# THE EFFECT OF NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION CRITICAL INFRASTRUCTURE PROTECTION STANDARDS ON BULK ELECTRIC SYSTEM RELIABILITY

by

Marlene Z. Ladendorff

EDWARD GOLDBERG, DM, Faculty Mentor and Chair

STEVEN BROWN, PhD, Committee Member

SUSAN VANN, PhD, Committee Member

Sue Talley, EdD, Dean, School of Business and Technology

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Philosophy

Capella University

August 2014





ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

**Abstract**

Compliance with regulations may not automatically produce a secure infrastructure. In the United States energy critical infrastructure sector, compliance with regulatory cyber security standards may not necessarily mean that an entity would be able to withstand a cyber attack on critical assets potentially supporting the reliability of the Bulk Electric System (BES). This qualitative exploratory inquiry study researched technical opinions of cyber security professionals in the energy critical infrastructure industry regarding the effect of the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards on the reliability of the BES. NERC entities had been required to be compliant with the standards for several years at the time this study was undertaken. There has been speculation regarding the efficacy of the standards to impact the reliability of the BES. However, there was a lack of scholarly or professional literature confirming assumptions concerning BES reliability. In this study, data was gathered through interviews with individuals who were CIP implementation experts. The purpose of this study was to identify a theme or themes regarding changes in the reliability of the BES as a result of the NERC CIP standards implementation. Interview data from the study generated 9 themes including a theme for the research question indicating that reliability of the BES had improved as a result of the implementation and enforcement of the CIP standards. Some of the more prominent themes included NERC fines having influenced entities in the implementation of the standards; entities have been more concerned about CIP compliance than securing their equipment; and entities have removed equipment from their facilities in order to avoid the requirements, and the associated expense, the standards would demand.

## Dedication

To Mom and Dad. Even though Dad says he is mad at me for being one college degree ahead of him, I know better.

**Acknowledgments**

Thanks to my mentor and dissertation committee advisor, Dr. Edward Goldberg. He hung in there and waited patiently for me while I resisted this dissertation topic for at least a year, probably more. He never gave up on me.

Thanks to my committee, Dr. Susan Vann, and Dr. Steven Brown, for agreeing to join me on this escapade.

Thanks to my friends who encouraged me for over five years to finish this.

Thanks to Jan, who helped me with editing when I needed it most.

Thanks to my husband, who has watched me struggle from the beginning…and is still married to me.

Thanks to Dr. D. for supporting and encouraging me.

Finally, thanks to Jill at Capella who single-handedly, and probably unknowingly, rescued me from the darkest moment of my PhD journey with one simple question, "Do you want to be *right*, or do you want to be *done* [graduate]?"

## Table of Contents

## List of Tables

## List of Figures

# CHAPTER 1. INTRODUCTION

## Introduction to the Problem

In the United States, critical infrastructure sectors support public health and welfare. Not all infrastructures in the United States are deemed critical. In order for an organization to be classified as critical to an infrastructure, certain criteria must be met. Executive Order 13010 (Order, 1996) provided a basic, broad statement regarding requirements for identifying an infrastructure organization as critical, stating that "certain national infrastructures are so vital that their incapacity or destruction would have debilitating impact on the defense of economic security of the United States" (p. 37347).

Organizations deemed critical to the infrastructure are ones that, over time, are essential to national defense, economic activity, public health and safety and national morale (Moteff, Copeland, & Fischer, 2003). Identified organizations are not restricted to governmental entities. Private sector organizations may also be identified as part of the critical infrastructure. Together, the government and private sector organizations are the network which comprises the United States critical infrastructure.

1 of the 16 sectors, as defined in the Presidential Policy Directive/PPD-21 (Directive, 2013), includes the energy sector. At the national level, critical infrastructure depends on reliable electrical power for uninterrupted operations (Massoud Amin & Wollenberg, 2005). On a smaller scale, dependency on electricity is illustrated through peoples' realistic expectations that light will emanate from a source connected to a light switch each time that switch is activated. Adding to the dependency on the reliability of the Bulk Electric System (BES) is a complacency that accompanies it; the more constant

and continuous the infrastructure, the less concern there is about it until it becomes unstable (Jackson, Edwards, Bowker, & Knobel, 2007).

A reliable electrical grid is the backbone of national safety and security (Lyons, Jacobi, & Starkweather, 2008). Threats to the BES include unforeseen outages due to weather, accidents that may affect transmission of electricity, and physical or cyber security threats with the potential to render portions or all of the BES inoperable. In a procurement language document produced by the Energy Sector Control Systems Working Group (Bartol et al., 2014), the effect of a successful cyber-attack on the energy critical infrastructure could have several consequences.

> A cyberattack on an energy delivery system can have significant impacts on the availability of the system to perform critical functions, the system integrity, and the confidentiality of sensitive information. Accidental and malevolent cyber threats to energy systems can impact national security, public safety, and the national economy. (p. 1)

The necessity to strengthen and protect the BES against threats is gaining recognition and importance in the United States.

Reliability of the BES falls under the auspices of the Federal Energy Regulatory Commission (FERC), a governmental entity. The North American Electric Reliability Corporation (NERC), a private company, became certified by FERC in 2006 as the Electric Reliability Organization (ERO) in the United States of America (Rowland, 2011). 14 reliability standards were developed by NERC with FERC providing oversight. Of these, the NERC Critical Infrastructure Protection (CIP) standards were implemented specifically in order to increase the ability of the BES to withstand cyber security attacks (Kaun, 2010).

## Background of the Study

The energy sector is 1 of 16 sectors of critical infrastructure in the United States. The BES is the backbone of the energy critical infrastructure sector. A report published by the U.S. House of Representatives (2013) stated that the BES traverses in excess of 200,000 miles of transmission lines, providing power to over 200 million people. Successful interoperability of the grid can be challenging but is required in order to maintain constant electrical flow (Schiff, 2007) at the consistent 60 hertz demanded by the electrical grid (Lambrechts, 2011). A cyber security attack could threaten that flow of electricity and disrupt the BES.

Illustrated in Figure 1 are the eight NERC Regional Entity (RE) abbreviated names. These REs report BES reliability information to NERC who then reports that information to FERC. NERC, a self-regulated body, is overseen by FERC and Canadian governmental organizations (Ellis et al., 2012). Figure 1 shows the geographic boundary for users, owners, and operators providing essentially all of the electricity in North America. Figure 1 highlights overlapping regional boundaries (in light-blue) between the Southwest Power Pool (SPP) and SERC Reliability Corporation (SERC).


*Note:* From "Reactive power interconnection requirements for PV and wind plants–recommendations to North American Electric Reliability Corporation (NERC)," by A. Ellis, et al. (2012), Sandia Corporation, pg. 9.

Figure 1. The Eight NERC REs

Table 1 identifies each abbreviated RE, listed in Figure 1, with its fully qualified name.

Table 1. Fully Qualified NERC RE Names (adapted from Ellis et al. (2012), pg. 9).

| Abbreviated Name | Fully Qualified Name |
|---|---|
| FRCC | Florida Reliability Coordinating Council |
| MRO | Midwest Reliability Organization |
| NPCC | Northeast Power Coordinating Council |
| RFC | Reliability First Corporation |
| SERC | SERC Reliability Corporation |

Table 1 (continued). Fully Qualified NERC RE Names (adapted from Ellis et al. (2012), pg. 9).

| Abbreviated Name | Fully Qualified Name |
|---|---|
| SPP | Southwest Power Pool |
| WECC | Western Electricity Coordinating Council |
| TRE | Texas Reliability Entity |

*Note:* From "Reactive power interconnection requirements for PV and wind plants–recommendations to North American Electric Reliability Corporation (NERC)" by A. Ellis, et al. (2012), Sandia Corporation, pg. 9.

Each region includes entities or organizations that are responsible for generation or management of power flowing through transmission lines or distribution networks (Chance, 2013) on the BES. All of NERC's reliability standards work in concert to ensure the reliability of the BES. In 2007, the NERC reliability standards, with the exception of the CIPs, became mandatory and enforceable for the BES (Stapleton, 2009). Three years later on July 1, 2010, complete compliance with the CIP standards joined the other NERC reliability standards in becoming compulsory for users, owners and operators of the BES (McClelland, 2012).

Three sections of the electrical grid combine to form the main grid in North America: the Eastern Interconnection, the Western Interconnection and the Electric Reliability Council of Texas or ERCOT (Lambrechts, 2011). The Texas Reliability Entity (TRE) is functionally independent from ERCOT and is the administrator of NERC

standards for ERCOT in Texas (Symbol & Year, 2014). These three large sections of the grid include smaller organizations that interconnect and synchronize their energy generation to the larger grid. The CIP standards were designed specifically to protect the elaborate, monumental combination of industrial control systems, distributed control systems and supervisory and data acquisition systems (Weiss, 2010) controlling and monitoring generators, electrical loads, breakers and switches (Stamp, Laviolette, Phillips, & Richardson, 2009) supporting the BES.

The terrorist attacks of September 11, 2001 changed how critical infrastructure entities would be secured from that date forward. The importance of protecting the critical infrastructure of the United States is well understood at the highest levels of government. The creation of the Department of Homeland Security (DHS) on November 25, 2002 (Thessin, 2003) was in response to the attacks of September 11, 2001. What the DHS is to national security, the NERC CIP standards are to supporting the protection and reliability (Benoit, 2008) of the BES. Nicholson (2009) succinctly stated that it is the responsibility of NERC to "ensure that the bulk electric system in North America is reliable, adequate and secure" (p. 16).

Electric reliability events such as the significant electrical blackout that affected the northeastern United States and Canada in August, 2003, emphasized the relevance of reliability in the energy critical infrastructure sector (Eto & LaCommare, 2008; Schneider, 2013). That momentous power failure continued for two days, affected 50 million citizens and resulted in over six billion dollars' worth of economic losses (Eccleston & Stuyvenberg, 2011), including looting and crime. This event emphasized public reliance on electric power and the underlying demand for reliable energy from the

BES. As such, the security of the energy sector is an issue of increasing importance (Lawson, 2004).

Cyber security incidents are on the rise. Between October, 2011, and February, 2012, cyber security attacks on computer systems supporting critical infrastructure increased to 86 events as compared to 11 events from the same timeframe in the previous year (Thilmany, 2012). Similarly, the U.S. House of Representatives (2013) report declared a 68% increase in 2012 from 2011 in cyber security events aimed at Federal agencies and critical infrastructure, as well as other industrial organizations. Ever increasing cyber security compromises to the equipment supporting the BES pose threats to the reliability of the grid.

## Statement of the Problem

The problem that prompted this research was change in the reliability of the BES. With increasing cyber security threats and attacks against critical infrastructure, concern exists that the BES may not be properly fortified. Efforts and investments have been made by organizations to comply with standards intended to secure the electric grid (Staggs, 2008). However, insufficient literature, scholarly or professional, exists regarding changes in BES reliability subsequent to standards implementations.

## Purpose of the Study

During a United States Congress House Committee on Science (2006) hearing on cyber security regarding the vulnerability and preparedness of the United States, Gerald Freese suggested that the process of working toward securing the energy critical infrastructure includes implementation of standards. Utilities supporting the BES are required to be in full compliance with CIP standards as of July, 2009 (McKay, 2011).

Improved BES reliability is the desired outcome from the implementation of reliability standards, including the CIPs. However, the fact that standards were required to be implemented does not guarantee that the reliability of the BES has improved (R. Wells, personal communication, October 15, 2013).

The purpose of this qualitative exploratory research was to identify a theme or themes in opinions regarding changes in the reliability of the BES as a result of the NERC CIP standards implementation. There is a dearth of data on this subject. Currently available information is inconclusive regarding how effective the standards have been in increasing the reliability of the BES since implementation has completed and enforcement efforts have commenced (Zhang & Stern, 2010). The results and conclusions from this study offered additional avenues of research that may be pursued to enlighten the scholastic, regulatory and professional community regarding BES reliability as a result of the CIP standards implementation.

Figure 2 illustrates a process flow diagram depicting steps from which the purpose of this study evolved.

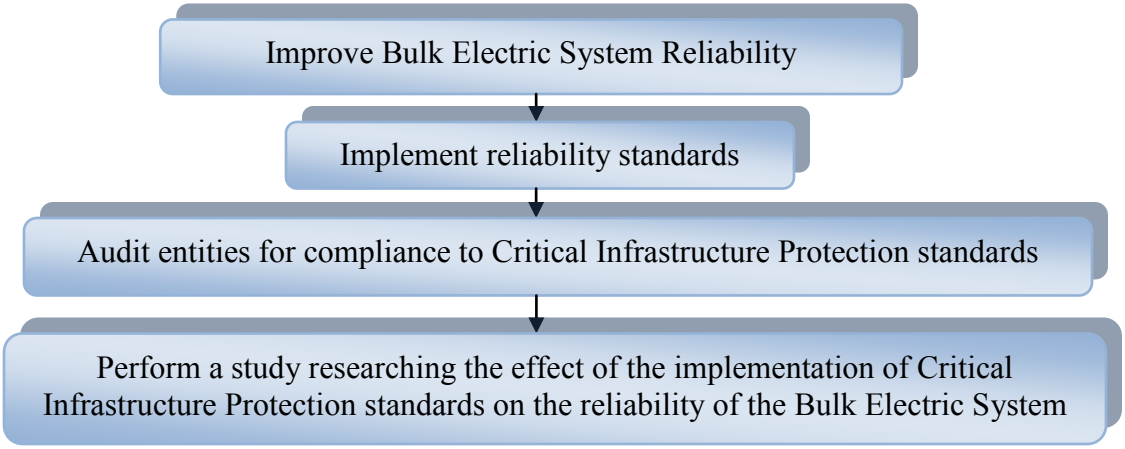


Figure 2. Purpose process flow diagram

## Rationale

Instead of concentrating on cultural insights accomplished through ethnographic methodologies or construction of a theory through a grounded theory approach, qualitative exploratory inquiry pursues the understanding of a process, phenomenon or the opinions of the people involved (Caelli, Ray, & Mill, 2008). There are no correct or incorrect research methods for this aim, but instead different methods fulfilling different purposes (Silverman & Marvasti, 2008). Qualitative research may offer valuable understanding regarding implementations of programs including research into policies and evaluations (Glenn, 2010). The design of this study was chosen by the researcher in support of the initiatory nature of the research.

All research, as a whole, is exploratory. Exploratory design, a subset of qualitative methodology, is focused on discovery and the construction of theories (Davies, 2006). This study was not focused on a theory or on developing a theory. Sometimes alternately referred to as descriptive qualitative research (Caelli et al., 2008), qualitative exploratory inquiry methodology favors a study where information or literature on the topic is scant.

Data collection, through semi-structured interviewing, was used to document themes in participants' opinions of the CIP standards. From the themes, insights and future scholastic research were developed. Continuing from this qualitative study, quantitative research may be initiated in the future to concentrate on focused areas where statistical analysis could offer deeper insights into CIP effectiveness. Qualitative exploratory research can lead to continued quantitative studies, according to Zikmund, Babin, Carr and Griffin (2012), who stated,

> Often, exploratory research may be needed to develop the ideas that lead to research hypothesis. In other words, in some situations the outcome of exploratory research is a testable research hypothesis. Confirmatory research then tests these hypotheses with quantitative data. The results of these tests help decision making by suggesting a specific course of action. (p. 135-136)

From a business perspective, an advantage of generating data regarding perceived effectiveness of standards implementation should give insight, at very modest cost, into the return on investment of regulatory compliance efforts by registered entities in the NERC regions. More importantly, registered entity management departments should be concerned about changing regulatory landscape should regulators perceive risks with the implementation of their regulations (Camm & Fox, 2010). Examining the conclusions to this exploratory study should offer insight into regulatory compliance efforts, in addition to answering the research question. Additionally, potential next steps in regulatory compliance may be illuminated through recommended future research as a result of this study.

Qualitative research methodology seeks to answer how/what/why questions in research, as opposed to quantitative methodology which looks for numerical measurements, for example, how many of something (Billson, 2010). The research question in this study did not search for a statistical solution to the research question. Instead, perceptions and opinions of participants were collected via semi-structured interviews. The researcher analyzed the results of the interviews for themes indicating a change in the reliability of the BES. By virtue of the newness of the CIP standards and lack of available literature regarding the effectiveness of the standards on the reliability of the BES, qualitative exploratory inquiry research methodology was the most appropriate methodological choice for this study.

