Critical Infrastructure Protection

Kris Hemme

Submitted in Partial Fulfillment of the Requirements for

INSS 5390

Capstone INSS

Dr. Misty Duke

University of Texas at El Paso

December, 5th 2014

U.S. critical infrastructure protection (CIP) necessitates both the provision of security from internal and external threats and the repair of physically damaged critical infrastructure which may disrupt services. For years, the U.S. infrastructure has been deteriorating, triggering enough damage and loss of life to give cause for major concern. CIP is typically only addressed after a major disaster or catastrophe due to the extreme scrutiny that follows these events. In fact, CIP has been addressed repeatedly since its inception in Presidential Decision Directive – 63 (PDD-63) signed by President Bill Clinton on May 22, 1998 (Clinton, 1998). This directive highlighted critical infrastructure as "a growing potential vulnerability" (Clinton, 1998, p. 1) and recognized that the United States has to view the U.S. national infrastructure from a national security perspective due to its importance to national and economic security. CIP must be addressed in a preventive, rather than reactive, manner. As such, there are sixteen critical infrastructure sectors, each with it's own protection plan and unique natural and man-made threats, deteriorations, and risks. A disaster or attack on any one of these critical infrastructures could cause serious damage to national security and possibly lead to the collapse of the entire infrastructure.

Since PDD-63 in 1998, policymaker attitudes toward CIP have evolved from being largely indifferent to recognizing the multiple man-made and natural threats to CIP, resulting in production of the National Infrastructure Protection Plan of 2013 (NIPP 2013,) which is described as, "...streamlined and adaptable to current risk, policy and strategic environments… and provides the foundation for an integrated and collaborative approach to achieve a vision of: A nation in which physical and cyber critical infrastructure remain secure and resilient..." (NIPP 2013: Partnering, 2013, p. 1). This evolution of policy has allowed CIP to reach a point at

which it is self-sufficient and flexible in addressing threats through regular quadrennial evaluations of CIP strategies. However, even though it is clear that the United States has the capabilities to address threats through flexible policy, research into past and recent disasters involving critical infrastructure indicates that the Department of Homeland Security (DHS) and each Sector Specific Agency (SSA) has not heeded previous threats and warnings regarding the potential consequences of poor maintenance, opting, instead, for a more aggressive effort towards preventing terrorist threats. This likely results from policymakers' awareness of the political capital gained through terrorism prevention that is largely absent from calls for resources to be spent on maintenance of infrastructure.

Assessments of the state of U.S. critical infrastructure. Assessments of U.S. critical infrastructure have generally indicated that, up until February 2013, there was no unified effort to protect the interrelated aspect of critical infrastructure due to nonexistent consensus on the interrelationships between sectors. This interrelationship between sectors is describes as the interdependencies sectors have on one another (i.e., all critical infrastructure sectors rely on the water and energy sector to provide the necessary power and water to remain operational). However, as explained in a review of the history of government response to CIP by Rourke (2007), the U.S. government has attempted to rectify this problem. CIP improved its defense against and awareness of possible threats posed by man-made disasters after the 1995 Oklahoma City bombings when President Clinton issued Presidential Decision Directive-39, calling for a government-wide evaluation and re-examination of its ability to protect critical infrastructure. As a result, the Attorney General provided an assessment of CIP (U.S. General Accounting Office, 2002) that highlighted the government's lack of attention to multiple

vulnerabilities within the physical infrastructure and to gaps in cyber-infrastructure and computer network protection. Fifteen months after the Attorney General's assessment, recommendations were made by a National Security Advisor-led interagency group, named the President's Commission on Critical Infrastructure Protection (PCCIP), which called for cooperation between the federal government and its private sector partners (U.S. General Accounting Office, 2002). This partnership is essential because the vast majority (approximately 85%) of the nation's critical infrastructure is owned and operated by the private sector (Critical Infrastructure Sector Partnerships, 2014). Ultimately, in February 2013, Presidential Policy Directive – 21 (PPD-21) "Critical Infrastructure Security and Resilience" was signed. The goal of this directive was to strengthen the security and resilience of critical infrastructure and advocate for an updated national framework for its protection (Department of Homeland Security, 2013). The Department of Homeland Security created the Integrated Task Force in order to implement PPD-21 during a nine-month time period starting in March 2013 before returning responsibility back to DHS agencies.

The American Society of Civil Engineers' (ASCE, 2013*)* drew similar conclusions and made similar recommendations as the PCCIP. Every four years ASCE releases a report card on the state of U.S. infrastructure. The latest overall assessment, conducted in 2013, gave an overall letter grade of D+. ASCE recommended improved cooperation and increased investment by the federal government and private critical infrastructure partners. According to the ASCE, it is particularly important to combine the resources of private owners/operators and those of the government that are dedicated to critical threat information, research, and development in order to create an effective defense against threats. This partnership, now

known as the Private Sector Preparedness Coordinating Council (PSPCC), is chaired by FEMA and includes representatives from the Science and Technology Directorate, Office of Infrastructure Protection, and Office of the Private Sector. PSPCC's mission is to oversee the adoption of preparedness standards by the private sector and to promote business preparedness.

