service be improved to increase its value to your mission? ***(Please portion mark comments.)***

To help us understand more about your organization so we can better tailor future products, please provide (OPTIONAL):

Name:

Organization:

Contact Number:

Position:

State: Select One

Email:

SUBMIT FORM

Privacy Act Statement

Paperwork Reduction Act Compliance Statement

UNCLASSIFIED

REV: 3 March 2015