## Research Question

Has the reliability of the North American Bulk Electric System been affected by the implementation of the North American Electric Reliability Corporation's Critical Infrastructure Protection Standards?

## Significance of the Study

Motivating factors for improving grid reliability include, but are not limited to, safety, security and monetary considerations. The blackout in 1965 brought about significant changes (Wollenberg, 2004) in the regulation of the BES. The expense of the New York City power outage in 1977 was approximately $350 million (Streeter, MacDonald, Apple, Kraus, & Galotti, 1983). The 2003 blackout, considered to be the largest power failure in the history of the United States and Canada (Prezant et al., 2005) contributed to 11 deaths (Minkel, 2008) and cost of over six billion dollars (Eccleston & Stuyvenberg, 2011).

History has illustrated the potentially fragile nature of the electrical grid and its' susceptibility to failure through the blackout in 1965 (Lerner, 2005), the power outage in New York City in 1977 (Streeter et al., 1983) and the infamous 2003 blackout (Amin & Schewe, 2007; Lyons et al., 2008) affecting Eastern United States. Power outages are, at the very least, inconvenient. Interruptions in customers' electrical service may require people to employ alternative methods of heating, cooling and other functions which are normally routine when the electrical supply is constant. At worst, blackouts may be considered disasters as determined by the loss of life and the severity of long-term property damage as well as damage to infrastructure (Boin & McConnell, 2007).

The first NERC standards became mandatory in March, 2007 (Zhang & Stern, 2010). These regulatory standards requirements have been in place for approximately five years. Conformity with NERC CIP standards was required as of December, 2009 (Kaun, 2010). Auditable compliance for these standards was compulsory by December, 2010 (Staggs, 2008). While these deadlines are in the past, results from this research regarding evaluation of themes in the effectiveness of the implementation of the standards provided tangible data from which conclusions were drawn.

In a technological context, studying claims of increased reliability in the BES as a result of the implementation of the CIP standards is significant with respect to the safety of residents in North America. Reliability is not measured under conditions of stress (Keogh & Cody, 2013), such as a cyber-attack, and documented evidence of past power failures is a reminder of the fallibility of the electrical grid. Confirmation, through research, that reliability changes in the BES are attributable to the enforcement of reliability standards should be a priority to both the regulators instituting the standards and the management of the registered entities performing the implementation.

An important consideration regarding research into this area was the timing of this study. With the recent implementation of NERC CIP standards, it was important to gather data before too much time passed. Quantitative researchers have found that retrospective study (studying the past through the lens of present-day subjects) may produce questionable results (Silverman, 2009). Therefore, the timing of this study was appropriate.

This research and the conclusions generated from it should be of interest to organizational and management personnel of registered entities who must comply with

the standards. Confirmation that the efforts entities have expended in implementing the standards have, indeed, improved the reliability of the BES should verify for management that their expenditures into compliance were pertinent. Validation of these efforts should have implications for the technological component of the entity organizations. It would stand to reason that if the work entities have performed to implement the CIP standards has indeed improved reliability of the BES, then the possibility that a cyber security attack on the grid producing a power failure should be reduced.

## Common Acronyms in the Field

Technical terminology is often abbreviated with three-letter acronyms (Jindra, 2005) and lengthy identifications (such as the name of a federal agency) which become truncated using only the first letter of each word as representation. This section is comprised of common acronyms as well as descriptions of three-letter acronyms and other abridged phrases or names which may serve to cause confusion amongst individuals unfamiliar with the terminology of the field in which this research was conducted.

*BES.* Bulk Electric System. As stated in NERC's glossary of terms (NERC, 2011),

> As defined by the Regional Reliability Organization, the electrical generation resources, transmission lines, interconnections with neighbouring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included in this definition. (IESO_GDE_0364, 2013)

*CIP.* Critical Infrastructure Protection. A NERC cyber security reliability standard.

*ERO.* Electric Reliability Organization proposing federal BES regulations and enforcing reliability standards (Coll-Mayor, Paget & Lightner, 2007).

*FERC.* Federal Energy Regulatory Commission, an independent governmental agency regulating the flow of natural gas, oil and electricity within the United States.

*NERC.* North American Electric Reliability Corporation. The ERO appointed by FERC.

*RE.* Regional Entity. The eight geographical regions which comprise NERC in North America.

## Assumptions and Limitations

Burns (1989) ascertained that an assumption in qualitative research "is that all data are context specific" (p. 48) which requires that the context of the study be understood by the researcher. This researcher is versed in NERC standards, is an expert in the field of cyber security in the electricity industry and has a critical understanding of the need for a reliability study at this point in the development of cyber security reliability standards for the BES. In addition to experience in the field of cyber security and the BES, understanding of regulatory processes, procedures and violations was essential. Two principle assumptions in this study were the probability that participants would be difficult to recruit and then, once recruited, participants could change their mind and withdraw from the study based on a fear that they could be identified by the data they provided, study confidentiality and anonymity protocol notwithstanding.

With a lack previous research on the effect of reliability standards on BES, a potentially obvious topical assumption may have been that any reliability standards implemented and enforced would produce an increase in the reliability of the electrical grid. Resistance to adopting that assumption was exercised and the commitment to remain neutral on any speculation regarding electrical grid reliability was a priority.

Neutrality was critical in order to avoid any potential bias while observing the research data. Conscious and continuous dedication to bias avoidance allowed data driven themes in the study to emerge.

Methodological assumptions, which normally fall into either a quantitative or qualitative category, frequently seem to contradict each other (Salem, 2012). Quantitative assumptions typically follow a statistical bent while qualitative assumptions delve into a more humanistic classification. This study, while not analyzing statistics, was attentive to the results collected from the interview participants in a way that would produce graphical representations of human interpretations. In other words, some of the data emanating from the research participant interviews was structured in a visual representation which may embody statistical results in a manner similar to a quantitative study.

Another methodological assumption that the researcher took into consideration for this study was the possibility for the results of the research, although qualitative in design, to be expressed, visually, in a format expressing a quantitative summary of the results (Mays & Pope, 1995). The data required encompassed technically based opinions from individuals regarding how they felt the CIP standards implementation has impacted the reliability of the BES. With the conclusions of this study potentially having implications in the business community, quantitative representations of the data offered a visual structure that should be palatable to management and operations individuals.

A limitation of this study may have existed in the singular focus on one NERC reliability standard, the CIP standards. NERC regulates and enforces multiple categories of reliability standards for the North American BES (Zhang & Stern, 2010). The CIP

category is comprised of 9 standards, 8 of those being specific to cyber security. With the increasing regulatory requirements to provide tighter cyber security for critical infrastructure organizations, the CIP standards were chosen in order to study data regarding participants' opinions on the effect this standard has had on the reliability of the BES.

Another limitation considered in this study was the fact that cyber security in the power industry is relatively new, especially regulatory compliance with standards. With the NERC reliability standards recently becoming enforceable (McClelland, 2012), more time with the standards in effect may be needed such that additional data could be generated from studies. New standards with limited and ambiguous guidance available to incorporate those standards (Abbotts, Anderson, & Kari, 2010) may require more time and experience with the standards implementation before entities may be able to provide researchers with complete data. A way to make that determination would be through analysis of conclusions from this exploratory study.

Currently, there are no available studies documenting any effects that the NERC CIP standards have had on the reliability of the BES. There is agreement in the industry that understanding the effects of the CIP standards on BES reliability is not only warranted but overdue (R. Wells, personal communication, October 15, 2013). Bacchetti (2002) stated that "research in new areas must start somewhere" (p. 1271). With a lack of documentation on the effectiveness of the NERC CIP standards on BES reliability, a qualitative exploratory inquiry research methodology was a suitable choice for this study. Succinctly stated, Zikmund et al. (2012) offer that exploratory research "can be an essential first step to a more conclusive, confirmatory study by reducing the chance of

beginning with an inadequate, incorrect, or misleading set of research objectives" (p. 137).

## Nature of the Study (or Theoretical/Conceptual Framework)

It may be common to think of implementing technology as the solution to securing critical infrastructure. Different departments in organizations may have different opinions regarding infrastructure protection. From a management and organizational perspective, securing business assets (such as the industrial control systems that operate a power plant) may fall under the departments responsible for business models and regulatory compliance (Anderson & Fuloria, 2010). From an engineering perspective, Henrie (2013) expressed that "engineering managers are responsible for ensuring the safe, efficient, and effective operation of process control systems which monitor and control the nations critical infrastructures" (p. 38).

Presidential Policy Directive/PDD-21(Directive, 2013) for Critical Infrastructure Security and Resilience outlines three strategic imperatives.

1. Refine and Clarify Functional Relationships across the Federal Government to Advance the National Unity of Effort to Strengthen Critical Infrastructure Security and Resilience;
2. Enable Efficient Information Exchange by Identifying Baseline Data and Systems Requirements for the Federal Government; and
3. Implement an Integration and Analysis Function to Inform Planning and Operational Decisions Regarding Critical Infrastructure. (p. 6-7)

The Presidential Directive outlines an objective for the policy, roles and responsibilities, research and development to support the policy, how the directive is to be implemented and the designation of the 16 critical infrastructure sectors and sector-specific agencies in the United States (Directive, 2013). The structure of the directive is similar to the

structure of a management plan for implementation of the security posture of an organization. Similar to the directive, Dutta and McCrohan's (2002) three pillar framework supporting an organizational and management approach to security accentuates management's duty to support that framework, which includes critical infrastructure, technology and the organization. This framework does not rely specifically on technology alone to defend against attacks but incorporates a management element which suggests that failures in security would be the result of failures in management (Dutta & McCrohan, 2002).

In research studies, some configuration reviews establish theories, searching for one that may assist the researcher with the collection of data, facilitating the formulation of ideas, and help bring the research together (Anfara & Mertz, 2006). Quantitative research methodologies require a theory to be specified so that the study may be designed to test that theory (Creswell, 2013). Qualitative research may also include a theory, for example self-efficacy or systems, and then expand on the conceptual and empirical specifics of that theory. Theoretical framework has also been likened to a framework similar to construction or scaffolding from which a study may be built upon (Plakhotnik & Rocco, 2009).

In this exploratory study, no theory on which to base the research was expected or anticipated. The development of themes as a result of the research study was the aspiration for this research rather than using a theory as a framework from which to build the study on (Morse, Barret, Mayan, Olson, & Spires, 2002). Additionally, the data analysis method selected for this study, thematic inductive analysis, supported the choice to forego a theoretical framework, instead concentrating on expanding themes which

were extracted specifically from the study data and not from a predetermined theory (Jebreen, 2012). The data from participants' input was used to indicate a theoretical framework, if one surfaced during the study.

## Organization of the Remainder of the Study

Continuing with the literature review, Chapter 2 presented a focused review of the history of critical infrastructure in the United States. Additionally, an introduction to FERC and NERC and their roles in the electricity industry were presented as well as historical electrical grid disturbances and how they influenced the development of reliability standards. The literature review also covered cyber security in the energy critical infrastructure and finally, the history and development of the NERC CIP reliability standards.

Chapter 3 included the methodology and design of this research study. A qualitative exploratory inquiry design was suitable for this study. Semi-structured telephone interviews with a sample frame from the defined population provided the data required for the study. Consistent with the research question, themes in participant opinions regarding the affect the NERC CIP standards have had on the reliability of the BES was the purpose of this study.

Chapter 4 summarized the results of the study. Chapter 5 presented conclusions drawn from the study results. Recommendations for continued research were also outlined. Benefits of this study were not limited to outlining new research opportunities for studying impacts to the reliability of the electrical grid or the efficacy of reliability standards. Operational and management suggestions regarding NERC CIP standards implementations were also offered in Chapter 5.

## CHAPTER 2. LITERATURE REVIEW

The literature review for this study focused on reviewing any available scholarly and professional documentation that confirmed North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards effects on the reliability of the Bulk Electric System (BES). With insufficient literature available, this review was organized into six sections outlining critical infrastructure from a historical and regulatory perspective. This perspective allowed the researcher the opportunity to lay ground work which benefited not only this study but future research surfacing as a result of the conclusions and recommendations from this study. A chronological format was followed in order to establish the historical perspective and understanding surrounding the electrical grid, NERC, cyber security and reliability standards.

The first section of the literature review focused on the history of critical infrastructure. The second section covered the federal government energy entity Federal Energy Regulatory Commission (FERC) and the private Electric Reliability Organization (ERO) Corporation, NERC. The third section reviewed historical disturbances on the electric grid. These disturbances had a direct impact on legislation passed and entities formed in order to improve the reliability of the grid. The fourth section of the review centered on the NERC reliability standards.

The fifth section reviewed literature spotlighting cyber security in energy critical infrastructure organizations, events or discoveries that changed the course of cyber security and how those events affected regulators and enforcement of standards with the intent of improving reliability of the BES. The sixth and final section of the literature review focused on NERC CIP history and development.

## A History of Critical Infrastructure

As society has matured and become more reliant on the interconnectivity of systems and infrastructures, there has been an increasing realization that the need for protecting those infrastructures is becoming essential. Differences between computers running mainstream operating systems (UNIX or Windows, for example (Weiss, 2010)) and control systems exist and the cyber protections for each can be different. Federal organizations, regulations and agencies were created by presidential offices as the demand for greater security increased. Augmented protection occurred as a response to breaches in security which, unfortunately, have the potential to, and sometimes did, result in casualties in the form of the destruction of equipment, human injuries or death.

The National Communication System (NCS) was established in 1963 (Hart & Ramsay, 2011) by President Kennedy. NCS was charged with establishing communication channels throughout the federal government in the event of an emergency, including a nuclear attack. The Federal Emergency Management Agency (FEMA) was created in 1979 (McLoughlin, 1985). FEMA's goals center around reducing risks associated with hurricanes and earthquakes as well as being engaged in civil defense (Hart & Ramsay, 2011).

The 1980's experienced significant changes in critical infrastructure protection. The first of these changes was President Regan's Executive Order to federal departments and agencies (Hart & Ramsey, 2011). This order required federal organizations to take responsibility for securing vital assets belonging to their organizations. As the years passed and infrastructure threats changed, the definition of infrastructure changed also (Moteff & Parfomak, 2004).

Prior to 1983, groups charged with infrastructure obligations included public organizations supporting social services as well as economic activity in the private sector (Moteff et al., 2003). At that time, primary concentration was on the public works scheme. Concern surrounded the physical condition and technological capabilities of public works and the government spending potentially required in order to ensure that physical and management essentials were adequate. Primary infrastructures under consideration at that time included public structures, roads and bridges, airports and other ports of harbor along with water/waste water systems. Other organizations including, but not limited to, telecommunications, electricity generation, fire safety and prison facilities were acknowledged (Vaughan & Pollard, 1984).

A report to Congress in 1983 outlined the state of the infrastructure in the United States. The Congressional Budget Office (CBO), author of the report presented to Congress, examined seven classifications of infrastructure which were deemed as unequivocally essential to the nation's economy (Moteff et al., 2003). These included

1. Highways
2. Public Transportation System
3. Wastewater Treatment Systems
4. Water Resources
5. Air Traffic Control
6. Airports
7. Municipal Water Supply

Through time, changes in infrastructure and the threat vectors utilized to create security incidences have reshaped the definition of infrastructure and what constitutes criticality.

As the information revolution gained momentum through the 1980's and 1990's, interconnectivity of systems and infrastructure components increased. Federal response to domestic attacks also continued. In the 1990's, violent events that illustrated security holes in the nation spurred increased governmental action to expand protection of the infrastructure. Some of those domestic incidents included the 1993 bombing of the World Trade Center and the 1995 bombing of Oklahoma City's Murrah Federal Building, along with the attack on the USS Cole in 2000 (Copeland, 2001).

After the September 11, 2001 terrorist attacks on the United States, the Department of Homeland Security (DHS) was formed in the spring of 2002 (Thessin, 2003). Changes to critical infrastructure protection ensued including, but not limited to, presidential directives, acts and plans. Then President Bush compared the creation of DHS with former President Harry S. Truman's predicament after the end of the World War II (Stanhouse, 2003). Truman embraced the need to unite United States defense, diplomacy and intelligence by creating the National Security Council (Stanhouse, 2003) in an effort to emerge victorious from the Cold War.

