Written Testimony of
Jim Bottum, Vice Provost for Computing & Information Technology and Chief Information Officer
Clemson University

Before the
U.S. House of Representatives

Committee on Homeland Security
The Honorable Michael T. McCaul, Chairman

Subcommittee on Oversight and Management Efficiency
The Honorable Jeff D. Duncan, Chairman

Emergency Preparedness: Are We Ready For A 21st Century Hugo?

November 21, 2014

Mr. Chairman, I would like to thank you and the Members of the Subcommittee for this opportunity to testify here today. I would like to begin by taking a moment to briefly acquaint you with Clemson University and my own background.

Located in Clemson, South Carolina, Clemson University is a nationally ranked, science and technology-oriented land grant public research university founded in 1889. Clemson is known for its emphasis on collaboration and a culture that encourages faculty and students to embrace bold ideas. With an enrollment of 21,857, Clemson is a high-energy, student-centered community dedicated to intellectual leadership, innovation, and service to the community.

As for myself, I currently serve as Clemson's Vice Provost for Computing and Information Technology and Chief Information Officer, and have served in that capacity since 2006. During my tenure here at Clemson, we have undergone a massive transformation of our cyberinfrastructure environment – to include our networking, storage, computational capabilities, and our data center – and have fashioned this environment to provide state-of-the-art services for research, education, and public service. Our high performance computing infrastructure is ranked as the 66th fastest supercomputer in the world, according to the June 2014 Top500 list[1], and we have been nationally recognized for building models that assist faculty, staff, and students in utilizing this infrastructure for research productivity.

Before coming to Clemson, I was the first Chief Information Officer at Purdue University, where I forged a new model for partnering with research (as recognized in a publication by the EDUCAUSE Center for Analysis and Research, 2005)[2]. Prior to this, I was the Executive Director at the National Center for Supercomputing Applications at the University of Illinois at Urbana-Champaign. I currently serve or previously have served

on a number of national committees, including the National Science Foundation's Advisory Committee on Cyberinfrastructure and the Internet2 Board of Trustees. I also currently serve as Internet2's Inaugural Presidential Fellow.

Introduction

On September 22, 1989, Hurricane Hugo made landfall on the coast of South Carolina just north of Charleston, as a Category 4 storm with estimated winds of 135 miles per hour or higher[3]. In addition to the impact of the high winds brought onshore by the storm, Hugo produced the highest storm tide ever recorded along the East Coast, and was the strongest storm to make landfall in the United States compared with the previous 20-year period[3]. Mainland damages from this storm were estimated at approximately $7 billion, and impacts were felt from Puerto Rico all the way through Pennsylvania[3].

In this, or even with storms not as powerful as Hurricane Hugo, it is of paramount importance that our localities, state, and nation are adequately prepared from not only an evacuation and emergency preparedness standpoint, but from an infrastructure point of view. However, there are **other considerations outside of natural disasters that have the potential to be even more catastrophic in their impact** – not necessarily through withstanding physical damage, but rather potential **economic and societal damage that could be associated with a hacking of our nation's infrastructure.**

This presents a significant threat to our national security, our ability to serve citizens with basic services, and our economic status. In today's technology environment, this threat is more prevalent than ever with our increased reliance upon technology and its associated infrastructure. Another threat, in addition to the offensive nature of the hacking threat, is our nation's cybersecurity expertise gap – one that has implications for our ability to defend our nation's critical infrastructure assets against these attacks. Our preparedness for the future depends upon our conscious planning for capacity in cybersecurity research and education, and in equipping the next generation of cyber-practitioners with the tools, techniques, and learning opportunities needed to ensure we have a cyber-ready workforce.

A shift from the notion of natural disasters to one of man-made origins also requires a broadening of our understanding and planning for such emergencies. Rather than following the traditional model found with hurricanes – one that often relies upon advance public notice and evacuation plans – cyberattacks that take down infrastructure can come with little to no advance warning, and with little to no time to deploy real-time emergency management plans. Natural disasters also generally have the most significant damages confined to a single, relatively small geographic area, whereas a cyberattack on critical infrastructure has the potential to affect the entire nation simultaneously. It is imperative that we understand the shifting paradigm from known threats to potentially unknown threats, and their ability to affect the way we prepare and respond to disasters.