The 2013 NIPP is the latest iteration in the U.S. federal government's ever-evolving conceptualization of the protection of critical infrastructure. This document is updated every four years in an effort to maintain critical infrastructure in the face of changing threats and vulnerabilities. The 2013 NIPP meets the requirements set forth by Presidential Policy Directive-21 and is analyzed as a benchmark for U.S. policy-related efforts to protect critical infrastructure. Sauter and Carafano (2012) provide reviews of the various threats facing U.S. national security, including current and past threats facing critical infrastructure, as well as a detailed description of the problems each sector is facing in regard to the NIPP. The authors report that the U.S. critical infrastructure, as a whole, consists of physical assets, information systems, and people, while individual sectors include power plants, railroads, hospitals, pipelines and government facilities. In addition, each sector is dependent on the other (i.e., dams provide water for hydroelectric plants, whereas emergency services requires transportation and paved roads). Sauter and Carafano state that there is a key defining difference between resiliency and protection in relation to infrastructure that must be considered when evaluating protection policies. Resilience places an emphasis on the ability to keep systems operating after a catastrophic event, whereas protection refers to security over the entire infrastructure system. Sauter and Carafano also highlight the potential consequences

of cyber-attacks, which can be used for online subterfuge, stealing of information, undermining government confidence, interrupting communication, and disruption and denial of government service. These attacks are capable of disruption and destruction of physical infrastructure. The authors conclude that the key to successful infrastructure policy involves the balance of costs and benefits, which requires weighing security concerns against economic competitiveness. Essentially, the U.S. government has acknowledged that there are problems and gaps in critical infrastructure protection policies and has attempted to remedy these gaps through constant and regular evaluation.

Overview of the current research

The purpose of the current research was to examine the current state of U.S. CIP and SSA effectiveness in implementing SSP's. This purpose was accomplished using the following methods. First, each SSP was evaluated according to how well it has adhered to the basic principles of risk assessment set forth by the 2013 NIPP in fulfillment of PPD-21. It was predicted that the criterion set by NIPP 2013 are sufficient to provide a guidance enabling SSA's to create effective protection plans. SSP's were created to support the NIPP by providing goals, priorities, and requirements for CIP; they facilitate the coordination of effective allocation of funding to reduce vulnerability, deter threats, and minimize the consequences of disasters or attacks. Preliminary predictions also suggested that the NIPP policy has improved in its flexibility in addressing multiple man-made and natural disasters. Second, qualitative data was gathered regarding major critical infrastructure disasters and failures through online searches for credible news sources, academic journals, and government reports. This data was used to evaluate how each SSA responded to the disaster according to its SSP.

Method

This research focused on the following areas of critical infrastructure: vital energy, transportation and public health sectors, all of which comprise roughly half of the U.S. critical infrastructure. Out of the sixteen sectors encompassing US critical infrastructure, the specific sectors examined were the Dams, Energy, Transportation Systems, and Water and Wastewater Systems sectors. This research addresses whether or not the Department of Homeland Security (DHS) has successfully implemented security to protect and maintain the reliance of these sectors. Data was gathered from online government sector status reports and by searching for each sector in conjunction with terminology indicative of failures, disasters, and attacks. More specifically, data was gathered through internet search engines (Google), online academic journal databases (JSTOR, LexisNexis Academic), and national news networks, as well as their affiliates (CNN, MSNBC, CBS, FOX News). Keywords and terms used for searching databases and in search engines included the following: critical infrastructure, critical infrastructure protection, homeland security, presidential directive, NIPP, sector specific plan, sector specific agency, dams sector, water sector, transportation systems sector, food & agriculture sector, energy sector, emergency services sector, success, criticism, threat, disaster, breakage, leak, maintenance.

In order to determine whether or not a report is providing evidence of a “success” or “failure”, attention was paid to how effectively SSA’s identified and responded to critical infrastructure risk. For example, did SSA’s repair or provide security to critical infrastructure prior to a man-made, natural, or maintenance-related disaster?

Searches were limited to the time frame spanning from the year 2003 when the Homeland Security Presidential Directive 7 was signed through the present year, 2014. This is the time period during which the United States has made vast leaps in policy due to events such as the September 11th World Trade Center terrorist attacks. Collected data were analyzed with regard to whether or not each sector specific agency has effectively utilized its SSP to respond to CIP failures or attacks.

Criteria that were used to assess whether or not the SSPs have successfully implemented security to protect and maintain critical infrastructure will be gathered from the National Infrastructure Protection Plan 2013: Sector Specific Plans (DHS, 2013, p. ?),which states:

> SSPs are tailored to address the unique characteristics and risk landscapes of each sector while also providing consistency for protective programs, public and private protection investments, and resources. SSPs serve to:
>
> I. Define sector security partners, authorities, regulatory bases, roles and responsibilities, and interdependencies;
> II. Establish or institutionalize already existing procedures for sector interaction, information sharing, coordination, and partnership;
> III. Establish the goals and objectives, developed collaboratively with security partners, required to achieve the desired protective posture for the sector;
> IV. Identify international considerations; and
> V. Identify the sector-specific approach or methodology that Sector-Specific Agencies (SSAs), in coordination with the Department of Homeland Security (DHS) and other security partners, will use to implement risk management framework activities consistent with the NIPP.