In 2002, the Homeland Security Act gave DHS the lead in recommending and organizing critical infrastructure security (Larence, 2007). Documents published in 2002 included the National Strategy for Homeland Security and the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (Hart & Ramsey, 2011) as well as the Homeland Security Presidential Directive 7 (HSPD 7) (Larence, 2007). HSPD 7 delineated more specific protection responsibilities required of DHS and sector-specific agencies which were assigned to protect specialized segments of the critical infrastructure, for example, but not limited to, energy, transportation and communications

(Moteff & Parfomak, 2004). These documents increased the number of critical infrastructure sectors from 7 to 13.

In 2006, DHS established the National Infrastructure Protection Plan (NIPP) to satisfy elements outlined in HSPD 7 that required DHS to develop a plan to incorporate steps to increase critical infrastructure security (Larence, 2007). The NIPP also included information on a government sector/private industry partnership designed to contribute to the security of Critical Infrastructure and Key Resources (CIKR) (Larence, 2007). Critical infrastructure organizations are not strictly comprised of government agencies and sectors but are a combination of public and private organizations. As such, cooperation between public and private entities should produce a stronger alliance with greater potential to protect the individual sections of the critical infrastructure.

As of 2011, 18 sectors of critical infrastructure had been defined in the NIPP (Schaffer, Keil, & Mayer, 2010) to include

1. Agriculture and Food
2. Banking and Finance
3. Chemical
4. Commercial Facilities
5. Communications
6. Critical Manufacturing
7. Dams
8. Defense Industrial Base
9. Emergency Services
10. Energy
11. Government Facilities

12. Healthcare and Public Health

13. Information Technology

14. National Monuments and Icons

15. Nuclear Reactors

16. Postal and Shipping

17. Transportation Systems

18. Water

These sectors were defined as CIKR sectors in the NIPP. The sectors contain cyber elements, as well as physical and human components, that should be protected (Hart & Ramsey, 2011). Respective sectors depend more heavily on some elements than others. For example, the cyber security element (as compared to the physical element) is predominant in the information technology (IT) and communications sectors while the energy and water sectors depend on the physical element more than cyber (Hart & Ramsey, 2011).

All of the CIKR sectors could be subject to an attack of some kind, such as a natural disaster, terrorist plot or an unintentional accident. With the increasing interconnectivity of the critical infrastructure, it may be possible for an attacker to plan on disrupting multiple CIKR sectors by interrupting one CIKR sector as a first strike, similar to the intent of the attacks on Pearl Harbor (Mazanec, 2009). For example, causing a major outage in the energy CIKR sector resulting in crippling blackouts could enable an attacker to then strike against the banking and finance CIKR or communications or multiple CIKR sectors. Therefore, protecting the critical

infrastructure against attack is becoming increasingly important and urgent (O'Rourke, 2007).

In 2013, Presidential Policy Directive/PPD-21 (Directive, 2013) reduced the number of critical infrastructure sectors from 18 to 16 (Petit et al., 2013). In contrast to the previously listed 18 sectors, the current 16 sectors include

1. Chemical
2. Dams
3. Financial Services
4. Commercial Facilities
5. Defense Industrial Base
6. Food and Agriculture
7. Communications
8. Emergency Services
9. Government Facilities
10. Critical Manufacturing
11. Energy
12. Healthcare and Public Health
13. Water Wastewater Systems
14. Information Technology
15. Nuclear Reactors, Materials, Waste
16. Transportation Systems

2 of the 18 previous sectors, National Monuments and Icons and Postal and Shipping, were combined with other sectors, resulting in a reduction of critical infrastructure sectors to 16 (GAO, 2013).

## FERC and NERC in the Energy Critical Infrastructure

Approximately 90 percent of the critical infrastructure in the United States is owned and operated by a combination of government and private sector businesses (Berkeley III, Gallegos, & Grayson, 2008). Protection standards and regulations govern both the public and private sector. In the energy critical infrastructure sector, the NRC regulates nuclear power reactors while FERC regulates other energy producing entities such as hydro-electric dams, coal fired and gas fired power plants. FERC is the federal agency governing the electrical sector with NERC performing ERO responsibilities including implementation, auditing and enforcement of reliability standards.

Nuclear facilities that generate electricity for the power grid in the United States include 104 reactors (Roberto & de la Rubia, 2007), a few of those reactors being in cold shutdown. Prior to the regulation of nuclear power plants, regulation of nuclear materials was the responsibility of the Atomic Energy Commission, instituted by Congress, which was founded out of the Atomic Energy Act of 1946. In 1974, the Atomic Energy Commission was disbanded and replaced with the NRC. Currently, nuclear reactors are regulated by the NRC and are not required to comply with the NERC CIP standards.

The NRC does not regulate the power production of nuclear reactors. The primary mission of the NRC is assuring protection of the publics' health and safety (Childers, 1989). For decades, nuclear power has appeared to be plagued with emotion and conflict in society. The accident at Three Mile Island in 1979 raised awareness significantly regarding the potential health and safety hazards present in the nuclear power industry, increasing the potential conflict surrounding nuclear power. More than 30 years later, the nuclear incidents in Fukushima, Japan following the earthquake and

resulting tsunami in 2011 compounded the emotion already plaguing the nuclear power industry.

An antecedent to FERC, the Federal Power Commission (FPC), was founded from the Federal Power Act of 1920, also referred to as the Federal Water Power Act of 1920 (Pollak, 2007). At the time of inception, the FPC was responsible for coordinating the promotion of hydroelectric power. Regulation of the natural gas industry, through the Natural Gas Act of 1938, was then added to FPC's hydroelectric responsibilities (Bell, 1964). Almost 40 years later and as a result of the Department of Energy Organization Act of 1977 (Congress, 1977), FPC was renamed the Federal Energy Regulatory Commission (FERC) under title IV of the Act.

FERC's stated mission is to provide regulation and oversight in the energy industries, holding the interests of the American public as their priority with regard to the economy, the environment, and safety (Inslee, Larsen, & McDermott, 2006). Contributing to the goal of achieving that mission, FERC is engaged in regulating the transmission of electricity, natural gas and oil in the United States, providing licensing to hydroelectric projects and providing analysis of liquefied natural gas terminal propositions. Two elemental objectives support FERC's mission. They include fairness in energy services (rates, terms and conditions) and assuring an energy infrastructure based on safety, reliability and efficiency.

When the Energy Policy Act was signed into law on August 8, 2005, FERC was required to issue a final rule outlining implementation of the new reliability foundation within 180 days of the Act being becoming law (Moot, 2006). On May 15, 2006, Moot (2006) reported to the Committee on Energy and Natural Resources that FERC was in

possession of an application from the North American Electric Reliability Council in which they requested to be certified as the ERO for FERC. In addition to this application, the North American Electric Reliability Council also submitted 102 reliability standards to FERC for approval (Sergel, Cook, & Counsel, 2006). On July 20, 2006, FERC certified NERC as the ERO.

2007 saw the first of the NERC reliability standards shift from voluntary to mandatory compliance for users, owners and operators of the BES, in addition to becoming enforceable by NERC in 2007. Also in 2007, the NERC CIP (cyber security) standards were rolled out. NERC, with assistance from the Regional Entities (REs), accomplish enforcement actions through audits, self-reports made voluntarily by BES users, owners and operators, and random independent checks and examinations of possible infractions of standards (Carpentier, 2011). Through these enforcement activities in the compliance program, NERC strives to achieve their goal of increased reliability for the BES.

## Electric Grid Disturbances

Deliberate cyber-attacks have planned actions and usually produce destructive results. Malware infections resulting from successful hacking attempts may leave computer hard drives inoperable, or worse, and may result in the compromise of sensitive or personal information. A cyber-attack concentrated on disabling the power grid may increase the speed with which a ground assault could then be implemented by terrorist forces (Lewis, 2010). And with the increasing connectivity of critical infrastructure systems, weakening one area of the BES could risk a compromise of larger sectors of the system which may produce a cascading effect on the grid (Church & Scaparra, 2007).

An attack on the electrical grid could result in catastrophic loss of power to the country (Church & Scaparra, 2007). A cyber-attack on the electrical grid could trigger a blackout with the potential to cascade throughout parts of the country, at a minimum. Compromising the power grid could be a pre-cursor to other attacks on U.S. soil (Lewis, 2010). While a cyber-attack by itself may not pose a threat to the security of the country, when combined with an organized and planned terrorist plot, it may provide an affective first strike.

While a deliberate, planned cyber-attack may be aimed at compromising the BES, non-malicious cyber incidents have caused localized power interruptions in the United States and other countries. The results of these disturbances have ranged from inconveniences, at a minimum, to injuries or death such as the 1999 Olympic Pipeline Company gasoline pipeline rupture in Bellingham, WA (Weiss, 2010). Power outages have had an impact on the grid (Farrell & Lave, 2002) and have served to drive government and regulatory agencies to work toward improving the reliability of the BES in an effort to minimize disturbances with a goal of reducing the detrimental effect that outages produce. Regulatory involvement through standards implementation is aimed at improving grid reliability.

In November 9, 1965, a power outage in the Northeastern United States was a significant event (Zhang & Stern, 2010) prompting the creation of the National Electric Reliability Council in 1968. In a report to the President of the United States from the Federal Power Commission in 1965, the blackout affected the majority of the Northeastern United States as well as the Province of Ontario. The investigation performed by the Federal Power Commission, with assistance from The Hydro-Electric

Power Commission of Ontario and other participating groups, found that the disturbance originated in the operation of a relay (Li, Yamashita, Liu, Zhang, & Hofmann, 2008) within a hydroelectric plant located on the Niagara River in Ontario. The faulty operation of this relay resulted in the cascading power outage that spread throughout the Northeastern United States. However, the investigation revealed no evidence of sabotage at any point during the blackout.

The power outage in New York City in July, 1977, was considered the most significant loss of power event since the black out in 1965 (Streeter et al., 1983). This occurrence is infamous for the civil unrest that erupted during the blackout. Causes contributing to the electrical disruption included human error (Apt, Lave, Talukdar, Morgan, & Ilic, 2004) and severe weather and equipment malfunctions. Although not necessarily a factor that influenced regulatory behavior regarding improving reliability of the grid, the 1977 blackout did incur an expense of approximately $350 million (Streeter, et al., 1983).

The western United States experienced two power outages in 1996, one on July second and third and the other on August 10. The July blackout originated in Idaho (Venkatasubramanian & Li, 2004) when a reactive power deficiency caused erratic voltages, leading to a divergent transient which gained momentum as electrical trips increased down the grid. While not a significant event contributing to regulatory efforts on the grid, the July outage affected two million rate payers (NERC, 2002). Electricity to most customers was returned within 30 minutes but others remained without power for up to six hours.

The August 10 disturbance, similar to the July disruption, was caused by a power line flashing (arching) and grounding to a tree. In contrast to the July disturbance, however, this event affected 7.5 million customers in 10 western states (Kim & Obah, 2007). Hot summer temperatures had increased the power load on transmission lines, contributing to the resulting cascading affect after the first event occurred. Power was restored to rate payers after approximately 16 hours (NERC, 2002).

Another major disturbance on the electric power grid occurred on August 14, 2003. Power transmission lines located in northern Ohio State shorted with foliage which had become overgrown, causing a failure of the power lines (Amin & Schewe, 2007). Under normal conditions, disturbances on the electrical grid are recognized by alarm systems designed to detect anomalies and activate warning signals for the human operators of the systems. On this day, however, erroneous software data resulted in no warnings or alarms being generated for the event, crippling the BES monitoring tool (Zhang & Stern, 2010) and leaving operators oblivious to the original disruption which then began replicating throughout the grid in the northeast. The result of that disturbance, the largest disruption of the power grid to that date, was a blackout that affected 50 million people in two Provinces in Canada and eight of the Northeastern United States for up to four days with a financial aftermath estimated between $8 billion and $12 billion total cost of the blackout (Stanton, Sampson, & Bloch, 2008).

Disturbances in the grid have influenced changes in regulatory efforts supporting the energy critical infrastructure. Attention to electric grid reliability increased as a result of the ubiquitous outcry from the public after the power outage in 1965 (McAllister & Dawson, 2010). Similarly, the August, 2003 blackout generated demand from the public

for an increase in the reliability of the power grid (Apt et al., 2004). When NERC was appointed as the ERO, reliability standards were written by NERC, approved by FERC, and became mandatory in 2007 (Taylor, 2009).

## NERC Reliability Standards

The 14 NERC reliability standards support the BES in North America by designating the reliability requirements for planning and operation. The standards undergo revision and updating in order to maintain alignment with changes in the industry and the country. Updates to the standards may not necessarily be performed simultaneously. Responding to situations or developments, such as an emerging security threat to equipment supporting the BES (Osofsky & Wiseman, 2013), may mandate changes in the standards to continue to provide the highest, most consistent level of reliability for the BES.

A list of the current NERC reliability standards for the electricity critical infrastructure (NERC, 2013) includes

1. Resource and Demand Balancing (BAL)
2. Critical Infrastructure Protection (CIP)
3. Communications (COM)
4. Emergency Preparedness and Operations (EOP)
5. Facilities Design, Connections and Maintenance (FAC)
6. Interchange Scheduling and Coordination (INT)
7. Interconnection Reliability Operations and Coordination (IRO)
8. Modeling, Data, and Analysis (MOD)
9. Nuclear (NUC)

10. Personnel Performance, Training, and Qualifications (PER)

11. Protection and Control (PRC)

12. Transmission Operations (TOP)

13. Transmission Planning (TPL)

14. Voltage and Reactive (VAR)

The Critical Infrastructure Protection standards, the area of concentration for this study, include eight standards supporting cyber security (Wang, Ruan, Xu, Wen, & Deng, 2010). The CIPs are the most recent addition to the NERC reliability standards. The eight cyber security CIP standards include (NERC, 2013):

1. CIP-002: Critical Cyber Asset Identification
2. CIP-003: Security Management Controls
3. CIP-004: Personnel and Training
4. CIP-005: Electronic Security Perimeter(s)
5. CIP-006: Physical Security of BES Cyber Systems
6. CIP-007: Systems Security Management
7. CIP-008: Incident Reporting and Response Planning
8. CIP-009: Recovery Plans for BES Cyber Systems

This research focused on studying subject matter expert opinions on the effect of cyber security standards, CIP-002 through CIP-009, on the reliability of the BES.

The standards are constantly reviewed for the possibility of revising or updating. A motivating factor for entities to comply with the NERC reliability standards may exist in the enforcement and fine assessments designated for violations of the standards (Stapleton, 2009). Examination of a single NERC standard (the CIPs) in this study may

provide encouragement for similar exploration of the remaining standards in an effort to increase grid reliability. Additionally, an important reality to remain cognizant of is the constant increase in complexity of the grid and its interconnections as well as the management of risk that should accompany such complexity. And while the elaborate interconnectivity of the electrical grid is increasing, so are the threats of sabotage to the computers and electronic components that operate and support the grid (Harkins, 2013).

## Cyber Security and the Energy Critical Infrastructure

Industrial Control Systems (ICS) and Supervisory Control And Data Acquisition (SCADA) systems are utilized to control industrial equipment that supports the operation of critical infrastructure organizations. Control systems security can differ significantly from security employed on IT systems (personal computers, servers and systems running versions of Microsoft's Windows operating system, for example) due in part to the specialized hardware and software running on ICS (Stouffer, Falco, & Scarfone, 2011). IT systems typically share intricate interconnectivity through networking which enables those systems to easily share information, a function that society has become increasingly dependent on over the few short decades that the internet has been in existence. Included with the interconnectivity of IT systems are risks of security compromises that could (and have) resulted in catastrophic loss of control of personal and financial information and identity theft, at a minimum (Nugent & Raisinghani, 2002).

Control systems have historically functioned as stand-alone, or air-gapped, systems that did not require connectivity to the internet or other systems in order to perform their functions. Communication between the control systems and the equipment it was monitoring or controlling were the sole connectivity requirements. Proprietary

protocols operating on unique hardware and software systems (Stouffer et al., 2011) utilized by ICS aided in providing security to control systems and equipment by contributing to their isolation. While these unique configurations have provided confidence in critical infrastructure security in the past, the evolution of new technology for increasing convenience and performance (Stamp, Campbell, DePoy, Dillinger, and Young, 2003) has introduced adversarial and natural threats (Stouffer et al., 2011) into the ICS landscape of our critical infrastructure entities.