State of Information Technology in 1989

Those who remember 1989 likely remember it much devoid of common technology – or

at least to those who were not involved in its development at this point in history. Computers were slow, expensive, and applications were left mostly to large corporations and the federal government. Networks were in a far different paradigm, with TCP/IP – the bedrock of modern Internet communications protocols – becoming the protocol standard for the ARPANET in 1983[4]. Mobile communications were virtually non-existent in this era, and mobile communication devices were far from a consumer good.

In 1989, technology was far from ubiquitous as it is today, and was primarily in the background of everyday life. During this year, Intel released the 80486 microprocessor which boasted a 64-bit floating-point unit with a clock rate of 33MHz[5] – this compared with Intel's latest processor (the Intel Xeon Phi) with a clock rate of an individual core reaching 1.238 GHz[6]. In this, we've witnessed a massive scaling concurrent with Moore's Law[7], which states that the overall processing power of computers will double approximately every two years.

Aside from computing capabilities in 1989, the Internet as we know it today did not exist. In 1985, the National Science Foundation funded the NSFNet, a 56 kilobit-per-second link between the San Diego Supercomputer Center, the National Center for Atmospheric Research, the National Center for Supercomputing Applications, the Pittsburgh Supercomputing Center, the Cornell Theory Center, and the John von Neumann Computer Center. This network was originally intended to be a backbone for other networks rather than used for connecting individualized systems, and in 1989, this backbone was upgraded to T1 – or 1.544 Mbps[8]. The average citizen in 1989 had no home network access and was much more likely to not have a device that had the ability to connect to any communications network.

Mobile devices were also not prevalent in 1989. Qualcomm, a leading mobile device manufacturer during the 1990s, made its first CDMA-based phone call during a demonstration in San Diego, California on November 7, 1989[9]. Prior to this, CDMA technology had been primarily used by the United States military for secure communications[9]. Mobile technologies until this point had been proprietary or protected, and this move marked the beginning of a shift toward more open mobile communications. However, in 1989, virtually all telecommunications were done through a wired device – making mobile communications an effective unknown to the general population at the time.

From a cursory glance at the history of computing and networking, one can deduce that in this time, cyberinfrastructure, and the relevant technologies that make up such a term, was not as heavily relied upon as it is today for critical functions such as banking, public services, emergency management, and communications. This has far-reaching implications in that **we as a nation today are far more reliant upon technology and communications infrastructure than we ever have been, and this necessitates resilient, reliable, and high performance cyberinfrastructure.**

State of Information Technology in 2014

In our time, technology has become the backbone that even the most basic functions of society depend upon on a daily basis. According to a study by Javelin Strategy & Research in 2012, only 27 percent of all retail point-of-sale purchases were made with cash, versus an estimated 66 percent of purchases being made with a credit or debit card[10]. These credit or debit card transactions depend upon secure networks for processing, whereas with cash payments, only a secure cash repository was required.

Further, according to the United States Census Bureau in 2013, an estimated 83.8 percent of all households in the United States reported computer ownership, and 74.4 percent of all households reported using the Internet[11]. This is in stark contrast to the state of technology proliferation in 1989, and has profound impacts on the way technology has integrated into our daily lives. Individuals are now reliant upon personal computers and a connection to the Internet for activities such as online banking, tax preparation, bill payment, e-mail communications, and news. This shift effectively dictates that our nation's emergency preparedness depends upon, in large part, to the availability and security of communications infrastructure components that enable access to the Internet.

Our nation's network backbone has grown in sharp contrast to the capabilities found in 1989, with the US-UCAN and Innovation Platform project currently delivering up to 100 Gb/s connectivity to research and education sites around the nation through Internet2[12, 13]. Also, unlike the network of 1989, millions of personal devices are now connected to the Internet, and range from personal desktop and laptop computers to mobile phones, automobiles, and even refrigerators. In this new paradigm, protection of and access to high-speed, high-availability networks is necessary not only for corporations, government agencies, and utility providers, but for the average consumer in order to meet the demands of today's world.