The NIPP 2013 outlines the methods and criteria the government and private sector critical infrastructure partners must work together to handle risks, achieve security and resilience. “NIPP 2013 represents an evolution from concepts introduced in the initial version of the NIPP release in 2006.” (DHS, 2013, p. ?). This evolution of CIP planning demonstrated a streamlined and adaptable approach to risks, policy, and to the strategic environment; additionally, the NIPP fosters and integrated and collaborative approach in its concept evolutions. In order to determine the effective implementation of roles and responsibilities by SSA’s, each SSP must provide evidence through documentation or through preparedness efforts that the corresponding SSA has fulfilled all five criteria set forth by the NIPP 2013.

Results

Dams sector

Certain critical infrastructure sectors interrelate with each other in such a way as to resemble a domino effect in which one sector’s collapse would affect the other sectors associated with its resources. The Dams sector is one such infrastructure; nearly every sector relies on water resources provided by dams. For example, the Emergency Services sector relies on water resources for firefighting water supply, emergency water supply, and waterborne access in the event of a significant disaster. The Energy sector also relies on dams because it provides approximately 8-12% of the nation’s power through the hydropower provided by dams. The Food and Agriculture sector utilizes water resources provided by dams for irrigation and water management. The Transportation Systems sector uses dams and locks to manage navigable water throughout inland waterways. The Water and Wastewater sector relies on the

dam sector assets to provide water to concentrated populations and commercial facilities in the U.S. (Department of Homeland Security: Dams Sector, 2013).

In response to the NIPP 2013 requirements, the Dams Sector Specific Plan (DSSP) was developed to complement the National Infrastructure Protection Plan (NIPP) in order to, "…achieve safer, more secure, and more resilient Dams sector through lessening vulnerabilities, deterring threats and minimizing the consequences of terrorist attacks, natural disaster, and other incidents." (Conklin, 2010, pg. *i*) In order to fulfil Criterion I and II of NIPP 2013, DSSP formed the Dams Sector Coordinating Council (SSC), Levee Sub-Sector Coordinating Council (LGCC), and the Dams Sector Government Coordinating Council (GCC) to address levee protection and resilience issues and cross-sector connections, enhance collaboration with state dam safety offices, and implement information-sharing operating procedures. DSSP clearly outlined its future goals and objectives within its 2010 report and has developed a cybersecurity framework which fulfills NIPP 2013 Criterion III. Criterion IV & V have been fulfilled through the development of coordinated multi-jurisdictional exercises involving government and private sector assets, and through web-based training modules focusing on crisis management, protective measures, and security awareness relevant to the dams sector (Conklin, 2010).

Overall, it seems the Dams SSP has fulfilled the requirement demanded by NIPP 2013. However, the dams sector has received a grade of D (Poor) from the ASCE "Report card for America's infrastructure." (ASCE, Dams D, 2013). Furthermore, the ASCE stated in their 2013 report that, "the nation's dams are aging and the number of high-hazard dams is on the rise." (ASCE, Dams D, 2013, p. ?). This threat was evident on December 14, 2005 in St. Louis, Missouri

when overtopping water at the Ameren UE Taum Suak storage facility overwhelmed the aging dam and caused massive failure (Witt, 2009). The number of deficient dams is estimated at more than 4,000, including 2,000 deficient high-hazard dams." (ASCE, Dams, 2013) The original purpose of the dams was to protect underdeveloped agricultural land, but a major threat stems from the fact that new developments and an increasing population have turned the agricultural land into urbanized zones. If these dams and levees were to fail there would be catastrophic floods as seen in the wake of both Hurricane Katrina and Hurricane Rita. Unfortunately, only 66% of high-hazard dams have emergency action plans and over 13,000 of those dams are located above population centers, creating a huge risk for potential and possible catastrophic disasters (Costa & Cooper, 2013).

Consequentially, DSSP primarily places responsibility for protecting populations from dam failure on local and state governments, who, in turn, can gain assistance to enhance dams through the Dam Safety Act of 2006. The DSSP is a good start but, in order to improve upon those preventative measures, the ASCE suggests that the federal government reauthorize the National Dam Safety Program, create a national levee safety programand a national dam rehabilitation and repair program, and complete the national levee inventory. This would cost an estimated $121 billion to repair and revitalize the sector (ASCE, Dams D, 2013). Fortunately, new DSSP collaboration is attempting to address issues raised by ASCE and successful prevention was seen at the Big Hole River Diversion Dam in Butte, Montana. In 2009, the century-old Big Hole River Dam was removed and replaced with new concrete intake structures through a project initiated by the City of Butte (DOWL HKM, 2014).