ICS and IT systems configurations differ in obvious as well as obscure respects. Each type of system may produce financial impacts to an organization in the form of data compromise (IT systems) or production losses (ICS). While the risk to human life and limb may not be evident in an IT system that experiences a cyber security event, it is axiomatic that the compromise of an ICS threatens not only personnel in close proximity to the systems but persons that may be impacted by the failure of the equipment that the ICS controls (loss of power to a population, for example). The possible consequences of a failure of critical infrastructure equipment due to compromise of ICS could be acute (Stamp et al., 2003), the most serious being loss of life.

ICSs were in use prior to the 1960's (Nicholson, Webber, Dyer, Patel, & Janicke, 2012). Not until the late 1990's did Internet-based technology begin to infiltrate ICS design (Stouffer et al., 2011). Typically, ICS lags IT systems security by five to 10 years due to the isolation ICS has historically maintained (Stamp et al., 2003). In light of the increasing connectivity of IT and ICS and the resulting surge in risk of cyber security breaches to ICSs, the Department of Energy has determined four objectives intended to

increase security for control systems in the energy sector (Cardenas, Amin, & Sastry, 2008) to include

1. Measure current security;
2. Develop and integrate protective measures;
3. Detect intrusion and implement response strategies; and
4. Sustain security improvements (pg. 9).

Critical infrastructure control systems and equipment are required to be highly available. Consider if the BES in the United States were only available 50 percent of the time. This could be considered low availability, translating into power being delivered to houses for only 12 out of 24 hours in a day. Fortunately, the actual target availability percentage that the power grid strives toward is 99.999, commonly referred to as the five 9s, and is considered to be a high degree of availability (Hoover, 2000). In reality, the power grid in the United States operates between 99.9 and 99.99 percent availability (Marnay, 2007).

A significant turning point in securing critical infrastructure occurred with the terrorist attacks of September 11, 2001. As physical and cyber security increased after the attacks, the vulnerability of the power grid, particularly to a cyber-attack, became more apparent. In fact, many cyber experts agreed the electricity critical infrastructure to be the most susceptible to cyber threats (King, 2009), primarily due to the increasing connectivity of controls networks to corporate IT networks. The closed-loop architecture that provided isolation to industrial control systems and protected them from vulnerabilities for decades is rapidly being replaced with connectivity capable of providing remote access which was not previously available to segregated systems.

Events affecting critical infrastructure have illustrated the need for heightened physical and cyber security. The terrorist attacks of September 11, 2001 increased attention on the vulnerability of the energy critical infrastructure, resulting in amplified research efforts surrounding cyber security. In January, 2003, the Slammer computer worm infiltrated the Davis-Besse nuclear power plant in Ohio, disabling the Plant Process Computer and the safety parameter display system (Byres & Lowe, 2004). Fortunately, the plant was offline at the time of the Slammer infection.

Outside of the United States, a disenchanted former employee of a water treatment plant in Queensland, Australia used purloined radio parts to deliver invalid commands to a sewage plant, resulting in an excess of 200,000 gallons of raw sewage dumping into local parks and rivers in April, 2000 (Nicol, 2011). In January, 2008, other countries reported computer hackers penetrating electric utilities with extortion ultimatums, resulting in at least one case where the hackers successfully disabled power to a few unidentified cities (Gleick, 2006). There is a possibility that the United States power grid has already been compromised by foreign countries, including China and Russia, intending to deposit malicious computer code on power grid systems (Nicol, 2011). This malware may be configured such that it could be activated at a future date in an effort to disrupt the BES.

In the United States, an experiment dubbed Aurora, carried out at the Idaho National Laboratory, demonstrated a man-in-the-middle (or spoofing) hacking attack on a diesel generator (Derene, 2009). The attacker submitted successive and expeditious on/off commands to the circuit breakers connected to the generator, resulting in the generator, which was connected to a test power grid, becoming out of sync with the grid

(Nicol, 2011). Once the generator was out of sync with the normal 60 cycles per second experienced on the power grid, the generator was quickly disabled and destroyed. The experiment exemplified the results of the successful attack when the generator shuddered and jerked (Gallant, 2011), emitting black and gray smoke before grinding to an abrupt and unrecoverable halt (Derene, 2009).

In 2010, a different type of malware erupted onto the cyber security landscape. A Windows-based worm, Stuxnet which contained a programmable logic controller root kit capable of reprogramming ICSs, infiltrated an Iranian nuclear facility (Hulme, 2011). Stuxnet was the first worm designed to interface with and infect SCADA systems (Gallant, 2011). Because Stuxnet was likely transported via portable media, it did not require network connectivity in order to move from system to system (Kerr, Rollins, & Theohary, 2010). Once it was unknowingly installed on a Windows based human-machine interface (HMI), it was able to travel through the HMI to the ICS interfacing with the HMI and reprogram controllers (Gallant, 2011).

One of the greatest threats to critical infrastructure organizations exists in the fact that a template for ICS cyber security breaches has already been designed and released through Stuxnet's infection of the Iranian nuclear plant. Ralph Langer (Gallant, 2011) considers Stuxnet to be a cyber weapon that may be easily replicated by simply copying the attack vector and use of ICS functionality already written into Stuxnet. Increased complexity of the Stuxnet worm was evident in the ability of the worm to control the speeds of the uranium enrichment centrifuges while sending normal equipment indications to operators, leading them to believe that equipment was functioning within normal parameters (Nicol, 2011). Additionally, even though Stuxnet was designed for a

specific ICS target, it may be possible to substitute alternate targets in subsequent versions of Stuxnet-like code.

In Hulme's (2011) article, Michael Assante, President and CEO of the National Board of Information Security Examiners and former vice president and chief security officer of NERC, characterized Stuxnet as "a weapons delivery system" (p. 40), likening the worm to a B-52 bomber airplane. Indeed, the Stuxnet worm was written for a decidedly precise target in ICS (Falliere, Murchu, & Chien, 2011) and displayed characteristics indicating that considerable financial backing and savvy code writing were required to exercise it. Stuxnet demonstrated the ability to control equipment (Kerr et al., 2010) and cause that equipment to become inoperable (Falliere et al., 2011). Inoperable equipment on the electrical grid may cause power failures which could contribute to unreliability of the grid, leading to the conclusion that protecting against cyber-attacks through implementation of the NERC CIPs may help ensure a more reliable and stable BES.

## NERC CIP History

Starting out as the National Electric Reliability Council, a voluntary organization sprung from the Northeast blackout of 1965, NERC has been in existence since 1968 (Gent, 1995). The Northeast blackout in 2003 prompted Congress to formulate security legislation, including regulations for cyber security, for the energy critical infrastructure (Messmer, 2006). One of the outcomes of the Energy Policy Act in 2005 was the approval for FERC to designate an ERO which would have the authority to implement and enforce compliance with standards designed to increase the reliability of the electrical grid in North America (Swanstrom & Jolivert, 2009). With FERC approving

NERC as the ERO in 2006 as noted in the annual report (NERC, 2011), NERC has had authority for enforcement of reliability standards and assessment of fines only since June, 2007 (Stapleton, 2009).

In 2003 and prior to ERO approval by FERC, NERC adopted Cyber Security Standard 1200 (Lindstrom, 2005). This standard was a precursor to the NERC CIP standards. While Standard 1200 increased awareness surrounding the issue of securing the BES (Risley & Carson, 2006), the CIPs were designed specifically to protect electric utilities from cyber-attack (Lindstrom, 2005) and focused on the control systems which operate critical equipment in the utilities (Staggs, 2008). The effort required by the power industry to comply with the NERC CIPs has been likened to the initial response by companies required to comply with the Sarbanes-Oxley regulation (Stapleton, 2009). Neither of these efforts were trivial undertakings.

The NERC 1200 standard was a voluntary program (Hamaker, 2006) considered "urgent action standards" (p. 34) following the terrorist attacks of September 11, 2001 and the blackout in 2003. NERC 1200 was designed as a security standard for the energy critical infrastructure to protect BES Critical Cyber Assets against compromise (Evans, et al., 2006). The CIP standards outline a structured approach to securing organizational assets which support the BES critical infrastructure. While retaining much of the original NERC 1200 Standard from 2003, CIP-002 through 009 exceeded the previous standard by, for example, requiring identification of Critical Cyber Assets (CIP-002) after determining if an organization owns one or more Critical Assets to the BES (Staggs, 2008).

Protection and security of the electronic transmission of information throughout the BES is an objective of the NERC CIPs. CIP-002 through 009, the Cyber Security Standards, became effective on October 1, 2005 (Naedele, 2005), were finalized by NERC in June, 2006 (Ralston, Graham, & Patel, 2006) and accepted by FERC in January, 2008 (Pollet, Sikora, & Batug, 2009). Upon acceptance of the CIPs, timeline requirements were set forth by NERC for entity compliance with the CIP standards. NERC CIP implementation guidelines stated that by December 31, 2008, entities must have been substantially compliant with the standards (Staggs, 2008). December 31, 2009 was the date that full compliance was to have been achieved and auditable compliance should have been reached by December 31, 2010 (Staggs, 2008).

NERC standards are not required to be on the same revision number but may be updated in response to a change in regulation or the environment in which the standard is involved. For example, CIP-006-3c (CIP standard 006, revision 3c) is currently active while CIP-007-3a (CIP standard 007, revision 3a) is in effect. Other factors that may affect CIP revisions include events such as the terrorist attacks of 2001. Keeping the standards flexible and updated helps to ensure maximum protection for the industry involved in protection of the critical infrastructure.

Regulatory standards seem to be in a constant state of flux and revision regardless of the status they are in; under development or active (Stanton, 2011). The CIPs are no exception. Revisions to any NERC standards are performed under a Notice of Proposed Rulemaking (NOPR). This rulemaking requires a period of public review of the revision, followed by a voting process, in addition to FERC acceptance.

Currently, entities are mandated to meet minimum requirements of the CIP standards (Lindstrom, 2005) in order to avoid possible fines for non-compliance. The electricity critical infrastructure subject to NERC CIP regulation is diverse, including gas and coal fired power plants, for example, and challenged with unique equipment throughout. Different configurations supporting different companies present momentous opportunities for adversaries to take advantage of in an attempt to attack the BES. Increasing security to the Critical Cyber Assets that support the reliability of the BES is the goal of the CIP standards.

The criticality of a reliable BES has been accentuated by the ramifications resulting from historical disruptions of electrical power in the United States. These instances of interruptions in the availability of electricity in the United States prompted legislation and regulation in an effort to increase the reliability of the BES. Advancing technology in the energy critical infrastructure are evident through the development of a smart electrical grid where analog equipment is being replaced with digital equipment, multiplying the attack landscape for cyber security hackers and putting the reliability of the BES at risk. Identifying the efficacy that the NERC CIP standards have had on improving the reliability of the BES is relevant to the safety and security of the nation.

# CHAPTER 3. METHODOLOGY

There was one research question in this study: has the reliability of the North American Bulk Electric System been affected by the implementation of the North American Electric Reliability Corporation's Critical Infrastructure Protection Standards? The purpose of this study was to identify a theme or themes in opinions regarding changes in the reliability of the Bulk Electric System (BES) as a result of the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards implementation.

## Research Design

Before something is able to be managed effectively, it should be measurable (Eto & LaCommare, 2008). In order to perform measurements, a definition of what is to be measured needs to be clear. Pekrun, Goetz, Titz, and Perry (2002) explained that qualitative, exploratory analysis may be best suited to develop insights into a study, adding that quantitative research is necessary to perform a follow on, more succinct analysis into causes and effects. Newman and Benz (1998) discussed the use of qualitative methodology to identify themes and explain what those themes were.

Qualitative research is a common response to a deficient condition or lack of understanding of a phenomenon (Bloomberg & Volpe, 2008). Qualitative methods have an unequivocal interpretive element requiring the researcher to be meticulous and deterministic throughout the study, perhaps more so than with quantitative research methods (Conrad & Serlin, 2006). Additionally, areas of research with little or no scholarly literature available are fitting candidates for qualitative exploratory studies (Davis & Hoffer, 2010). Lending support to exploratory research methodology in the

energy critical infrastructure sector in the United States, a research study into the development of clean energy in Colorado and Montana was conducted via an exploratory study due to scant, if any, available scholarly literature (Davis & Hoffer, 2010).

Creswell's (2012) five approaches to qualitative research include grounded theory, narrative research, ethnography, case studies and phenomenology. Qualitative exploratory inquiry, a social research methodology, often encompasses paradigms including naturalistic, positivist, post-modern and constructivist (Seale, 1999). The qualitative exploratory inquiry methodology chosen for this study was influenced by a narrative research approach. Narrative inquiry relies on stories told by participants who communicate (verbally or written) their experiences of an event or action or a series of events/actions which may then be ordered chronologically (Creswell, 2012).

Holloway and Biley (2011) state that qualitative researchers should tender a story through their study, a story rooted in the evidence of the research but spotlighting the meaning of the evidence more than the measurements performed in the study. This reasoning strengthened the choice to formulate an adapted narrative research approach for this study. The semi-structured interviews allowed the participants to be as brief or verbose as they desired during their discussions of their opinions and experiences with CIP implementations and BES reliability. The open-ended configuration of the interview questions encouraged conversations between the researcher and the participants, resulting in the potential for additional data which may have gone unexplored under a more restrictive research design.

In narrative research, questions asked by the researcher are chronological or story-type questions involving the participants' experiences over a period of time (Creswell,

Hanson, Clark Plano, & Morales, 2007). The chronology focus of the narrative approach adapted for this study illuminated timelines of entities' implementation of the CIP standards. Within the narrative process in qualitative research, interviews may involve career or life stories (Jones, 2013). This study's participant story-telling was shorter than life or career stories due to the fact that the CIP standards had only been implemented for a limited time.

Given (2008) stated that "researchers explore when they possess little or no scientific knowledge about the group, process, activity, or situation they want to examine but nevertheless have reason to believe contains elements worth discovering" (p. 327). With a scarcity of research on the topic of interest, Jones (2007) exercised exploratory methodology in a study rooted in a retail industry in the United Kingdom. Bowman (2004) stated that marketing managers "often use exploratory research to learn about the market" (p. 1). To date, scholastic or professional research into the effect of NERC CIP reliability standards on (BES) reliability has yet to be documented.

Semi-structured interviews, a malleable interview method suitable for smaller research projects (Drever, 1995), comprised the data collection methodology for this study. The interviews were performed via telephone due to the large geographic representation of the NERC regions throughout the United States. Telephone interviews are useful when the likelihood is high that the researcher will only get one chance to interview the participants (Cohen & Crabtree, 2006). Face to face interviews have a history as a preferred interviewing method, but telephones are a common communication tool (Cachia & Millward, 2011) and were sufficient for this study. Additionally, in-person interviewing would have been cost prohibitive for the researcher.

Semi-structured interviews employing open ended questions stimulate depth of responses from participants (Dearnley, 2005). The open-ended question format implemented in this study offered participants the opportunity to expand on their answers if they desired to do so. Semi-structured interviews also afforded the researcher latitude to ask probing questions and look for additional information selectively according to the answers provided by the participants. As such, the semi-structured interview configuration supported the intent to conduct the inquiry into the phenomenon being studied, allowing themes to materialize instead of starting the study with pre-conceived notions and proceeding with trying to prove them (Hand, 2003).

Standard practices for recording interviews include the use of video cameras or audio recorders or scribing notes (Whiting, 2008). Audio recordings were performed and hand-scribed notes utilized during the interviews for this study. The regulatory atmosphere surrounding the reliability standards may have generated some apprehension, either real or perceived, for current entity members (for example, regular full-time employees) wishing to partake in the study. Recording interviews may have caused hesitation in potential participants. Therefore, all participants were assured, verbally and in writing, of complete confidentiality with respect to their involvement in the study.