Mobile devices have now become the norm for point-to-point communications. According to CTIA, a communications industry trade group, nearly 90 percent of households in the United States use wireless service, and an estimated 40% of adults in the United States live in a wireless-only household[14]. This, coupled with the recent revelation that the number of mobile phones in the United States recently eclipsed the totality of the U.S. population, reveals that the general population is heavily reliant upon mobile devices for communication with the outside world. A recent exposé by NBC's *The Today Show* captured in photographs what amounts to a monumental shift in the adoption and use of mobile technologies through a visual depiction of the differences from a papal event in 2005 to another in 2013[15]. These photos are referenced as Appendix A.

Our nation's infrastructure is now also heavily dependent upon computerized systems and network interconnections for the delivery of basic services to the population. This dependency comes with the risk of vulnerabilities to the communications components of these systems, and the risk of unauthorized entities gaining access to the control mechanisms found within these systems. The U.S. Government Accountability Office, in

its 2012 report entitled "*Cybersecurity: Challenges in Securing the Electricity Grid*," said that the nation's power infrastructure suffers from a lack of security features consistently built into smart grid systems, and that the electricity industry as a whole did not have metrics for evaluating cybersecurity[16]. This, coupled with an inevitable rise in computerized systems for oil and gas delivery, water and sewer services, and traffic control mechanisms makes a clear case for the need for comprehensive planning with regard to protecting the computer systems that our national infrastructure relies upon.

With this increased reliance upon technology and computer systems to drive our country's critical infrastructure, **the next major disaster we face may not be a natural disaster, but rather a cyber-disaster as a result of a catastrophic cyberattack.** For that, Mr. Chairman, I believe we as a nation are not adequately prepared. Fundamental shifts in both the way we prepare for a cyber-disaster and the way we defend against such an attack are needed for us to better protect our national security interests and ensure our systems, networks, and overall population are prepared for the potential occurrence of such an event.

Case Study: Hurricane Katrina's Effect on IT Infrastructure

Perhaps the greatest test of our emergency preparedness for a large-scale natural disaster's impact on information technology infrastructure occurred with Hurricane Katrina's landfall in New Orleans in 2005. Flooding quickly became the paramount concern as the levees around New Orleans could not withstand the storm surge, and one representative from the American Society of Civil Engineers called this "the worst engineering catastrophe in U.S. history[17]." Exposure to water causes most IT components to cease to function, and this was the case with many computing and networking centers across the greater New Orleans area during the aftermath of Katrina. In addition to the impacts on the computing infrastructure, Hurricane Katrina virtually shut down transportation networks and reliable telephone communications within the 504 (New Orleans) area code[18].

According to a study released in the *American Behavioral Scientist* journal on the sociological implications of a post-Katrina New Orleans, the study cited that "*in the confusion of the massive evacuations from the New Orleans area, families and friends lost track of one another. Few evacuees had expected to be gone for more than a day or two. They did not make arrangements to contact one another, and they had no information on the whereabouts and well-being of their families and friends for days afterward*[19]."

Tulane University in New Orleans sustained an estimated $200 million in damages associated with the disaster, and was forced to cancel classes for the remainder of the Fall 2005 academic semester[20]. This proved for the higher education community that traditional notions of disaster planning and business continuity were false; a campus could not effectively shift its entire operation to a remote-access system for distance learning and maintain normal business operations "on-demand." The disaster affected Tulane's ability to not only serve its students in an academic context for the remainder of

the semester, but to facilitate payroll or run their email system[21].

Healthcare infrastructure also sustained critical damage – outside of primary damage to physical medical facilities, some systems containing electronic medical records (EMRs) also became inoperable (due mainly to either flooding or lack of power) and many Katrina evacuees did not have paper copies of their medical records when they left the city. This presents a major challenge in healthcare delivery in a major disaster, and efforts are underway to ensure more seamless exchanges of health information to better prepare for disasters in the wake of Katrina's lessons[22].

Katrina taught us many lessons on the impact a disaster can have on our technology-dependent world, and these impacts are still being studied and modeled today. What Katrina did show our nation, however, is that we still have strides to make in our disaster planning and emergency management efforts.

Cyber-Disasters – How Do We Prepare?