Water sector

The U.S. critical Water and Wastewater sector includes systems that provide freshwater and wastewater collection and management for the nation. There are approximately 160,000 drinking water systems and approximately 16,000 publicly owned wastewater treatment facilities that service the nation at any given time (Sauter & Carafano, 2012, pp. 416). The SSA charged with managing and maintaining the U.S. water systems is the Environmental Protection Agency (EPA), who provides personnel for the management and protection of all water and wastewater systems. DHS states that the water and wastewater sector are, "…vulnerable to a variety of attacks, including contamination with deadly agents, physical attacks such as the release of toxic gaseous chemicals and cyber-attacks…[Resulting] in large numbers of illnesses or casualties and the denial of emergency services vital to public health." (DHS, Water and wastewater systems, 2013, p. ?). To fulfil Criterion I of NIPP 2013, the Water Sector Coordinating Council (WSCC) took on a more proactive approach in its SSP by forming specialized products that unify the sector with the overall NIPP 2010 security strategy, continuing goals, and milestones. The Water Sector created the Nation's first Critical Infrastructure and Key Resource (CIKR) resilience-based security metrics initiative in order to meet Criterion II of the NIPP (Figure 1).

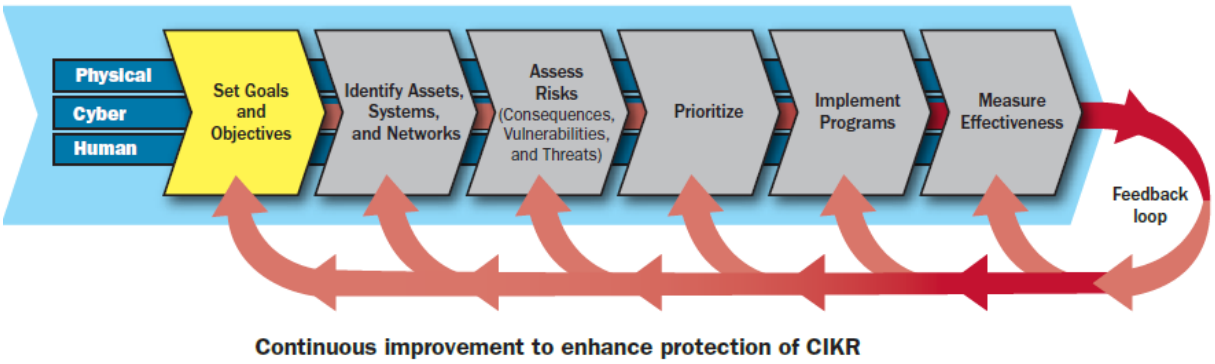

Figure 1 (Broussard, Water Sector Specific Plan, 2010)

The CIKR framework provides a unifying structure for the integration of current and future CIP efforts into a single cross-national NIPP risk management framework. In fact, most SSP's have adopted this framework to fulfill Criterion II of NIPP. The Water and Wastewater sector adhered to Criterion III by establishing Water Security Initiatives in major U.S. cities (Cincinnati, Dallas, New York City, Philadelphia, and San Francisco) and using information gathered from the initiatives to publish three temporary guiding documents to advise utilities on the design, development, deployment, and use of contaminant monitoring and warning systems. (Broussard, 2010). The Water and Wastewater sector responded to NIPP Criterion IV, which requires consideration of international issues by promoting, developing, and establishing intrastate mutual aid and assistance agreements. One example of an agreement is the Water and Wastewater Agency Response Network comprised of over 47 states with a mutual aid agreement to promote a "utilities-helping-utilities" approach to response and recovery. NIPP Criterion V requires SSP's to coordinate with DHS and its security partners. The Water Sector has complied with this criterion by establishing a regional laboratory under the Environmental

Protection Agency (EPA). Although the Water sector SSP has managed to fulfill all NIPP criteria, the ASCE's 2013 Infrastructure report card gave the water and wastewater sector a grade of D ("poor") due to the century-old water pipelines and water mains that result in over 240,000 water main breaks per year (ASCE, Drinking Water D, 2013). One such water main break happened on July 30, 2014 in the midst of a drought in Los Angeles, California. A 30-inch, 93 year old pipe burst under Sunset Boulevard near the University of California, Los Angeles (UCLA) campus, trapping 5 individuals and costing millions of dollars in damage to streets and nearby buildings (Hamilton, 2014). This is one example of water main damage in a country with more than one million miles of water mains, some dating back to the Civil War; the condition of most of these mains is unknown. However, there are some examples of progress, such as in the City of Chicago, which has been steadily replacing more than 30 miles of century-old water mains per year (Mihalopoulos, 2011). Proper planning and management has allowed the City of Chicago to finance the projects and, possibly, upgrade the systems.

Laboratory Alliance program.

An additional problem with this sector concerns wastewater systems, which require maintenance and expansion of pipelines to address sanitary sewer overflows, combined sewer overflows, and other pipe-related issues (ASCE, Wastewater D, 2013). This relates to DHS's concerns of contamination, in which aging treatment plants with inadequate capacity discharge an estimated 900 billion gallons of *untreated* sewage each year into freshwater sources that are used to provide water to the nation. The Water and Wastewater sector, like the Dams sector, is highly interrelated with other sectors, meaning that damage to this sector can have consequences for other areas of critical infrastructure.