The hand-scribed notes created from the interviews were input into a removable drive on the researchers' personal computer after completion of the interview in order to minimize distractions (keyboard clacking) during the interview. Precautions utilized to protect participants and the data that was generated from the interviews included storage of original data sheets (hand-written notes), audio recordings and any other data gathering material in a locked safe under sole control of the researcher. Hardening

(encryption, password protection) of the removable computer drive (where the transcribed data was stored) ensured protection of electronic data.

The interview data was organized such that it would be a monumental, if not impossible, task for a third person to identify individual participant responses. Anonymity safeguards included reference to participants by general terms and coding (Participant 1 identified as P1, Participant 2 identified as P2, and so forth) and reference to NERC regions (Region One, Region Two, and so forth), as applicable, rather than specific entities within the regions. In addition to regions, the functional entity from the sample frame (e.g., Generator Owner, Transmission Owner, and so forth) that the participant belonged to was used, if applicable, in place of specific companies that the participants were or had been associated with. Upon completion of the research, confidential and sanitized information regarding the results of the study was offered to all participants.

## Sample

The population from which the sample frame was defined, and the samples of participants for the interviews chosen, included all 18 functional entities in NERC (NERC, 2011). This population included:

1. Standards Developers
2. Compliance Enforcement Authorities
3. Reliability Assurers
4. Planning Coordinators
5. Transmission Planners
6. Resource Planners

7. Reliability Coordinators
8. Balancing Authorities
9. Market Operators (Resource Integrators)
10. Transmission Operations
11. Interchange Coordinators
12. Transmission Service Providers
13. Transmission Owners
14. Distribution Providers
15. Generator Operators
16. Generator Owners
17. Purchasing-Selling Entities
18. Load-Servicing Entities

Each of the eight regions of NERC is comprised of organizations which include these functional entities. Some regions have higher concentrations of functional entities due to their geographical location. For example, while the Western Electric Coordinating Committee is the largest region, geographically (Shin, Gibson, Wangen, & Perez, 2011), it does not have the population density of other regions such as the Reliability First Corporation.

The sample frame for this study included a sub-section of eight functional entities taken from the population. This sub-section was comprised of entities involved in the reliability of the BES. The level of engagement of the entity in reliability activities varied depending on their responsibilities. While the level of engagement was not within

the scope of this study, individual opinions regarding the effect of the CIP standards on the reliability of the BES was the focus in answering the research question.

The sample frame of the eight functional entities derived from the research population included:

1. Reliability Assurer
2. Reliability Coordinator
3. Balancing Authority
4. Transmission Operator
5. Interchange Coordinator
6. Transmission Owner
7. Generator Operator
8. Load-Servicing Entity

Purposive sampling, sometimes termed expert or judgmental sampling, is one of three categories of non-probability sampling (Battaglia, 2008). In this study, participants were purposefully selected based on specific, non-random criteria (Teddlie & Yu, 2007). The use of purposive sampling for participant selection in this study offered the researcher the opportunity to select individuals with potentially abundant information (Jebreen, 2012) that would most likely be applicable to the research question. Interview participants were selected from the eight functional entities specified in the sample frame. The continental United States was the geographic boundary from which the participants were selected. Current or former involvement in one or more of the eight NERC regions was additional inclusion criteria for participation in this study.

Any organizations not required, by regulation, to comply with any NERC CIP standards were excluded from this study. An example of an exclusion included nuclear power plants. The exclusion criteria also applied to citizens of Alaska and Hawaii since these two states are not included in the NERC regions in North America (McClelland, 2012). Figure 1 illustrated the inclusion of Canadian geography in the NERC regions. The Federal Energy Regulatory Commission (FERC) is not responsible for energy regulation in Canada, resulting in those areas being excluded from this study.

To recruit study participants, a management individual at the Edison Electric Institute (EEI) was contacted via email with a description of the study and the request for participants. EEI was given the researchers' contact information for potential participants to inquire. This method of communication offered anonymity and confidentiality to potential participants such that the researcher had no knowledge of participant information unless contact was initiated by the individual. Once the researcher was contacted, consent forms were emailed to the interested person for signature indicating interest in participating in the study and consent to be audio recorded.

## Instrumentation/Measures

Proceeding with the exploratory study format, semi-structured interview questions were developed for the telephone interviews. Research interviews performed over the telephone or in person have definite differences, the most obvious being the lack of a visual interface between the interviewer and the interviewee during telephone interviews (Irvine, Drew, & Sainsbury, 2013). With a lack of visual input for the researcher during the interviews, this study did not rely on interviewee body language to add to the data collected during the interviews. The information gained from participants through

answers to the questions, probes and discussions was the single method of data collection.

During semi-structured (and unstructured) interviews, it is not uncommon for interviewees to answer interview questions by telling stories (Abell, Locke, Condor, Gibson, & Stevenson, 2006). For this study, participant engagement and story-telling was encouraged so that their experiences with the implementation of the CIP reliability standards would offer deeper insight into how participants felt that the standards have affected BES reliability. Participants' story telling included details of their experiences and their opinions of those experiences. Those details contained data that may not have come to mind if they were simply answering questions when prompted by the researcher.

The semi-structured interview instrument used in this study was adapted from an existing instrument developed for semi-structured interviews in a study of coping strategies toward discrimination in academic settings (Kim, Hall, Anderson, & Willingham, 2011). The structure of the Kim et al. (2011) instrument was maintained but the content was modified to reflect the questions applicable to this study. The architecture of this instrument allowed the opportunity for probing questions. Probes were employed during the interviews, as appropriate, to offer a more in-depth discussion of questions that were particularly interesting to the researcher (Bariball & White, 1994).

## Data Collection

Semi-structured interviews include aspects from structured and unstructured interviews (Cachia & Millward, 2011). Open-ended questions comprise the interview which gives the interviewer an adjustable framework to work within (Dearnley, 2005). Having the latitude to probe and ask participants for additional information in areas of

interest was an important component of the data gathering phase of the study. Therefore, a semi-structured architecture for data collection was best suited for this study.

In preparation for the interviews, consent forms were sent to participants. These forms were signed and returned to the researcher prior to commencement of the following steps for the interviews.

1. Prior to the interview, the researcher contacted participants either by telephone or email, introduced herself, and arranged a time and date for the telephone interview. The researcher informed participants that the interview should last approximately 30 minutes. Additionally, the researcher asked the participants to contact her should the scheduled time for the interview need to be modified, and ensured that the participants had her contact information.

2. The day of the interview, the researcher called the participant promptly at the agreed upon time for the interview. Once contact was established, the researcher informed participants when the interview was about to begin. The researcher informed participants that they would be recorded during the interview, asked for confirmation of agreement to be audio recorded and, upon confirmation, began the audio recording. The researcher instructed participants that all information shared with the researcher was confidential. Additionally, their interview data would be sanitized before being published in the dissertation results. The researcher reminded participants that they were free to stop the interview at any time, for any reason. The researcher also explained that if participants withdrew from the study, their data would be destroyed. The researcher asked participants if they had any questions, if they understood everything that had been explained to them and if they were ready to begin. When participants agreed that they were ready to start the interview, the researcher asked the first question.

3. Upon completion of the interview, the researcher asked participants if there was anything they wished to add. Once participants confirmed that they did not have any additional information, the researcher asked participants if they had any questions or if they wanted to change any of their answers. The researcher asked participants to contact her if they thought of something after the interview that they wished to be included in their interview. Lastly, the researcher informed participants that they would be receiving compiled, sanitized results of the study after all of the interviews had been completed.

Taking into consideration the number of interviews required for this study, Mason (2010) offered that fewer study participants are required when the study has a narrow focus and participants are experienced in the study topic. The specificity of this study required that participants be knowledgeable and experienced with the NERC CIP standards, therefore qualifying this study, according to Mason (2010), as having a narrow focus with experienced participants. The permissible sample size of participants for the study, as suggested by Guest, Bunce, and Johnson (2006), indicated that data saturation (the threshold where the researcher detects no dissimilar leitmotif in the data examined) be utilized to assist in determining the number of interviewees.

Guest et al. (2006) suggested,

> Using data from a study involving 60 in-depth interviews with women in two West African countries, the authors systematically document the degree of data saturation and variability over the course of thematic analysis. They operationalize saturation and make evidence-based recommendations regarding nonprobabilistic sample sizes for interviews. Based on the data set, they found that saturation occurred within the first 12 interviews, although basic elements for metathemes were present as early as six interviews. (p. 59)

The target number of participants in this study was originally determined to be a minimum of 8 interviews with up to 12 deemed reasonable. However, a literature review of Hancock, Windridge, and Ockelford (2007) suggested that between 20 to 60 interview participants was adequate. In this study, there were no preconceived notions regarding at what point (how many interviews) data saturation may occur. By verifying that patterns which emerged during the data collection were consistent and new data was redundant (Bowen, 2008), confirmation that data saturation was achieved assured that the process of data collection did not end prematurely.

After a review of the scholastic literature from Guest et al., (2006) and data from Hancock et al. (2007), a minimum of 12 participants with a maximum of 40 was determined acceptable. However, if data saturation was attained prior to the completion of 40 interviews, the data collection portion of the study was deemed complete.

## Data Analysis

The data analysis method chosen for this study was thematic analysis using an inductive approach. Inductive techniques are appropriate as either a distinct mode of analysis or as an intrinsic philosophy (Jebreen, 2012). For this study, the former mode was applicable. Jebreen (2012) indicated that "choosing an inductive approach through thematic analysis (a 'data driven' approach) for the study determines that the objective of the study is to obtain an understanding of a phenomenon, rather than to test a hypothesis" (p. 170). Thematic analysis has been widely utilized in broad and differing areas of research including mathematics, the social and physical sciences, and medicine (Boyatzis, 1998).

Deductive analysis involves a researcher bringing their theoretical proposition to the research, from which a theme is developed. Inductive analysis is not influenced by preconceptions but draws a theme from the study's raw data (Joffe, 2011). The inductive approach to thematic analysis is a four step process. The steps include researcher immersion in the data, coding of the data, developing categories from the data and finally resulting in the cultivation of themes (Green et al., 2007).

The methodology involved in the data analysis for this study was not a singular focus on the qualitative. In this study, analyzing the data and presenting the results in a format that was scholastically as well as professionally comprehensible resulted in the

combination of qualitative and quantitative techniques, as suggested by Mays and Pope (1995).

> Another option is to combine a qualitative analysis with some quantitative summary of the results. The quantification is used merely to condense the results to make them easily intelligible; the approach to the analysis remains qualitative since naturally occurring events identified on theoretical grounds are being counted (p. 112).

Qualitative data analysis, as described by Zhang and Wildemuth (2009) "was developed primarily in anthropology, qualitative sociology, and psychology, in order to explore the meanings underlying physical messages" (p. 1). This study was not searching for underlying meanings in data but analyzed data for a theme or themes that arose from interviews with experts in the field of the NERC CIP standards.

## Validity and Reliability

Regarding validity and reliability in qualitative inquiry research, Morse et al. (2002) attest that "Without rigor, research is worthless, becomes fiction, and loses its utility" (p. 2). Applying rigor to validity and reliability in qualitative research involves several steps. Rigor in reliability includes continuous auditing of decisions during the data gathering process coupled with triangulation while rigor in validity involves, at a minimum, constant observation, detailed journaling or record keeping and triangulation (Long & Johnson, 2000). Rigor in qualitative research is naturalistic while rigor in quantitative research is rationalistic (Morse et al., 2002).

Quantitative research focuses on reliability and validity in order to determine the quality of the research (Zhang & Wildemuth, 2009). The qualitative equivalent to reliability and validity is trustworthiness which is achieved through credibility, transferability, dependability and confirmability (Shenton, 2004; Zhang & Wildemuth,

2009). Table 2 was adapted from Krefting (1991) to explain what criteria were implemented in order to achieve trustworthiness in this study.

Table 2. Strategies for Achieving Trustworthiness (adapted from Krefting, (1991) pg. 217).

| Strategy | Criteria |
|---|---|
| Credibility | Reflexivity-the researcher was part of the qualitative research process and assessed the influence of their background, interests and perceptions on the process.<br><br>Triangulation of data sources-a range of participants: cyber security experts, auditors, management, consultants and contractors. Triangulation of data analysis-thematic inductive analysis performed by the researcher was confirmed with NVivo 10 qualitative research software.<br><br>Interview technique-repetition of questions, internal consistency of interviews.<br><br>Researcher authority-practiced interviewing skills prior to data collection. Researcher is also a cyber security expert in the energy critical infrastructure sector. |
| Transferability | Dense description-provided participant information (cyber experts, auditors, and so on). |

Table 2 (continued). Strategies for Achieving Trustworthiness (adapted from Krefting, 1991, pg. 217).

| Strategy | Criteria |
|---|---|
| Dependability | Triangulation-as performed in Credibility.<br><br>Code-recode procedure-researcher assigned codes during the data analysis phase, then recoded the same data several weeks later and compared the results. |
| Confirmability | Triangulation-as performed in Credibility.<br><br>Reflexivity-as performed in Credibility. |

*Note:* From "Rigor in qualitative research: The assessment of trustworthiness" by L. Krefting, *The American Journal of Occupational Therapy*, *45*(3), pg. 217.

Regarding the transferability strategy, Lincoln and Guba (1985) expressed that the researcher is not responsible for providing the measure of transferability but rather to supply appropriate information from which others may make a transferability determination.

Triangulation refers to the reviewing of data which was collected through the use of different collection methodologies (Oliver-Hoyo & Allen, 2006). Triangulation may also refer to the use of quantitative research methods combined with qualitative methods in the development of research (Haase, Heiney, Ruccione, & Stutzer, 1999). This study employed triangulation during the data collection phase of the research through interviewing not only cyber security experts in the field of NERC CIPs but also

managerial individuals. Audit, compliance and risk experts also participated. Additionally, individuals experienced implementing CIPs for electrical utility entities serving large populations (millions of customers) as well as individuals experienced with smaller to medium sized entities (thousands of customers) were interviewed.

Methodical design of the interview questions was followed by a rigorous field test with subject matter experts in the field of NERC CIPs before participant recruitment commenced. Modification of an existing interview instrument reduced the likelihood of errors in the research data as compared with a new instrument. Existing interview instruments have previously undergone usage and verification through past studies. Through that process, opportunities for correction and modification aide in the development of an appropriate data gathering instrument, making those existing instruments preferable to attempting the design of a new, untested instrument.

The field test of the interview questions included technical and non-technical subject matter experts. The technical subject matter experts examined the questions for technical accuracy and applicability in the field of NERC CIP standards. The non-technical subject matter expert, a practicing psychologist, reviewed the questions as well as the interview protocol from a human interaction perspective. The rigor of combining technical and non-technical field testing offered increased reliability and validity to the adapted interview instrument.

In-person interviews allow researchers to watch body language and other cues from the participants that are not visible in telephone interviews, giving the interviewer more opportunities to secure data. Conversely, body language of the interviewer, often used to acknowledge the participant during the interview (Murray, 2003), is not seen by

the participant during telephone interviews. Performing interviews over the telephone at a distance requires that the researcher listen intently to the responses of the participants to confirm data is being recorded accurately. The telephone interview configuration employed in this study included audio recordings of the interviews to assist with data collection and verification.

## Ethical Considerations

Ethical issues are a substantial consideration when performing interviews (Kajornboon, 2005). Assuring participants that their confidentiality would be maintained before, during, and after this study was of the highest priority. The researcher explained to participants that neither their names nor any personal information would be associated with any interview data. Also, the researcher confirmed with participants that they understood their option to decline or withdraw from the interview at any time. The researcher also requested that the interviewees acknowledged that they understood those statements of confidentiality and the option to end their participation in the study.

Kajornboon's (2005) potential ethical issues in interviewing are expressed in Table 3 along with the planned mitigations, if needed, for this study.