Natural disasters, such as the one experienced with Hurricane Katrina, can often be scoped in advance of their arrival to assess the potential impact of the event, and to deploy the proper evacuation and emergency protocols necessary to prevent loss of life. However, with cyber-disasters, the scope can be unknown, and with this, the scale of the impact unknown. This leads to a need for a greater understanding of the potential impacts of such a disaster, and how the nation's emergency management divisions develop plans for maintaining order and facilitating recovery.

Mr. Chairman, I would submit that in the most hurricane-prone areas of our nation, most residents understand the implications of an evacuation plan and emergency managers in these areas are well versed in the procedures that are associated with ensuring the area is adequately prepared for a storm. However, **I do not believe this nation is adequately prepared for a potential cyber-disaster that affects the operation of infrastructure such as power, banking, or telecommunications.**

One primary example comes to mind – our power infrastructure – that demonstrates our need to become more vigilant in defending against the potential for a large-scale attack in these areas.

Power Infrastructure

The state and security of our power infrastructure has perhaps been the most researched of these topics, and with that comes some startling revelations about our state of preparedness for a large-scale attack in this area. According to a National Research Council report, entitled *Terrorism and the Electric Power Delivery System*, "if carried out in a carefully planned way, by people who knew what they were doing, such an attack could deny large regions of the country access to bulk system power for weeks or even months[23]." While the report goes on to say that a cyber-attack on the grid would be unlikely to cause extended outages, this is not to say that such an outage could not occur,

and could potentially be coupled with a physical attack on the power infrastructure. In a study done for Bloomberg in 2012 by the Ponemon Institute, utility and energy companies surveyed said that they would need an average annual budget of $344.6 million to reach a level where they could successfully combat 95% of their cyber threats[24]. This represents a nearly 10-fold increase from the current level of $45.8 million[24]. Lawrence Ponemon, Chairman of the Ponemon Institute, a firm that conducts independent research on privacy, data protection and information security policy[25], stated in an 2012 interview with Bloomberg that, "the consequences of a successful attack against critical infrastructure makes these cost increases look like chump change," and that "it would put people into the Dark Ages[24]."

One example of the impact of a power system failure is the blackout that occurred in the Northeast United States and parts of Canada in August of 2003. This blackout affected an estimated 50 million people in Ohio, Michigan, Pennsylvania, New York, Vermont, Massachusetts, Connecticut, New Jersey, and Ontario, Canada, and power was not restored in some parts of the country for up to four days[26]. Consequently, this blackout was primarily initiated by a software failure in an alarm and logging system in the control room of the First Energy Corporation[26].

In a piece documenting the impact of the blackout, CNN reported that "the outage stopped trains, elevators, and the normal flow of traffic and life[27]." In Michigan, the population's water supply was affected because of the system's dependence on electric pumps, and Amtrak stopped all trains leaving the New York City area as well as in Michigan between Detroit, Dearborn, and Pontiac[27]. The blackout also affected airports, communications networks, fuel pumps, and traffic signals.

The 2003 blackout shows us how dependent we are upon a readily available and reliable power supply to perform daily functions – and how quickly the failure of a computerized system can wreak havoc on a region's power availability. This incident's total cost was estimated at between $4 billion and $10 billion in the United States, and approximately $2.3 billion in Canada – where the nation's gross domestic product was down 0.7% for the month of August[26]. This impact suggests that not only do our systems and much of the remainder of our infrastructure rely on power, but our entire economy also relies upon this resource as a critical component.

Power is the necessary backbone upon which virtually all information technology systems operate, and a reliable power supply is always a primary consideration in systems-level disaster planning. Perhaps most close to me is the great lengths to which we have gone at Clemson to ensure we adequately plan for any *temporary* power failures and keep our systems operational for our customers. We have developed a state-of-the-art data center and computing facility that houses our enterprise systems including our student information system, payroll and finance systems, and our learning management system for the campus. We also house the campus' high performance computing system, and run the system responsible for the State of South Carolina's Medicaid eligibility and claims processing system. A temporary power failure, one lasting less than a full 24-hour day, has been modeled using our existing uninterruptible power supply (UPS) and

generator capacity, and it is estimated that with our current load, Clemson could operate its systems for approximately 38 hours on both generators, and 46 hours on a single generator. This is critical for business continuity for Clemson's operations – and for the state's Medicaid system to operate without service interruption.