It is possible to achieve water infrastructure security through the four steps suggested by ASCE: 1) raise awareness regarding the true cost of supplying clean, reliable drinking water and encourage strategies for water conservation; 2) revive the State Revolving Loan Fund under the Safe Drinking Water Act and Clean Water Act, which would reauthorize federal funding to a minimum of $20 billion over five years giving the Water sector the necessary funding for maintenance and security; 3) eliminate the cap on private bonds for water infrastructure projects in order to increase private financing and support; and 4) establish water investment programs and a federal water infrastructure trust fund to provide financial support for the burden of repair (ASCE, Drinking Water D, 2013). All steps are currently being addressed by the Water and Wastewater SSP and are outlined in Goals 1-4 (Broussard, 2010, pp. 16-18). The complete repair and investment costs for improving the Water and Wastewater sector is approximately $633 billion and rising, which means that the threats to this sector are growing slowly despite DHS efforts.

Transportation System sector. The transportation system efficiently and securely transports goods and people through the country and overseas. It consists of seven subsectors: Aviation, Highway Infrastructure, Maritime Transportation System, Mass Transit and Passenger Rail, Pipeline Systems, Freight Rail, Postal and Shipping (DHS, Transportation Systems Sector, 2013).

These subsectors are vital to the transportation sector, as well as to other vital critical infrastructure sectors. The Transportation System sector is immense, consisting of 450 commercial airports, 4 million miles of roadways, 10,000 miles of navigable waterways, mass transit systems, 143,000 miles of train track and more. It is managed by three cooperating

agencies responsible for travel and entry to the U.S. by land, sea, and air; these SSA's are Transportation System Administration (TSA), the U.S. Coast Guard (USCG) and the Department of Transportation (Sauter & Carafano, 2012,). This research evaluates the Highway Infrastructure sub-sector (bridges, roads, and transit). Criterion I is addressed by the SSA's in charge of the Transportation Systems sector through the inclusion in the SSP of a Managing and Coordinating model, which outlines the three SSA's and their roles, individual duties, and cooperative duties (Sammon, 2010). Criterion II & IV are fulfilled throughthe Transportation security SSP's adoption of the CIKR risk management model developed by the water sector. In addition providing a unifying structure, CIKR has allowed Transportation System SSA's to formulate a cooperative risk management framework internally and across national NIPP sectors. The Transportation System SSP lists all objectives and goals for immediate and long-term plans within its 2010 report, as well as details on how the SSA's will carry out their goals (Sammon, 2010). For Criterion IV, all three SSA's, USCG, TSA, and DOT, have identified international considerations when dealing with immigration, imports, exports, and travel between states and countries.

The potential risks and threats to the transportation sector are varied in spectrum from problems caused by infrastructure disrepair to terrorist attacks, such as the 9/11 World Trade Center attack in New York. As with the dams and water sectors, many critical infrastructure sectors are interrelated with the transportation sector and its function to move people and goods in mass quickly and securely. The ASCE's 2013 Infrastructure Report Card gives the transportation sector a C+ (”mediocre”) for bridges, a D (“poor”) for roads, and a D (“poor”) for transit systems (ASCE, Bridges C+, 2013; ASCE, Roads D, 2013; ASCE, Transit D, 2013).

Forty-two percent of the nation's major urban highways are congested daily which costs $101 billion in lost time and fuel annually, while nearly 11% of the nation's bridges are considered structurally deficient (ASCE, Bridges C+, 2013). From 2012 to present, Los Angeles has been judged to be the U.S. city highest in traffic gridlock in the United States. Vehicles in L.A spend a cumulative 6.6 million extra hours on the road due to heavy traffic costing millions to the state economy (Pritchard, 2014). These examples indicate how much time can be lost on congested highways across the nation, potentially hampering multiple critical infrastructures from fulfilling their operational goals. For example, if there is constant gridlock in a city, it would obstruct emergency response personnel and medical personnel comprising the Emergency Services sector.

Nationwide, during the 1950's to 1970's most bridges were constructed through the Interstate Highway System and were with cheap and easy-to-build material (Lowy & Baker, 2013). Interstate Highway System bridges were meant to be erected quickly and were designed to last approximately 50-60 years; however, most bridges are passing their 50-year expiration date, resulting in the potential for collapse. For example, the Mount Vernon, Washington I-5 bridge collapsed into the Washington River after a semi-truck collided into it (Valdes, 2013). In response to these threats, the Oregon Legislature passed the Oregon Transportation Investment Act in 2003 which increased priority of the state's bridge program. Although it cost $1.3 billion, it saved the state an estimated $123 billion in potential lost production that would result from collapsed bridges. ASCE concluded that the only long-term remedy to the deterioration of the bridges subsector is to develop a national strategic plan that addresses

structurally deficient and functionally obsolete bridges, followed by research into making bridges more structurally resilient (ASCE, Bridges, 2013).

In the Transit subsector, over 55% of U.S. households have access to the transit system (e.g. metro rail systems, taxis, city buses) and, of that the percentage that have access, there was an increase in metro usage by 9% in the past decade, despite the fact that these systems are deficient and deteriorating. This means that, over time, more and more people will rely on transportation systems with maintenance backlogs. (ASCE, Transit D, 2013). Transportation maintenance backlog stems from irregular monitoring of the condition of transit fleets by Transportation system SSA's. Many transit sector agencies do not conduct regular, comprehensive asset condition assessments, placing the transit sector behind its respective transportation sector counterparts. Slow economic growth has caused many local and state government to cut funding for the obsolete and aging transit fleets, resulting in an increased cost to passengers (ASCE, Transit D, 2013). $112 billion is needed in order to fully repair and install improvements to these transit systems. Despite serious cuts in funding and in service, many transit agencies have still managed to be leaders in making us of technological advances, such as offering real-time arrival information and online route planning, in order to make their systems convenient, reliable, and secure. This is consistent with ASCE's recommendations of having the U.S. government adequately fund maintenance of transit vehicles and facilities to maintain a state of "good repair" and to reduce system life-cycle costs.