Table 3. Potential Ethical Concerns (adapted from Kajornboon (2005), pg. 8).

| Potential Ethical Concern | Mitigation |
|---|---|
| Explain the purpose of the study | Informed participants what the study was about and their role. |

Table 3 (continued). Potential Ethical Concerns (adapted from Kajornboon (2005), pg. 8).

| Potential Ethical Concern | Mitigation |
|---|---|
| Guarantees, promises, and incentives | No incentives offered for participation. |
| Effect of the interview on participants: stress, regulatory repercussions (real or perceived), peer pressure | Described the confidentiality and anonymity protections of the data from the interviews as safeguards for participants. |
| Confidentiality and anonymity | Only the researcher had study data access. |
| Consent | Informed consent obtained via forms signed by participants and securely stored by the researcher. |
| Data availability/ownership | Raw data: researcher only.<br>Results data: owned by the researcher, offered to participants. Published dissertation: publically available. |
| Effect on mental health | Very low risk, no mitigation planned. |
| Ethical advisor | None required. |
| Pushing for data | If any hesitation or reluctance was indicated by the participant, the researcher moved on and did not continue probing. |

*Note:* From "Using interviews as research instruments" *E-Journal for Research Teachers*" by A. B. Kajornboon, *E-Journal for Research Teachers*, pg. 8.

Research ethics are in place to protect participants from any harm or suffering as a result of the research in which they are participating (Swanson & Holton III, 2005). In order to protect the anonymity and confidentiality of the participants in this study to the

greatest extent possible, consent forms containing the names of interviewees were coded. Any reference to participants was expressed per the applicable code. For example, Participant 1 was the code assigned to the first participant, Participant 2 for the second participant, and so on. If at any time a participant expressed the desire to terminate participation in the study, any record of that participant was destroyed.

Ensuring participant confidentiality in this study was essential to ease potential fears of reprisal, retribution or retaliation from a regulator, company, corporation or individual. Security measures enacted to protect the confidentiality of the interviewees and their responses to the study questions, specifically the electronic data and audio recordings from the interviews, included storage on an encrypted, two-factor authentication password protected portable computer drive (removable media) which was designated specifically for storage of data related to the study and contained no other data, applications or programs. Hard-copy data, such as hand-scribed notes, were stored in a combination locked fire-proof safe. Hard-copy data requiring destruction was accomplished via cross-cut style paper shredder. Destruction of electronic data, when required, was performed by deleting files from the portable drive.

# CHAPTER 4. RESULTS

## Introduction: The Study and the Researcher

This chapter presents the data collected and analyzed, the findings, and the results of the study. Semi-structured interviews provided the data collection methodology for the data to answer the research question regarding the effect of the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards on the reliability of the Bulk Electric System (BES). The organization of this chapter includes an explanation of the researchers' interest in the study topic, a description of the sample used for data collection, a discussion of the methodological approach as it applied to the data analysis and results, and concluded with a summarization of the findings.

Several factors influenced the researchers' interest in the topic of this study. An increase in cyber-attacks on critical infrastructure in the United States (Order, 2013) has prompted increased awareness of the vulnerability surrounding the BES. Increased legislation in response to cyber-attacks has resulted in regulation, including the NERC CIP standards, in an effort to protect the BES. A scholastic study on the efficacy of the implementation of the CIP standards on the reliability of the BES had not been documented at the time this research was undertaken.

A professional background implementing cyber security programs in the nuclear power industry equipped the researcher with experience necessary to understand the concepts surrounding the security of the BES. When the Federal Energy Regulatory Commission (FERC) issued order 706-B (Blanton, 2010) which potentially mandated nuclear power plant regulation under the NERC CIPs, the nuclear industry responded

with an explanation to exclude nuclear from NERC regulation. As an author of a cyber security plan for a nuclear power plant, the researcher became intimately acquainted with FERC, NERC, and the CIP standards during the process of modifying the cyber security plan to include the FERC accepted exception for nuclear from the CIPs.

Purported claims of increased reliability of the BES as a result of CIP standards implementation have lacked supportive scholarly documentation, piquing the researchers' interest in BES reliability and the CIP standards. This interest resulted in the design and development of an exploratory study of opinions from professional individuals experienced with CIP implementation regarding CIP efficacy on BES reliability. The choice of exploratory methodology was supported by scholarly literature on the topic to include, but not limited to, Bacchetti (2002), and Zikmund et al. (2012). During the process of the study, the researcher joined an organization where access to other researchers working on BES reliability was abundant. As a result, the researcher became not only scholastically but professionally immersed in the research question for the study.

This was the first qualitative study the researcher had performed. A member of the researchers' dissertation committee was a practicing psychologist with whom the researcher engaged in order to hone her interviewing skills. The rigorous field test coupled with interview practice adequately prepared the researcher to be an unbiased research instrument for the data collection. The researchers' experience in cyber security and the electricity industry ensured adequate technical understanding of the participant feedback as well as providing an empathetic perspective that was useful when the application of probing questions was indicated.

## Description of the Sample

The target participant sample frame was designed to be a sub-set of the population of the 18 NERC functional entities. Eight entities were purposefully chosen as the most appropriate group to provide applicable data to address the research question. Recruitment of participants was performed through contact with Edison Electric Institute (EEI). NERC entity membership, along with CIP implementation experience, was inclusion criteria.

EEI recruitment produced one participant who later withdrew from the study. Under the direction and guidance of EEI executives, participant recruitment was expanded outside of the eight originally intended functional entities while retaining the requirement of CIP implementation experience. Membership within a NERC entity was expanded to include individuals supporting CIP implementations within NERC entities (for example, contractors and other independents) in lieu of requiring direct entity membership. The modified participant recruitment methodology generated increased interest in participation and a sufficient number of participants were recruited.

Some participants were regular full time employees of a functional entity. Other participants included contractors, consultants and individuals not directly employed by an entity as a regular employee. Table 4 represents regular full time entity employees, by job title, for the position they held within the entity at the time of their interview and the approximate customer base the entity provided electricity to, supported, or served. Multiple individuals with the same job title were represented in parenthesis next to the job title. Some participants chose not to reveal the customer base of the entity for which they were employed or contracted to work for. Where possible, in cases of unknown or

undetermined customer bases, an estimate was approximated through open source information from the Internet.

Table 4. Participants Directly Employed by a Functional Entity

| Position Description | Customer Base |
|---|---|
| Auditor (2) | Unknown |
| Manager | Unknown |
| Superintendent | <50,000 |
| Compliance Manager | <350,000 |
| Strategist | <five million |
| Director | >600,000 |

Table 5 represents participants not directly employed by a functional entity. It was not uncommon for some of these individuals to have assisted with CIP implementations in more than one entity with different customer bases.

Table 5. Participants Indirectly Employed by a Functional Entity

| Position Description | Customer Base |
|---|---|
| Cyber Security Advisor | Unknown |
| Consultant | Unknown |
| Cyber Security Consultant | >one million |
| Cyber Security and Compliance Consultant | Entity supplied over 50 percent of the power for over four and a half million customers |
| Cyber Expert/Researcher | Unknown |
| Project Manager/Engineer | Unknown |

## Methodological Approach as Applied to the Data Analysis

Carspecken's (1996) five stage method for critical qualitative research has been utilized when performing research coined as critical qualitative research, or critical ethnography. This model has been implemented in the nursing profession as a way to study social phenomenon (Hardcastle, Usher, & Holmes, 2005). The five stages of the model include initiating a basic record to uncover what is happening; an analysis of what is happening from the researcher's point of view; data gathering through interviews, observations or other methods; a discovery phase and analysis of systems; and explaining relationships between systems (Hardcastle et al., 2005).

Carspecken's (1996) methodology has been viewed as a fruitful, adaptable avenue for research in critical ethnography (Holmes & Smyth, 2011). As applicable as the five stage model may be for critical ethnography, this study did not fit neatly into the same model. However, the basic ideas in the model held a sound basis which was adaptable as a model for this research. Therefore, a modified version of Carspecken's (1996) model was employed in combination with an integrated research model designed by Kaptein and Schwartz (2008) in a study of the effectiveness of a management instrument, business codes.

The integrated research model developed by Kaptein and Schwartz (2008) took into account multiple factors that influenced the effectiveness of business codes. The expectations of the stakeholders of a business, combined with external components, were input into the model. Once internal to the model, the content of the business codes was developed through a process which began with the corporations' objectives and proceeded through the development of the code(s), implementation and administration, and conduct of the organizations' employees, including management. The effect this process had on the corporation was the last step of the internal section of the model, at which point the model was exited with a review of the stakeholder and social effects of the business codes (Kaptein & Schwartz, 2008).

The adapted model for this study incorporated concepts from Carspecken's (1996) qualitative inquiry model and the integrated research model created by Kaptein and Schwartz, (2008). The adapted model engaged in this study included 5 steps:

1. Identification of a potential gap in real and perceived BES reliability which resulted in the development of a research question.
2. Purposive sampling implemented for participant selection.

3. Collection of data through semi-structured interviews.

4. Thematic inductive data analysis of themes, including data input into NVivo qualitative software to bolster trustworthiness of results and conclusions.

5. Conclusions and recommendations.

The first step in the model was appropriate not only from a scholastic perspective but applicable to an operations and management environment tasked with implementation and maintenance of the CIP standards. At some point, stakeholders in entities required to comply with reliability standards may be asking questions regarding the level of compliance the organization has achieved as well as identifying areas for improvement during implementation of future standards revisions.

The study's model remained viable as the criteria for participants expanded in response to a lack of participation in the study. Requirements for participation broadened from the sample frame (the eight functional entities) to the population which encompassed all 18 NERC functional entities. Additionally, the model allowed seamless progression of the research into the thematic inductive data analysis process. This transition supported the level of rigor required for data trustworthiness in this qualitative exploratory inquiry study.

## Data and Results

In a format suggested by Mays and Pope (1995), this section presented the qualitative data for the study combined with a quantitative summary of the results. Data from each participant interview was organized in a qualitative format that included insights and details from participants that went beyond simply answering the interview questions. The qualitative data presentation and analysis was followed by a quantitative

summary (figures, charts, or tables, as appropriate) illustrating the results of participant answers to the interview questions. This quantitative summary of results was attained by inputting the qualitative data analysis into NVivo software where the graphical renditions of the data were then generated. The NVivo software renderings of the graphics were presented in this section of the chapter. The analysis of the data resulted in the generation of themes which are presented at the end of the Data and Results section.

**Qualitative Data Presentation**

The presentation of the data results followed a sequential format. The qualitative data presentation began with response and discussion data from the interview with Participant 1 (P1). The data presentation continued with Participant 2 (P2), and so on.

**Participant 1 (P1)**

In a discussion about the power grid (BES) in general, P1 mentioned that local power companies are concerned that federal agencies are unaware of what it takes to deliver power. P1 explained that the system requires greater attention than is currently being given to it. P1 stated that "electric power has never been more in demand" than it is currently. P1 did not feel that "regulators or DHS or politicians had a common standard for system recovery time" in the event of an outage, regardless of the cause of that outage.

Management and regulation of the BES is a complicated process. P1 expressed an impression that "the legislature…at both the state and national level…don't really have much understanding of how the system works." There seem to be inconsistencies within the operation of the BES itself. P1 said that "systems are governed and managed

in a completely different way. Transmission is a national issue. The distribution side of things is very fragmented. Much less so on the transmission side."

Local power companies and smaller utilities may be exempt from regulatory responsibilities to the BES but may experience some concerns that differ from large transmission and generation facilities or other utilities. P1 conversed about ride along experiences (a citizen riding along with a power company employee driving out to remote locations for equipment checks) where the utility individual expressed a great concern regarding what one person could do with a six-pack (of alcohol) and a gun. Shooting transformers may result in oil and other liquid leakages in addition to disabling the equipment. P1 made reference to the 2013 incident in California (Metcalf) where gunfire damage was inflicted on transformers.

Regulation schemes include a violation and fine component for non-compliance. Fines vary depending on the severity of the infraction. Small utilities trying to meet their bottom line and serve their customers may not be able to absorb a significant fine where a large utility could. When asked if regulatory fines might be a factor in driving compliance with the CIP standards, P1 responded, "A very large fine is going to drive behavior as long as the cost of that fine exceeds, you know, your tolerance for other things."

P1 expressed an opinion concerning how the CIPs were interpreted by the people involved in the implementation, enforcement, and auditing of the standards. Ensuring that everyone is operating with the same understanding of the standards is a key to confirming that the standards are applied consistently. P1 stressed that there needs to be a common use of vocabulary in the CIP environment. NERC compiled a glossary of terms for the

CIP standards, but the concern regarding a common vocabulary extends beyond that glossary.

**Participant 2 (P2)**

P2 expressed concern over inconsistencies across the regulator, NERC. Examples of inconsistencies include a lack of understanding, by NERC, of the CIP standards which may have resulted in inadequate training of the regional auditors responsible for performing CIP audits, such as "one set of rules for one region and another set of rules for another region and sometimes they were in direct conflict." P2 gave an example of auditors breaking their own rules by requesting to take an entity's documentation offsite when NERC had indicated that auditors were not allowed to take any entity documents offsite. These inconsistencies have the potential to become significant when one entity, organization or company spans multiple NERC regions.

It was the opinion of P2 that there is "too much time doing paperwork and not enough time maintaining the system and improving the security" in order to increase the reliability of the BES. The energy critical infrastructure risks degradation when people that know how to maintain systems are pulled away to do CIP paperwork. If a piece of equipment supporting the BES is in need of maintenance, the person responsible for that equipment feels as though "I can't get to it right now, I gotta work NERC CIP. If this [piece of equipment] goes down, I lose the plant. If this [CIP documentation] goes down I lose a million dollars a day", referring to the maximum fine allowed by law for blatant non-compliance of a NERC reliability standard. With regard to the implementation of the CIP standards, it was P2's opinion that "we are not demonstrating security, we are documenting security."

The cost of complying with NERC CIP standards goes beyond violations and fines. P2 stated that "companies that couldn't spend $50,000 to upgrade their control system [are] spending $100,000 on documentation controls so that they could *prove* to NERC that they had done what they said they had done." A situation like this could impact the cyber security controls protecting equipment which supports the BES and, therefore, potentially affect the reliability of the BES. Similar to comments made by P1, P2 conveyed,

> One company had the most sophisticated network protection I had ever seen. NERC came in to look at their architecture and wanted them to tear it all out because they did not understand it. It took the company 6 months to convince NERC that this was the best protection they could do for the control systems the company was running.

Finances are a factor in meeting compliance, especially for entities that are "running on a ragged edge. Every company is going to make their decisions based on dollars." Fines from NERC for non-compliance can reach $1 million per day, per incident, with a 3x multiplier if the infraction was intentional or showed blatant disregard. These numbers make the legal department of an organization very nervous. One misstep in not providing proof to auditors that the entity is complying with standards could result in a fine that could wipe out profits for a small utility. P2 continued, "now think about that: we fail to provide a piece of paperwork that proves that we're doing this…and we could lose a million dollars a day."

P2 was contracted, by the CEO of a company providing electricity services to a customer base of over 25 million, to perform cyber security consulting. After completing an assessment of the cyber security program for the entity, P2 informed the CEO that it would be necessary to spend over $15 million to provide adequate cyber protection for

the entity and comply with the NERC CIP standards. The CEO responded by saying that he had never heard of a utility being hacked. P2 responded, "If you were hacked, would you tell the public?"

**Participant 3 (P3)**

P3 added to P2's comments regarding the costs associated with CIP compliance. P3 stated that their entity had budgeted over $500,000 to comply with just one of the standards within the CIP suite. Furthermore, that money only covered the current year. Additional funding would be required for subsequent years as the program maintained their compliance. P3 expressed that money being spent on the CIPs is money taken away from reliability and customer services, not to mention, as P2 pointed out, equipment upgrades and maintenance.

The money aspect of compliance with standards also reaches into testing and exercising of plans and processes for equipment, emergency response, and recovery from cyber-attacks. P3 outlined a situation where an exercise was cancelled by their compliance group, citing potential non-compliance with one of the CIP standards as the reason. The logic behind the compliance groups' action was that if a potential weakness was found, it may need to be reported and the entity risked receiving a fine from NERC. P3 questioned the compliance group about their decision, stating that it was impossible to discover and fix weaknesses if exercising and testing was not allowed to find those weaknesses. The compliance group continued to refuse the testing, resulting in a catch-22 situation.

Similar to P2's comment regarding the arduous amount of paperwork required to comply with CIP standards, P3 conveyed that the CIPs require entities to be "very

heavily documented….documentation is extremely intensive." As previously noted by P2, a side effect of the paperwork required for compliance exists where the primary people that were responsible for maintaining equipment were removed from that equipment to generate compliance paperwork for the CIPs. The reasoning behind using primary support people to complete compliance paperwork for that equipment is expertise. The most qualified person to document the equipment is the person most familiar with it, the primary support person. Unfortunately, unless there is another person equally skilled with the equipment to backfill for the primary person, a support delta within that equipment may be introduced, creating an opportunity for system compromise or cyber-attack which may potentially have an effect on the reliability of the BES.