Coupled with the potential threat of a power loss, **we need to increase the importance of robust disaster recovery and business continuity (DR/BC) planning for our state and nation, especially for government-operated systems.** Clemson is currently relatively well positioned in its environment, but our need for real-time, reliable disaster recovery and business continuity is ever-growing, and our reliance upon electronic messaging (e-mail), electronic payroll systems, and healthcare systems show no signs of decreasing. Aside from implications of a power loss, DR/BC plans are important for a wide variety of reasons – to include system hardware or software failures, data backups, or disaster events that affect other necessary functions of the primary site.

With the advent of cloud technologies and the potential cost-savings associated with their adoption through leveraging shared investments, DR/BC planning in the cloud computing environment should be considered as a mechanism for ensuring minimum technology, system, and distance requirements are met while also maintaining a reasonable cost. With any provider of these services, however, there are considerations for the real-time nature of a system's ability to transfer locations with minimal service loss, and a remote site's ability to run the critical systems of the company, agency, or campus. As discovered with the Tulane University example during Hurricane Katrina, generally accepted notions of disaster recovery and business continuity plans can be challenged by the relative unknown any disaster brings, and it is important to continually test these plans in as-close-to production environments as is feasible.

Implications for Data Security

Aside from risks associated with our basic infrastructure being compromised, perhaps another paramount risk is the loss or disclosure of critical data due to either inadequate security protocols or human error. In the era of "big data," it becomes increasingly important to protect our most valuable data from external threats. According to IBM, in 2012, nearly 2.5 exabytes of data were created on a daily basis and as storage density increases, coupled with declining storage costs, this is only expected to grow[28]. Likewise, as computing devices such as phones and portable tablets continue their penetration into all aspects of society, it is increasingly likely that these devices will contribute to an exponential rise in data storage needs.

This presents a two-fold problem for ensuring the security of data and the underlying computing infrastructure on which it is stored. First, ensuring that proper security controls are applied to the data itself to prevent unauthorized access, use, or disclosure is of paramount importance, and second, to protect the infrastructure from growing ubiquity of these devices' need for access. Authorized users and consumers are not only demanding more connectivity to resources, but our economy has become increasingly dependent on the ability to communicate in real time or in near real-time. As our

dependence on this real time need for data escalates for personal devices as well as for economic and national security needs, so does the valuation and susceptibility of the data itself.

In a 2013 report published by PandaLabs, nearly 20% of all malicious code ever to be in circulation (known as malware) was created during the year 2013[29]. This means that nearly 82,000 pieces of new malware were created each day during 2013[29]. Many of these malicious codes are designed to compromise computing systems in order to release or provide access to sensitive data stores. While many cybersecurity-related events may be targeting the infrastructure for purposes of interruption of services, most cyber criminals will be attempting to acquire or compromise sensitive data for personal or nation-state advantages. It is becoming increasingly clear with each newly published report in this space that several nations are engaging in cyber-warfare. Some of these operations are covert for purposes of privileged data acquisition, and others for purposes of activities such as the accusations levied against Russia prior to the Georgian invasion in 2008[30].

Clemson University takes the threat of a possible cyber-attack as legitimate and real on a continual and daily basis. After joining Clemson University in 2006, one of the first actions I took was to create an Office of Information Security and Privacy to oversee the security and privacy activities of the university. From my experience in previous positions, I identified this is an immediate and critical need for the University. Securing computing systems and data in higher education has its own set of unique challenges commonly not found in other industries, but still faces similar threats. Universities, in general, are under attack daily due to the open nature of higher education, the vast amounts of computing infrastructure used by a wide variety of users, and the large volumes of intellectual property created by researchers. Also, taking into account all of the personally identifiable information, financial information, and health care data created and consumed by typical universities, it is clear why these institutions become very large targets for cyber criminals.