The ASCE has recommended steps for improving the transportation sector (ASCE, Bridges C+, 2013; ASCE, Roads D, 2013; ASCE, Transit D, 2013). First, public access to transit should be increased in urban, suburban, and rural communities; second, the federal

government must identify a reliable source of revenue, besides the relying on the fuel tax, to fund highway repairs and improvements. These steps could possibly jump start investment into the transportation sector and slowly close the investment gap; all steps have been addressed in goal 3 and goal 4 of the Transportation SSP. By, "…effectively using resources by minimizing duplicate efforts, improving coordination, and aligning resources to address high sector risks," (Sammon, 2010, p. 25 – 26). DHS has anticipated the risks and threats to the transportation sector and can potentially fulfill the investment gap over the long run.

Energy sector

The Energy sector is has been declared "uniquely critical" by Presidential Policy Directive 21 because it provides an enabling function across the fifteen other critical infrastructure sectors (Department of Homeland Security: Energy Sector, 2013). Over 80% of the energy infrastructure is owned by the private sector and is responsible for supplying the nation with fuel for the transportation sector and electricity for homes and businesses. This sector is divided into three subsectors (electricity, oil, and natural gas) and includes production platforms, processing, refining facilities, terminals, nuclear, coal power plants, transmission, distribution, and control and communications systems (Sauter & Carafano, 2012). NIPP Criterion I is addressed by the Energy SSA through its efforts to federally authorize the North American Electric Reliability Corporation to develop additional reliability standards for the power grid (Hoffman, 2010). Both the electricity subsector and the oil and natural gas subsectors have begun an enhanced approach to planning for cyber security threats to infrastructure, in fulfillment of Criterion II of NIPP. The energy sector worked closely with the chemical sector to implement new goals and objectives with security partners regarding safety

and security at chemical facilities. This demonstrated an effort by the energy sector to achieve Criterion III through collaborating to strengthen security between the energy and chemical sectors, which share energy-related facilities and infrastructure (Hoffman, 2010). The energy sector has accomplished Criterion IV by constantly being kept abreast of the interdependencies of infrastructure that crosses international borders. Oil and natural gas pipelines and electric transmission lines have helped the energy sector and its SSP integrate the U.S. with the rest of the North American continent (Hoffman, 2010). In 2010, the energy sector employed the CIKR risk management model, which fulfils Criterion V by implementing a framework capable of crossing SSA's and better coordinating with DHS (Hoffman, 2010).

There are multiple potential risks and threats to the energy sector that have not been addressed and are currently causing major problems for some portions of the U.S. The U.S. relies on aging electrical grids and pipelines. Limited maintenance of these grids and pipelines has caused power fluctuations and interruptions, privately owned Energy sector infrastructure and business energy infrastructure configurations have posed challenges to implementing security initiatives. This is mainly due to private and business Energy infrastructure owners often leaving its critical infrastructure with minimal security, which can make it a target for an attacke (ASCE: Energy D+, 2013). Aging power lines have resulted in an increase in the number of outages from 76 in 2007 to over 307 in 2011, placing, not only the Energy sector at risk, but also all 15 other critical infrastructure agencies that are dependent on the energy it provides (ASCE: Energy D+, 2013). However, as an example of improvement, in 2012 the San Diego Gas & Electric company addressed the San Diego region blackouts and brownouts problems by completing a 500,000 volt transmission line, called the Sunrise Powerlink, linking San Diego to

the Imperial Valley (SDGE, 2013). This gave the San Diego region a link to one of the most renewable energy rich regions in the state of California. Yet, despite instances of success, the oil and gas subsectors, primarily owned by the private sector since 2008, have experienced a series of oil and gas pipeline failures. One example of failure took place in March 2014 in New York City in which when a 127 year-old gas main explosed, killing eight, injuring dozens, and collapsing a five-story building (Sanchez, 2014).

In response to the potential risks and to disastrous incidents, the energy sector specific plan (ESSP) was developed by DHS and introduces, "…several new topics in preparing for all hazards and natural disaster. Protecting and improving the resilience of the Energy Sector in the face of manmade and natural disaster is an ongoing effort that requires continued vigilance, contingency planning and training." (Hoffman, 2010, p. ?).

In order to fully improve and secure the energy sector, the ASCE suggests the federal government take incremental steps to address problems within the Energy sector: 1) identify and prioritize risks to energy security and develop standards and guidelines for managing maintenance programs, 2) create incentives to promote energy conservation and the installation and development of efficient renewable energy generation, and 3) adopt a national energy policy that anticipates and adapts to possible energy needs, all while increasing the efficiency of energy use and decreasing dependence on fossil fuels (ASCE, Energy D+, 2013). These steps have been noted and addressed by Energy SSP goals 1 –6 and through the energy SSA's efforts to bridge public security policy with private sectors managing the energy sector (Hoffman, 2010).