P3 echoed a similar comment made by P1 regarding how the standards were written. P3 stated that the CIP standards are interpreted and people interpret things differently. An entity in one NERC region may have a completely different understanding of the standards than an entity in a different region. P3 questioned the cyber program implementations throughout the NERC regions, saying, "is it a true apples-to-apples comparison between utilities that say they've complied?"

**Participant 4 (P4)**

P4 expressed that smaller entities (utilities) may not be classified or identified, by application of a risk-based assessment methodology, as Critical Assets that support the reliability of the BES. The only CIP standard requiring compliance from an entity not identified as a Critical Asset to the BES was CIP-002, Critical Cyber Asset Identification. The remaining standards, CIP-003 through CIP-009, were not required. Therefore, those entities required to comply with only one standard (for example, small utilities) had most

likely not incurred the expenses that larger entities (identified as Critical Assets to the BES) had been subjected to during implementation of all eight CIP standards.

P4 confirmed that complying with the CIP standards has cost utility companies money. Comparing utilities that are only responsible for compliance with CIP-002 with utilities that must comply with all CIP standards, P4 stated, "If you had to be fully compliant with 3 [CIP-003] thru 9 [CIP-009], then there'd be a lot more financial impact" to the company. Consistent with statements from P2 and P3, P4 acknowledged the financial obligations required for CIP compliance and the differences that exist between entities with regard to the financial requirements of each.

**Participant 5 (P5)**

P5 echoed P4's comments regarding the financial demands burdening entities required to comply with CIP standards, indicating that one entity where P5 had performed consulting activities spent over $10 million to comply with CIP-002 only. Some entities have taken a unique approach to compliance and the investments required meeting those requirements. P5 had experienced situations where "some of the transmission owners….are gaming the system in order to prevent the application of the CIP standards." To accomplish this, some companies have modified their networks, for example, in order to avoid compliance with CIP-003 through CIP-009. It made more sense to spend the money creating separate networks than spending more money to comply with the CIPs.

Other entities addressed the financial requirements of compliance by comparing the amounts of previous fines with the cost of implementation. The NERC website lists details of compliance fines and which regulatory standard those fines were assigned to.

P5 stated that if an entity researched the NERC website and found maximum fines of, for example, $10,000,

> Their accountants had figured out, why spend millions of dollars in compliance when, if we do have a violation, it's probably only going to set us back about $10 thousand. $10 thousand versus millions of dollars, that's a no brainer.

P2 had discussed the NERC maximum $1 million per day fine related to regulatory non-compliance. It was the opinion of P5 that originally, the million dollar fine scared people and served as a deterrent. After all, people were generally trying to do the right thing with regard to the implementation of the CIP standards. The million dollar fine was exotic and dramatic but it is not being used. P5 continued, "If someone were fined a million dollars, the ripple effect throughout the industry would be instantaneous." The industry is of the opinion that the million dollar fine is egregious and should only apply to the most blatant, dangerous and willful violation.

Finances are not the only aspect of regulatory compliance that offer challenges for entities. P5 stressed that politics always play a role in the protection of the critical infrastructure. In addition, those working to protect critical infrastructure will always be in a response mode regarding attacks. It is not possible to know where the next cyber-attack will come from or what it will look like. Adding to cyber protection challenges, P5 made it clear that physical attacks on, for example, transmission lines cannot be prevented and made reference to the 2013 attack on the California (Metcalf) transformers, an event which was also mentioned by P1.

Other challenges of protecting the BES include the availability of information. P5 commented that the major generating stations, transmission lines and other electrical grid component locations and details are freely available through Google Earth and other

electronic resources. However, a small consolation may exist. In P5's opinion, a terrorist would be very careful about attacking the BES because they may also need power for their electronic devices in order to carry out an attack.

**Participant 6 (P6)**

In parallel with comments made by P5, P6 discussed the creativity used by entities in order to potentially eliminate equipment from CIP compliance requirements. Depending on how an entity wrote their risk based methodology procedure, systems could end up being out of scope for compliance with CIP standards. All NERC registered entities wrote their own procedures describing their risk based methodology. Therefore, if a methodology was carefully crafted, desired systems could end up out of scope and the financial obligation to CIP compliance reduced.

P2, P3, P4, and P5 all stated that currently, revision 3 of the NERC CIP standards has been implemented throughout the NERC regions. NERC is due to roll out revision 5 in 2014. Revision 4 was cancelled so entities will move from revision 3 to revision 5. P6 stated that revision 5 of the CIP standards will address deltas in the process entities have been using to write their risk based methodology, specifically the issues in defining what systems should be in scope for CIP standards implementation.

As P2 indicated, P6 had also experienced CIP auditors not appearing to be auditing for the same things in entities' cyber security programs. Some auditors looked at the format and naming convention of cyber procedures, not the technical content, as evidence that the entities' cyber program was implemented correctly. P6 indicated that there appears to be a lack of consistency in the audit process across the United States, a

comment that paralleled statements made by P2 regarding a lack of consistency. P6 suggested that this could be a side effect of the immaturity of the CIP program.

P6 stressed how confirming that the right equipment is being protected is critical, therefore emphasizing the importance of appropriate audits. P6 placed emphasis on effective audit practices and training because cyber security in the energy critical infrastructure differs from other critical infrastructure sectors such as, for example, finance. In the finance sector, confidentiality of data is the top priority. Cyber security in the energy sector "is not about protecting the information, it's about protecting the operations of those systems" that support the BES. P6 raised an interesting question: when was the last time a control systems' credit card information was hacked?

**Participant 7 (P7)**

In reference to CIP standards regulation, P7 stated,

> There is a focus on being compliant. I would say 25 percent of middle level management that I've worked with is interested or serious about cyber security but their seriousness is always trumped by the lack of resources allocated by management. And given a lack of resources, playing the compliance game always trumps the cyber security.

This comment was similar to P5's statement regarding entities "gaming the system" in such a way that they could avoid compliance with CIP standards for their equipment to the greatest extent possible, minimizing financial impact to the company.

P7 discussed cyber security compliance and audits. It was P7's opinion that when it came to entities working on CIP compliance, "doing the check box to make sure they can illustrate that they are being compliant and that they have a policy and a procedure to address all of the required components" is what was being performed. This statement is consistent with a statement from P5 inferring that critical infrastructure protection is a

concept, not a program. Implementing standards and passing audits does not necessarily confirm that an entity is truly protecting themselves against cyber-attacks.

It was P7's belief "that local utility management does not see or anticipate or have a quantifiable perspective on being a viable target that somebody would want to attack." Utility people feel that they are a lower risk of attack as compared to other critical infrastructure entities, for example, finance, dams, water and wastewater systems, and so on. Yet the energy critical infrastructure provides power to other critical infrastructures, some of which may experience significant impacts if electricity became unavailable. If the BES were successfully attacked and compromised, cascading effects would certainly occur, as demonstrated by electrical outages such as the blackout in 2003.

P7 aired concern over the physical security of the BES, a topic that had been discussed by P1 and P5 with regard to the shooting of the transformers in California. General physical security issues extend beyond the scope of this research but are becoming increasingly integrated with cyber security in the energy sector as security breaches continue. P7 stated that security regulations for equipment outside of entities' physical security perimeters (e.g., transformers and power lines) do not currently exist. As a result of the incident in California, new security regulations are under consideration. The Federal Energy Regulatory Commission (FERC) has directed NERC to develop a regulation to address the vulnerabilities of electrical equipment not protected by a physical security perimeter.

**Participant 8 (P8)**

P1 referenced the need for a common vocabulary in a regulatory environment such that everyone involved in the implementation of the standards would have the same

understanding of terms. P8 commented that "a lot of people didn't understand some of the terms" when working on the CIP standards. Especially for those CIP standards that required great attention to detail and particularly when the evaluation of many assets was involved, common interpretations of terms is significant. While P8 was describing experiences within their company and with one particular standard, P8 stressed that a common understanding of terms within the NERC regions, as well as what is expected of entities when designing their cyber security programs to protect their equipment, is vital. Without that understanding, issues such as those described by P6 regarding inconsistent auditor expectations between regions should be expected.

P8 also expressed frustration over the plethora of documentation required by CIP regulations. P8 felt that time was wasted writing reports and not focusing on, for example, intrusion detection and other controls to provide security to equipment. There is a threat out there and most people want to focus on preventing that threat from executing a successful cyber-attack on their facility. Having to prove to a regulator that an entity is compliant is not helping that entity become more secure. P8 stated that "to hire someone to have to do pieces of paper to prove is…a regulatory exercise."

Continuing with the documentation requirements for compliance as well as maintenance of the cyber program, P8 stated that there are quarterly and monthly reporting requirements associated with CIP compliance. P2 and P3's discussions regarding extended paperwork requirements for CIP compliance were continued and reiterated by P8. P8 said that the CIPs were a "very heavily paperwork set of standards." Furthermore, P8 echoed comments made by P2 on equipment experts being removed from their system responsibilities in order to complete compliance paperwork. People at

P8's company were doing other jobs, such as Information Technology, and then pulled from those jobs to do CIP paperwork requirements.

**Participant 9 (P9)**

On the topic of entities removing people from equipment they support in order to perform required regulatory documentation efforts, P9 stated that the regulator (NERC) expects entities to backfill positions where the primary technical support person is removed to write CIP documentation. Unfortunately, this solution adds to the financial burden the entity must face to comply successfully with the regulations. And while P9 did not express a personal opinion on this topic with regard to the CIP standards themselves, reference was made to other individuals' statements. Even though the words "this is worthless" (referring to the CIP standards implementation) had not specifically been heard, criticality about what the standards contain and require of entities seemed to have been a topic of considerable discussion.

At the forefront for P9 was a concern regarding the relationship between reliability and resiliency. Reliability can be considered what it takes to keep the lights on. Resiliency includes robustness, adaptability and communications. Resiliency feeds into reliability. P9 had several questions in reference to how resiliency and its components blend into reliability standards. What does this new world (of reliability and resiliency) look like? Where is all of this going and how do we make sure we are not just checking boxes, especially with the introduction and expansion of the smart grid?

Of even greater interest was a larger question from P9 regarding how the energy critical infrastructure would hold up under a coordinated attack. A coordinated attack would likely contain multiple components, for example, a physical attack with a cyber

component or components, or vice versa. NERC CIP standards were developed to improve the reliability of the BES and strengthen entities' cyber element against attack. The BES has not yet experienced a cyber-attack of a magnitude that would put the standards to a test. P9 included another question: how do entities work with the government on a security strategy and what does that strategy look like? A lack of continuity in such basic elements as understanding terms in standards, an issue also mentioned by P1, may suggest that even though compliance with the CIP standards is now mandatory and enforceable, there is more work to be performed before the regulator may declare an increase in the reliability of the BES as compared to a pre-CIP implementation perspective.

**Participant 10 (P10)**

With the expense involved in compliance with the CIP standards, P10 pointed out that "organizations worked very hard to not have or have very little…assets that they had to protect", assets that would fall into scope of the CIP standards. Some entities were trying so hard to keep equipment out of scope that they spent money to "rip out fiber and CAT-5 [networking cable] and replaced it with serial [cable] to get away from routable protocols" that would have brought networks into compliance scope. Entities calculated that it would be cheaper to replace fiber and CAT-5 network cable with serial cable in order to remove equipment from the CIPs scope. Doing so eliminated the requirement to comply with CIP standards for those networks and equipment.

P10 and P3 had similar experiences with a lack of understanding of the CIP standards. Audits of entities where P10 had performed contract work received comments, from the auditor, that the entity had not interpreted the standards correctly,

requiring a re-examination of the entities paperwork and wording changes implemented, where appropriate. P10 commented that many electricity industry people consider the CIP standards to be an exercise in paperwork. The onerous paperwork requirements of the NERC CIPs had been discussed by P2, P3, and P8.

When discussing CIP audits and the possible fines for violations, P10 explained that "the fear of audit greatly exceeds the fear of a cyber compromise. Always. Absolutely always." For the small cooperative entities, big fines are a very big deal. P10 also expressed that if an entity fails an audit, "you get hung up in the virtual hall of shame", meaning that the rest of the industry and, for that matter the world, will see the failure, akin to the hacking fear comment made by P2: "if you were hacked, would you tell the public?" Non-compliance violations and fines, along with successful cyber-attacks, are public record available for anyone to view on the NERC website. P10 mentioned that companies use fines as fuel to take to their CEO's to get them to allocate more money for cyber security.

Entities have taken time to perform calculations regarding the expense required to implement the CIP standards versus receiving and paying a fine for violation of the standards. If an entity calculated that they would potentially get fined $1.5 million for non-compliance in an area that would require $2.5 million to become compliant, they chose to take the chance that they would get caught and fined. Paying a $1.5 million fine would still save them a million dollars. Based on this approach, entities may be driven to compliance (or non-compliance) by potential fines. P10 emphasized that "the CIP standards were not designed to punish people. They were designed to incentivize them,

to give them some framework to do better security that was deemed to have a positive influence on the BES of North America."

In spite of the fact that complying with the NERC CIPs is an expensive endeavor, there is a potential benefit that P10 articulated in "the benefit of being compliant is you inherently should become more secure." P10 continued with "People are expecting the implementation of the NERC CIP standards to mean you are entirely secure, and that is not the case. That is never going to be the case" because the actions of an adversary cannot be anticipated. Only the adversary knows what attack will be attempted. A comment P5 made with respect to critical infrastructure always being in a response mode regarding attacks and not knowing where the next cyber-attack will come from or what it will look like paralleled these remarks made by P10.

**Participant 11 (P11)**

One of the professional duties performed by P11 was involvement with peer and user groups within the energy industry. Duplicating a similar comment from P2, P11 expressed that peer groups within the industry were frustrated with NERC CIP auditors that had different requirements during audits. For example, some auditors understood requirements that documentation stay on site with the entity while other auditors wanted to take documents with them when they left the site. Furthermore, some auditors were hands-on with an entity during the audit, working with the entity to meet their CIP objectives. Other auditors were the opposite. To P11, there appeared to be a lack of consistency in the audit process.

Utilities are motivated, by fines for non-compliance, to comply with regulations. P11 stated, "The fines are the driver." P11 continued, saying that utilities want to be

secure, but the fine structure drives them to NERC CIP compliance rather than holistic cyber security. The lack of auditor consistency is also a factor for utilities.

The electricity industry was trying to integrate cyber security before the CIP standards were introduced. When the standards became a requirement, entities changed how they were implementing cyber security. P11 remarked that "their budgets are largely directed toward meeting compliance objectives due to regulatory fines" that can be imposed by the regulator (NERC). P11 saw significant concern throughout the industry regarding security projects that had been put on hold and "personnel and available funds are directed toward compliance" rather than securing equipment that supports the reliability of the BES.

P11 stated that companies are "constraining security improvements to only that which is included in NERC CIP in order to meet compliance requirements." Equipment that falls outside of compliance requirements with the standards may not receive needed upgrades or updating. The requirement for entities to show compliance potentially outweighs the need to be secure. The result may be an entity which is compliant with regulations but not secure against cyber-attack, thus leaving equipment and the BES potentially vulnerable.

When it came to staff required for CIP standards implementation, entities made significant changes in business operations. A large entity that P11 consulted with had rerouted their entire control systems cyber security staff for approximately 18 months to work on CIP compliance. Along with moving staff, security improvements that were in process were also redirected. All cyber security funding and staff were diverted to work on compliance with the CIP standards.

The CIP standards have requirements for securing the remote access capabilities of entities. P11 witnessed situations in more than a few utilities where remote access implementations were converted back to serial communications in order to reduce the amount of equipment requiring CIP compliance. P11 exclaimed astonishment with "the agility and motivation of the utilities to remove remote communications (routable protocols including TCP/IP) and return to serial communications as a result of remote communication regulation in NERC CIP and potential fines for non-compliance." P2 and P10 had also commented on entity concerns with regulatory fines and how that concern affected program and equipment implementations.