To protect all of this data and infrastructure, Clemson University employs many industry-accepted practices to prevent not only unauthorized intrusion into protected spaces, but to also avoid any interruption in services. Clemson's Computing and Information Technology organization also has a dedicated 24/7 Network Operations Center (NOC) for all network monitoring and operations. Mission-critical systems are consistently scrutinized for security-related concerns before, during, and after deployment and network activity is monitored for anomalies. We undergo numerous internal and external audits administered by both state and federal agencies annually where processes, systems, and facilities are evaluated.

With this, it has become more important than ever for organizations to have a primary focus on protecting their information technology infrastructure and data from potential cyber criminals. In today's world, no enterprise, agency, or entity is exempt from attack; in fact, even individuals should employ appropriate practices to ensure their personal data is not compromised.

An Eye Toward The Future

Given the multitude of potential threats, our nation must be vigilant in our actions to prepare for the future. I would therefore submit, Mr. Chairman, that **in order for our nation to be prepared to defend against cyber-disasters and other cyber-threats, we must invest in the future of cybersecurity research, education, and training to prepare the next generation workforce.** This is vital to ensuring that our nation remains secure, competitive, and sustains our position as a world leader on the global stage. At Clemson, one industry partner has expressed to us that there are points in time where the company will have up to 300 open cybersecurity-related positions without enough qualified applicants to fill them. I fear our nation faces an upcoming crisis in our cybersecurity workforce if investments are not made to encourage this career path and to ensure robust education and training programs at our nation's universities.

Additionally, in order to protect the security of data in our age, more efforts are needed in the area of secure application development, as security must start within the application itself. In general, we are not adequately educating the next generation of programmers in the development of secure code or secure code development principles. We will likely continue to see common applications that we have become dependent upon for daily use becoming vulnerable over time as weaknesses are discovered.

Earlier this year, the commonly used OpenSSL cryptographic software library was discovered to have a critical vulnerability referred to as the Heartbleed bug[31]. OpenSSL was used to provide for the security of data and communications in many devices and systems. This discovered vulnerability would allow an attacker to have access to information that ordinarily would be protected by Secure Socket Layer/Transport Layer Security (SSL/TLS) encryption protocols. This oversight in programming required many in the computing industry to have to take production systems offline, evaluate all of their systems for applicability, and then spend days to weeks of remediating the issues – including revoking and re-issuing all new certificates on their servers once all vulnerability patching was complete.

In 2008, the Comprehensive National Cyber-Security Initiative (CNCI) identified 12 initiatives to combat the threats that cybersecurity has to our economy and national security[32]. In response to Initiative 8 from the CNCI's charge – the need to expand cyber education – Clemson University and the information technology division have dedicated resources to help combat this shortage in cybersecurity practitioners.

One program at Clemson is the Cyber-infrastructure General Practitioner Program (NSF Award 1251544), where rather than becoming cyberinfrastructure (CI) users with limited skill sets, we intend to help students become innovative and productive CI "general practitioners" by providing participating undergraduate and graduate students with the critical broad perspective of CI needed to make the best decisions and make best use of available resources. These experiences primarily take the form of Creative Inquiry[33] courses that are added to (or substituted into) a student's regular course curriculum for his/her major. Once a student has demonstrated proficiency in a particular area, we work

to find internship activities or projects sponsored by the IT organization or by one of our many commercial partners.

A second program at Clemson is designed to provide an immersive educational experience for those looking for a career in the information security field. Currently, there is an information security student organization at Clemson where students, advised by members of the Office of Information Security and Privacy, compete in both state and national competitions. Many of these students, and others from across the University, are currently taking security-related undergraduate courses offered by the University, but a gap exists in applications of operational security. Set to open in the spring of 2015, we will have a dedicated, student-centered Security Operations Center (SOC) on campus designed to employ students through official university internships and partner them with our Information Security and Privacy Office.

During the day, all operational security needs and incident responses will be maintained by the SOC and between operational needs, the students will be taught real-life skills in penetration testing, audits, compliance, and risk assessment. Industry-accepted practices and tools will be used to provide these students with demonstrable skills to make them competitive in the workforce. We have engaged public and private industry partners who will be participating in this program and they have identified this a great need for them to fulfill their future staffing needs in this space.