Discussion

This research has demonstrated that the U.S. has many challenges that must be addressed by the government-mandated NIPP and its SSP's. Despite the mission and goals provided by the NIPP, it is impossible to protect critical infrastructure from *all* possible risks and threats. Critical infrastructure must become resilient in the face of a catastrophic disaster or attack. SSA's must be able to not only protect infrastructure from attack or disaster, but also keep sectors in service through the development of plans that prepare sectors to handle most threats. This type of *resilience* calls for SSA's to structure SSP's to be able to absorb, adapt, and recover from a catastrophic events and helps determine whether or not DHS has been successful in providing CIP.

This research was unable to evaluate all aspects of U.S. critical infrastructure. Due to the immense size and scope of the entire U.S. critical infrastructure a full team of data collectors and researchers would be needed to fully explore all 16 critical infrastructure sectors and each subsector. Fortunately, to meet this end, in March, 2013, DHS established a nine-month Integrated Task Force (ITF) comprised of eight working groups, each focused on specific policy implementations, to evaluate and guide SSA's into implementing NIPP 2010 and PPD-21. Additionally, further research is needed to evaluate critical infrastructure cyber security. Cyber security is the new frontier in risk assessment and its full implementation as directed by PPD-21 needs to be further researched.

Qualitative data gathered from news documentation and reports from the ASCE have indicated that there is a serious lack of maintenance and funding needed to update and repair

the nation's critical infrastructure; approximately $3.6 trillion by the year 2020. All SSP's evaluated by this report have been found to be compliant with all criteria set forth by the 2010 NIPP and have demonstrated excellent ability to reduce risks from man-made disasters. The National Security Strategy of 2010, a document describing the strategy to protect the U.S. from foreign and domestic threats, lists CIP as part of the main strategy by stating, "…When incidents occur, we must show reliance by maintaining critical operations and functions, returning to our normal life, and learning from disaster so that their lessons can be translated into pragmatic changes when necessary." (White House, 2010, p.?). This demonstrates how CIP fits within the overall structure of the homeland security enterprise and SSA's have been shown to be compliant in providing recovery and solutions to disasters. However, the larger threat stems not from occasional natural or man-made disasters, but from a lack of maintenance, which now cost an estimated $3.6 trillion to remedy. If critical infrastructure maintenance is not effectively addressed, there may be severe negative consequences for national security.

References

American Society of Civil Engineers. (2013). Report card for America's infrastructure: Dams. Retrieved from http://www.infrastructurereportcard.org/.

American Society of Civil Engineers. *Bridges C+*. (2013). Retrieved November 30, 2014, from http://www.infrastructurereportcard.org/a/#p/bridges/overview

American Society of Civil Engineers. *Dams D*. (2013). Retrieved November 30, 2014, from http://www.infrastructurereportcard.org/a/#p/dams/overview

American Society of Civil Engineers. *Drinking Water D*. (2013). Retrieved November 30, 2014, from http://www.infrastructurereportcard.org/a/#p/drinking-water/overview

American Society of Civil Engineers. *Energy D+*. (2013). Retrieved November 30, 2014, from http://www.infrastructurereportcard.org/a/#p/energy/overview

American Society of Civil Engineers. *Levees D-*. (2013). Retrieved November 30, 2014, from http://www.infrastructurereportcard.org/a/#p/levees/overview

American Society of Civil Engineers. *Roads D*. (2013). Retrieved November 30, 2014, from http://www.infrastructurereportcard.org/a/#p/roads/overview

American Society of Civil Engineers. *Transit D*. (2013). Retrieved November 30, 2014, from http://www.infrastructurereportcard.org/a/#p/transit/overview

American Society of Civil Engineers. *Wastewater D*. (2013). Retrieved November 30, 2014, from http://www.infrastructurereportcard.org/a/#p/wastewater/overview

Broussard, D. The Department of Homeland Security, Water Sector. (2010). *Water sector-specific plan: An annex to the national infrastructure protection plan*. Retrieved from website: http://www.dhs.gov/xlibrary/assets/nipp-ssp-water-2010.pdf

Clinton, W. J. The White House, Office of the President. (1995). *U.s. policy on counterterrorism*. Retrieved from The White House website: http://www.clintonlibrary.gov/_previous/Documents/2010 FOIA/Presidential Directives/PDD-39.pdf

Clinton, W. J. The White House, Office of the President. (1998). *Presidential decision directive/nsc-63*. Washington D.C.: The White House.