Even with these efforts, we as a nation need to collectively make education and training in cybersecurity a priority to keep pace with the growing demand of professionals in this area. A workforce that is capable of preparing and protecting our infrastructure is paramount, and much like the probable future medical doctor shortage this nation is facing, if we do not begin to provide the education and training to those who will be tasked with protecting our infrastructure, the vulnerabilities we face will continue to grow without the professionals educated to protect it.

Conclusion

In conclusion, it is evidenced that as our society has become more reliant upon information technology as a backbone for many of our most important functions as a nation and as an economy, we also have a duty to prepare for a potential disaster that affects these systems. In 1989, information technology took a back-seat role in our society, and that no longer holds true in 2014. Therefore, any major disaster – natural or otherwise – is likely to have a significant impact on our cyberinfrastructure environment, and our emergency preparedness plans must account for this.

Furthermore, increased emphasis is needed on developing robust disaster recovery and business continuity plans for our nation's most critical systems, and to build redundant capabilities that can serve us during these times of crisis. Additionally, I believe we as a nation have progress to make if we are to be prepared in terms of emergency planning – especially for a cyber-disaster – but also in terms of our long-range strategic efforts to ensure a robust and competitive cybersecurity workforce.

Appendix A

Year: 2005
Photo Credit: Luca Bruno, AP
Retrieved from: http://photoblog.nbcnews.com/_news/2013/03/14/17312316-witnessing-papal-history-changes-with-digital-age

Year: 2013
Photo Credit: Michael Sohn, AP
Retrieved from: http://photoblog.nbcnews.com/_news/2013/03/14/17312316-witnessing-papal-history-changes-with-digital-age

References

[1]Top500.org (June 2014). Top500 List – June 2014. Retrieved from http://www.top500.org/list/2014/06/

[2]Spicer, Donald & Metz, Bruce (July 25, 2005). A New Model For Supporting Research At Purdue University. *Educause Center for Analysis and Research (ECAR), Case Study 7*. Retrieved from https://net.educause.edu/ir/library/pdf/ers0605/cs/ECS0507.pdf

[3]National Weather Service – National Oceanic and Atmospheric Administration (n.d.). Hurricane Hugo: 25th Anniversary. Retrieved from http://www.weather.gov/chs/Hugo25thAnniversary

[4]TCP/IP (n.d.). In *Encyclopædia Britannica online*. Retrieved from http://www.britannica.com/EBchecked/topic/602945/TCPIP

[5]Computer History Museum (n.d.). Timeline of Computer History – 1989. Retrieved from http://www.computerhistory.org/timeline/?year=1989

[6]Intel Corporation (n.d.). Intel Xeon Phi Coprocessor 7100 Series. Retrieved from http://ark.intel.com/products/series/75809

[7]Moore, Gordon, Intel Corporation (n.d.). Moore's Law and Intel Innovation. Retrieved from http://www.intel.com/content/www/us/en/history/museum-gordon-moore-law.html

[8]Kessler, Gary (August 5, 1994; Updated November 13, 2014). An Overview of TCP/IP Protocols and the Internet. Retrieved from http://www.garykessler.net/library/tcpip.html

[9]Qualcomm Corporation (n.d.). History – Qualcomm. Retrieved from https://www.qualcomm.com/company/about/history

[10]Javelin Strategy & Research, Greenwich Associates LLC (June 6, 2012). RETAIL POINT OF SALE FORECAST 2012-2017: Cash is No Longer King; Cards and Mobile Payments Likely to Rise. Retrieved from https://www.javelinstrategy.com/brochure/251

[11]File, Thom and Ryan, Camille (November 2014). Computer and Internet Use in the United States: 2013. U.S. Department of Commerce Economics and Statistics Administration, U.S. Census Bureau. Retrieved from www.census.gov/prod/2013pubs/p20-569.pdf

[12]Internet2 (n.d.). Innovation Platform. Retrieved from http://www.internet2.edu/vision-initiatives/initiatives/innovation-platform/

[13]Internet2 (n.d.). U.S. UCAN. Retrieved from http://www.internet2.edu/vision-initiatives/initiatives/us-ucan/

[14]CTIA – The Wireless Association (n.d.). Wireless Quick Facts. Retrieved from http://www.ctia.org/your-wireless-life/how-wireless-works/wireless-quick-facts