Conklin, C. W. U.S. Department of Homeland Security, Dams Sector. (2010). *Dams sector-specific plan: an annex to the national infrastructure protection plan*. Retrieved from website: http://www.dhs.gov/xlibrary/assets/nipp-ssp-dams-2010.pdf

Costa, K., & Cooper, D. (2013, September 20). The 10 states most threatened by high-hazard, deficient dams. *Center for American Progress*. Retrieved from http://www.americanprogress.org/issues/economy/news/2012/09/20/38679/the-10-states-most-threatened-by-high-hazard-deficient-dams/

Critical Infrastructure Sector Partnerships. (2014, April 22). Retrieved November 6, 2014, from http://www.dhs.gov/critical-infrastructure-sector-partnerships

Department of Homeland Security, (2003). *Homeland security presidential directive 7: Critical infrastructure identification, prioritization, and protection*. Retrieved from website: https://www.dhs.gov/homeland-security-presidential-directive-7

Department of Homeland Security. (2013). *Dams sector: Sector overview*. Retrieved from http://www.dhs.gov/dams-sector

Department of Homeland Security. (2013, August 6). *Strengthening the security and resilience of the nation's critical infrastructure*. Retrieved from http://www.dhs.gov/strengthening-security-and-resilience-nation's-critical-infrastructure

Department of Homeland Security. (2013). Energy sector: sector overview. Retrieved from http://www.dhs.gov/energy-sector

Department of Homeland Security, (2013). *Nipp 2013: Partnering for critical infrastructure security and resilience*. Washington D.C.: Department Of Homeland Security.

Department of Homeland Security. (2013). Transportation systems sector: Sector overview. Retrieved from http://www.dhs.gov/transportation-systems-sector

Department of Homeland Security. (2013). *Water and wastewater systems sector: Sector overview.* Retrieved from http://www.dhs.gov/water-and-wastewater-systems-sector

DOWL HKM. (2014). *Big Hole River Diversion Dam and Pump Station Replacement*. Retrieved from http://www.dowlhkm.org/Big-Hole-River-Diversion-Dam-and-Pump-Station-Replacement

Hamilton, M. (2014, July 30). Broken water main floods UCLA; 5 people rescued. Retrieved November 30, 2014, from http://bigstory.ap.org/article/broken-water-main-floods-ucla-drivers-rescued

Hoffman P. The Department of Homeland Security, Energy Sector. (2010). *Energy sector-specific plan: An annex to the national infrastructure protection plan*. Retrieved from website: http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf

Lowy, J., & Baker, M. (2013, September 15). AP Impact: Many us bridges old, risky and rundown. *Associated Press*. Retrieved from http://bigstory.ap.org/article/ap-impact-many-us-bridges-old-risky-and-rundown

Mihalopoulos, D. (2011, December 17). City Inaugurates Costly Plan to Replace Aged Water Mains. Retrieved November 30, 2014, from http://www.nytimes.com/2011/12/18/us/chicago-inaugurates-costly-plan-to-replace-aged-water-mains.html?pagewanted=all&_r=0

Moteff, J. (2005). Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences. CRS Report for Congress, (Order Code RL32561).

O'Rourke, T. (2007). Critical Infrastructure, Interdependencies, and Resilience. *The Bridge, 37*(1), 22-29.

Pritchard, J. (2014, February 13). What California freeway has the most gridlock? Retrieved from http://bigstory.ap.org/article/what-california-freeway-has-most-gridlock

Sammon, J. P. The Department of Homeland Security, Transportation Systems Sector. (2010).*Transportation systems sector-specific plan: An annex to the national infrastructure protection plan*. Retrieved from website: http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf

Sanchez, R. (2014, March 17). New york explosion exposes nation's aging and dangerous gas mains.*CNN U.S.*. Retrieved from http://www.cnn.com/2014/03/15/us/aging-gas-infrastructure/

Sauter, M. A., & Carafano, J. J. (2012). Homeland security: A complete guide. (2nd ed., pp. 403-427). New York: Mc Graw Hill.

U.S. General Accounting Office, Report to the Committee on Governmental Affairs, U.S. Senate. (2002). *Critical infrastructure protection: Federal efforts require a more coordinated and comprehensive approach for protecting information systems* (GAO-02-474). Retrieved from GAO website: http://www.gao.gov/new.items/d02474.pdfhttp://www.gao.gov/new.items

/d02474.pdf

SDGE. (2013, April 2). National Award Recognizes SDG&E Environmental Monitoring Program. Retrieved from http://www.sdge.com/newsroom/press-releases/2013-04-02/national-award-recognizes-sdge-environmental-monitoring-program

Valdes, M., & Baker, M. (2013, May 24). I-5 bridge collapses into Wash. river, injuring 3. Retrieved from http://bigstory.ap.org/article/i-5-bridge-collapses-nw-wash-people-water

Werner, S. J. (2000). *America's national critical infrastructure assurance plan: Can compromise win in an uncompromising world?*. (Unpublished master's thesis, National Defense University).

The White House. The White House, Office of the President. (2010). *National security strategy*. Retrieved from The White House website: http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

The White House. Office of the Press Secretary. (2013). *Presidential policy directive: Critical infrastructure security and reilience*. Retrieved from website: http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

The White House. The Department of Homeland Security, (2013). *Executive order (eo) 13636 improving critical infrastructure cybersecurity presidential policy directive (ppd)-21 critical infrastructure security and resilience*. Retrieved from website: http://www.dhs.gov/sites/default/files/publications/EO-PPD Fact Sheet 12March13.pdf

Witt, E. (2009, October 18). National Weather Service Weather Forecast Office. Retrieved November 30, 2014, from http://www.crh.noaa.gov/lsx/?n=12_14_2005