[15]Dellaverson, Carlo. (March 14, 2013). Witnessing Papal history changes with digital age. *NBC News Photo Blog*. Retrieved from http://photoblog.nbcnews.com/_news/2013/03/14/17312316-witnessing-papal-history-changes-with-digital-age

[16]Wilshusen, Gregory (July 17, 2012). Cybersecurity: Challenges in Securing the Electricity Grid. Retrieved from http://www.gao.gov/assets/600/592508.pdf

[17]Roth, Lawrence (n.d.). The New Orleans Levees: The Worst Engineering Catastrophe in U.S. History – What Went Wrong and Why. Retrieved from http://biotech.law.lsu.edu/climate/ocean-rise/against-the-deluge/01-new_orleans_levees.pdf

[18]Morrow, J.J. (n.d.). Hurricane Preparedness After Action Review. Retrieved from www.tulane.edu/.../Hurricane_Katrina_After_Action_Critique.ppt

[19]Shklovski, Irina; Burke, Moira; Kiesler, Sara; and Kraut, Robert. (February 18, 2010). Technology Adoption and Use in the Aftermath of Hurricane Katrina in New Orleans. *American Behavioral Scientist, XX(X)-I-19*. Retrieved from *http://www.cs.cmu.edu/~kiesler/publications/2010pdfs/2010Shklovski.pdf*

[20]Pinto, Barbara (December 9, 2005). Katrina Wallops Tulane University. *ABC News*. Retrieved from http://abcnews.go.com/US/HurricaneKatrina/story?id=1390382

[21]Cowen, Scott (September 3, 2005 and August 30, 2005). Previous Messages from President Cowen – Tulane University. Retrieved from http://www.tulane.edu/past.html

[22]United States Department of Health and Human Services (July 11, 2013). States prepare for seamless exchange of health records after disasters. Retrieved from http://www.hhs.gov/news/press/2013pres/07/20130711a.html

[23]National Research Council (2012). *Terrorism and the Electric Power Delivery System*. Washington, DC: The National Academies Press. Retrieved from http://www.nap.edu/catalog.php?record_id=12050

[24]Engleman, Eric and Strohm, Chris (January 31, 2012). Cybersecurity Disaster Seen in U.S. Survey Citing Spending Gaps. *Bloomberg News*. Retrieved from http://www.bloomberg.com/news/2012-01-31/cybersecurity-disaster-seen-in-u-s-survey-citing-spending-gaps.html

[25]Ponemon Institute (n.d.). Ponemon Institute – Why We Are Unique. Retrieved from http://www.ponemon.org/about-ponemon

[26]U.S.-Canada Power System Outage Task Force (April 2004). Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations. Retrieved from https://reports.energy.gov/BlackoutFinal-Web.pdf

[27]CNN News (August 14, 2003). Major power outage hits New York, other large cities. Retrieved from http://www.cnn.com/2003/US/08/14/power.outage/

[28]IBM Corporation (n.d.). Demystifying Big Data: Decoding The Big Data Commission Report. Retrieved from https://www-304.ibm.com/events/wwe/grp/grp004.nsf/vLookupPDFs/Tim%20Paydos'%20Presentation/$file/Tim%20Paydos'%20Presentation.pdf

[29]Udemans, Chris (April 14, 2014). 20% of malware generated in 2013 – PandaLabs. Retrieved from http://www.humanipo.com/news/42720/20-of-malware-generated-in-2013-pandalabs/

[30]Markoff, John (August 12, 2008). Before the Gunfire, Cyberattacks. *The New York Times*. Retrieved from http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1&

[31]Kirk, Jeremy (April 8, 2014). Critical OpenSSL Heartbleed bug puts encrypted communications at risk. *PCWorld*. Retrieved from http://www.pcworld.com/article/2140920/heartbleed-bug-in-openssl-puts-encrypted-communications-at-risk.html

[32]The White House (n.d.). The Comprehensive National Cybersecurity Initiative. Retrieved from http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

[33] Creative Inquiry (n.d.). Creative Inquiry and Undergraduate Research. Retrieved from http://www.clemson.edu/academics/programs/creative-inquiry/