P11 briefly discussed impressions regarding NERC. It was the opinion of P11 that NERC developed regulations based on what they felt they could manage. This type of development may or may not meet what is required to actually increase the security and reliability of the BES. P11 stated, "Security is a moving target that compliance and standards approach can never keep up with", referring to the fact that cyber security is not able to predict what threats may occur, only protect themselves against what is known and position themselves to recover from an attack as expeditiously as possible. P11 felt that cyber security awareness is a good thing, saying, "Any awareness is going to improve peoples' understanding."

**Participant 12 (P12)**

P12 discussed unintended consequences which had resulted from the implementation of the NERC CIP standards. Specifically, "anytime you put regulations in place, there are unintended consequences as people try to maneuver to better position themselves with respect to those requirements." An example of an unintended

consequence, according to P12, is engineering design of systems and equipment in utilities. P12 stated that the "standards are driving engineering design" instead of appropriate engineering practices and cyber security requirements.

P12 debated the continued effectiveness of the CIP standards by saying,

> People talk about the effectiveness and are the CIPs doing any good….I think there's two aspects to that. One is retrospective and the other is forward looking. Retrospectively, I think…very easy to make the case that the standards have had some positive effects….I think from that perspective, looking back, they were useful…the bigger question going forward is whether they are still relevant and whether they are, today, improving the state of security and I think that's an entirely different answer. In my opinion, I think you can make a pretty good case that the CIP standards are *not* improving the state of security from where we are today and where we need to go.

Resources which are being consumed in order to comply with the standards would be better applied elsewhere, P12 continued, questioning that "Perhaps the CIP standards have outlived their usefulness? I think you can make a credible argument that that is the case."

The dialogue surrounding the topic of the continued appropriateness of the CIPs is a political hot button. P12 expressed that people are so beaten down that they assume the continued existence of the standards is a foregone conclusion. P12 stated that "there will be new and more stuff coming in the way of regulations." New standards, CIP-010 and CIP-011, are adopted and progressing toward finality. Other CIP standards are currently in draft form.

**Participant 13 (P13)**

The CIP program had been complete in P13's organization for over five years. An audit was performed in 2009 with acceptable results. The CIP standard that was the most difficult to implement was CIP-006, Physical Security of BES Cyber Systems. P13

indicated that the identification of the perimeter was significant as was the integration of physical access equipment (card key access, for example). The combination of monetary investments along with time and personnel resources resulted in CIP-006 being a complex standard to put into effect.

P13 exhibited reservation when discussing the CIPs effect on the reliability of the BES. A definitive yes or no was not indicated. Alternatively, P13 stated that it would be foolish to express an opinion suggesting that the BES had suffered a negative effect from the implementation of the CIPs. Specifically, "anytime you have more people looking at the state of preparedness of an entity…you're gonna yield a stronger, more resilient entity." This assertion resembled opinions voiced by previous participants indicating a raised level of cyber security awareness equating to increased cyber security which, in turn, leads to a strengthening of the reliability of the BES.

P13 was unsure of the exact number of personnel required to put the CIP program into effect for their entity. Even so, P13 pointed out that over 50 people were responsible for the implementation and maintenance of their program. The program utilized full time personnel in addition to contract individuals, as necessary. P13 indicated that prior to the CIP requirements, fewer people were involved with cyber security in their organization, an observation that was consistent throughout the interviews in this study and reflected in the Quantitative Summary of Results section.

**Quantitative Summary of Results**

As with the qualitative data presentation, the quantitative summary of results (Mays & Pope, 1995) was also presented sequentially beginning with data from Interview Question 1 and continued with Interview Question 2, and so on. The quantitative

summary section culminated with data applicable to the Research Question (RQ). The study interviews generated data from which themes were derived. A compilation of the themes followed the summary of results from the RQ. Data from NVivo qualitative research software was included and discussed in the Quantitative Summary of Results (Mays & Pope, 1995) section.

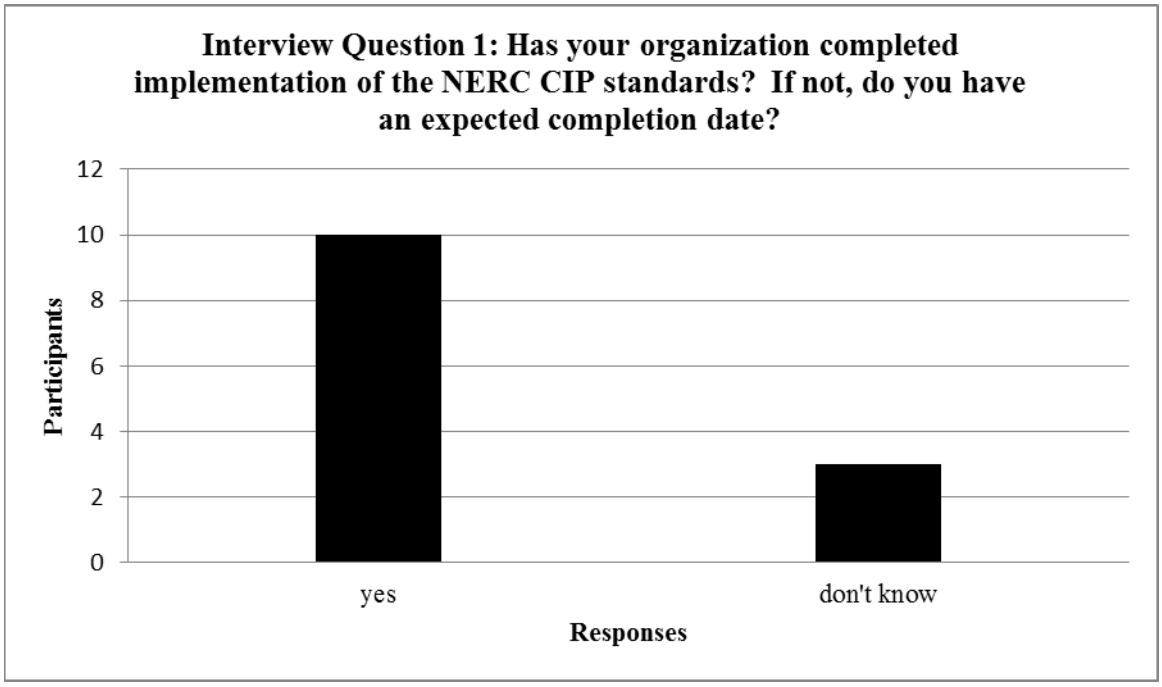


Figure 3. Summary results for Interview Question 1

There were no responses for Interview Question 1 indicating incomplete implementations of NERC CIP programs. P2 made a comment regarding initial CIP regulation and compliance requirements. Some organizations where P2 had performed contract work were in denial, saying, "CIPs don't apply to us." P2 stated that at some point, those entities reversed themselves, saying, "It does apply, and now we have to do

something about it" which resulted in some unorganized approaches to addressing the standards. In an effort to make the right choices, entities put committees together with individuals that were not necessarily the appropriate people, had to reorganize, and finally got technical people involved to start the CIP compliance program at the organization. P10 was of the opinion that while implementation of the CIP standards was complete at their entity, implementation is never truly complete. P10 stated that "It's an ongoing, evolving process" due to the fact that cyber security is constantly changing.

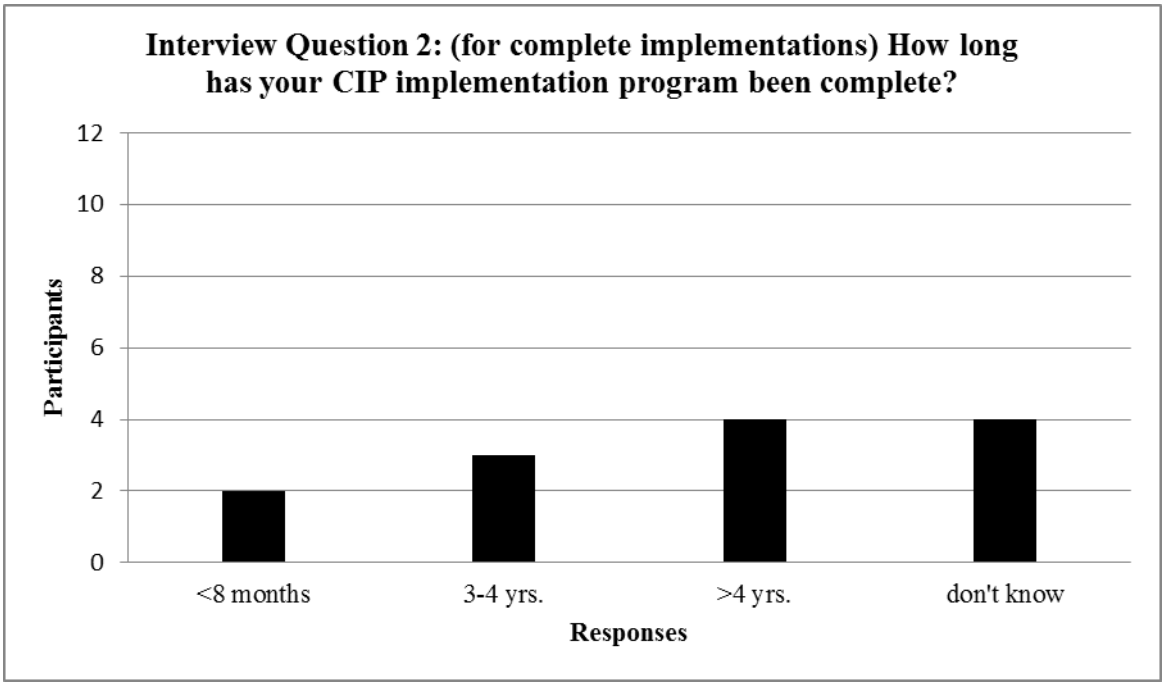


Figure 4. Summary results for Interview Question 2

Program completions ranged from a few months to more than four years.

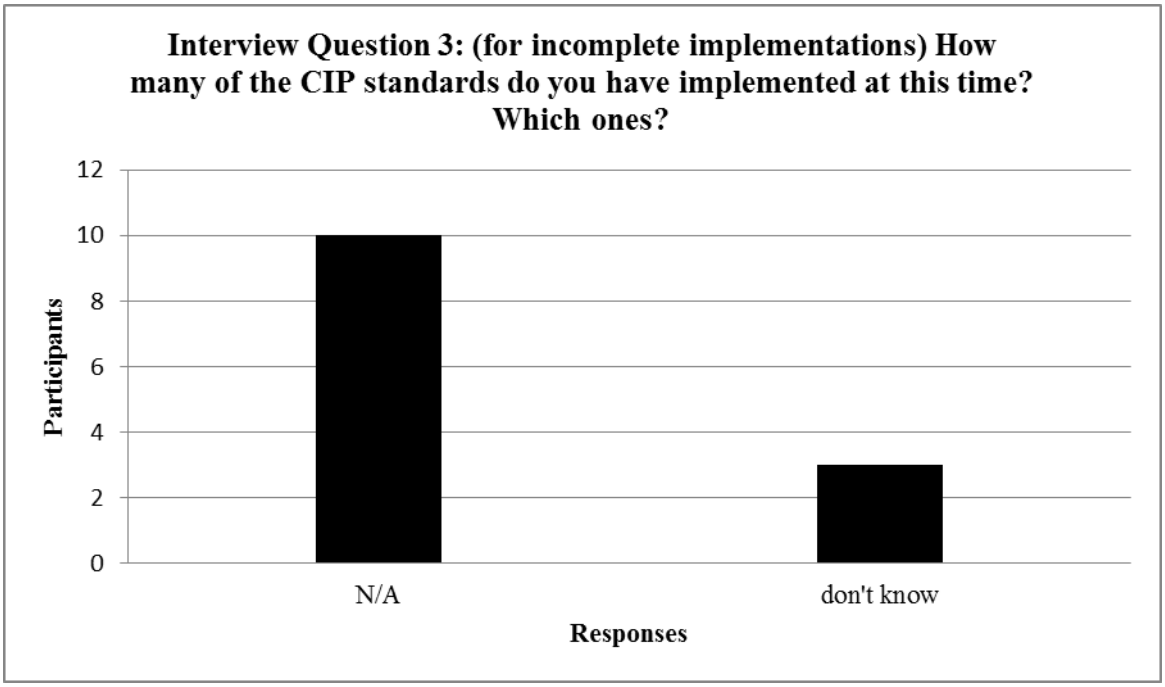


Figure 5. Summary results for Interview Question 3

Study data indicated no incomplete implementations.

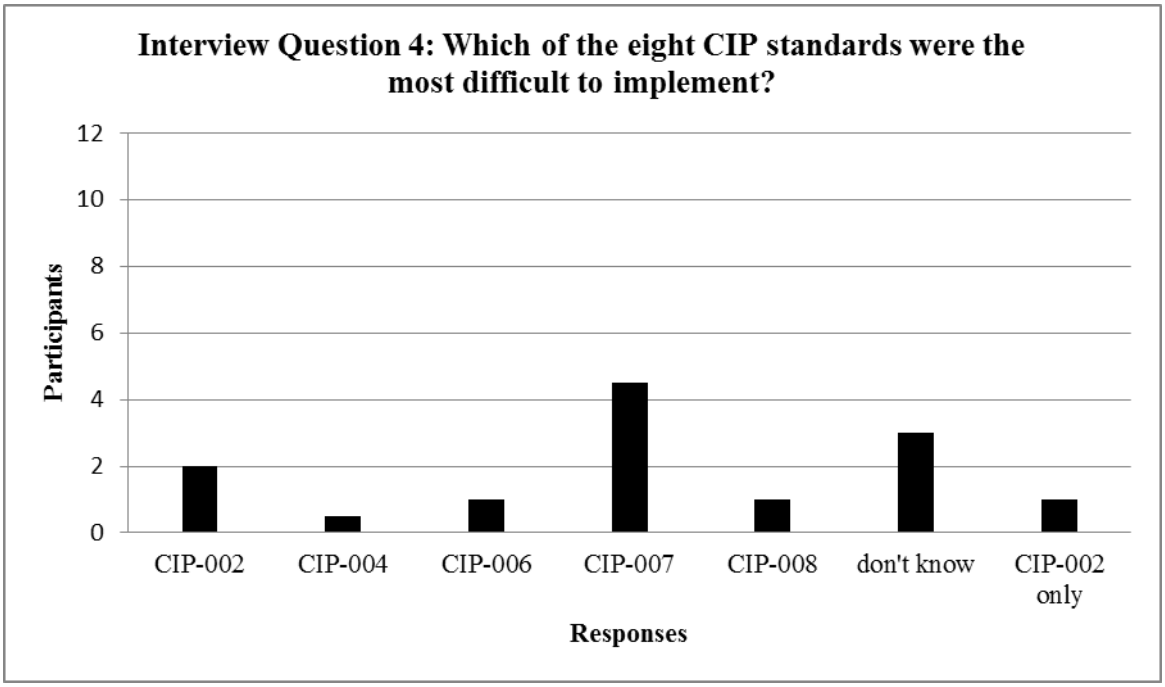


Figure 6. Summary results for Interview Question 4

Interview data indicated that none of the participants felt that CIP-003, CIP-005, or CIP-009 were among the most difficult to implement. P12 noted that CIP-004, Personnel and Training, was the most difficult from an organizational perspective. The number of potential instances for failure in that standard was high. From a technical perspective, P12 mentioned CIP-007 as the most complex, citing the technical feasibility exceptions available for entities to take advantage of being difficult to manage and track. To avoid skewing the data in Interview Question 4, the response from P12 was divided in half. .5 applied to CIP-004 and .5 applied to CIP-007.

One participant represented a smaller entity only required, by regulation, to comply with CIP-002. Figure 6 represented the data from that participant as CIP-002 only. Even though the entity had a singular standard compliance requirement, the participant expressed that their utility implemented portions of the other standards in the CIP suite. CIP-003 through CIP-009 made good engineering sense to the utility, according to the participant. Therefore, choosing to apply sections of the additional standards was a prudent business decision.

The NERC website contains data regarding entity violations of regulatory standards and the amount of fines assigned for violations. P5 explained, "Look at violation statistics. You will see that CIP-007 is the most violated standard." Data collected in this study indicated that participants felt CIP-007 was the most difficult standard to implement.

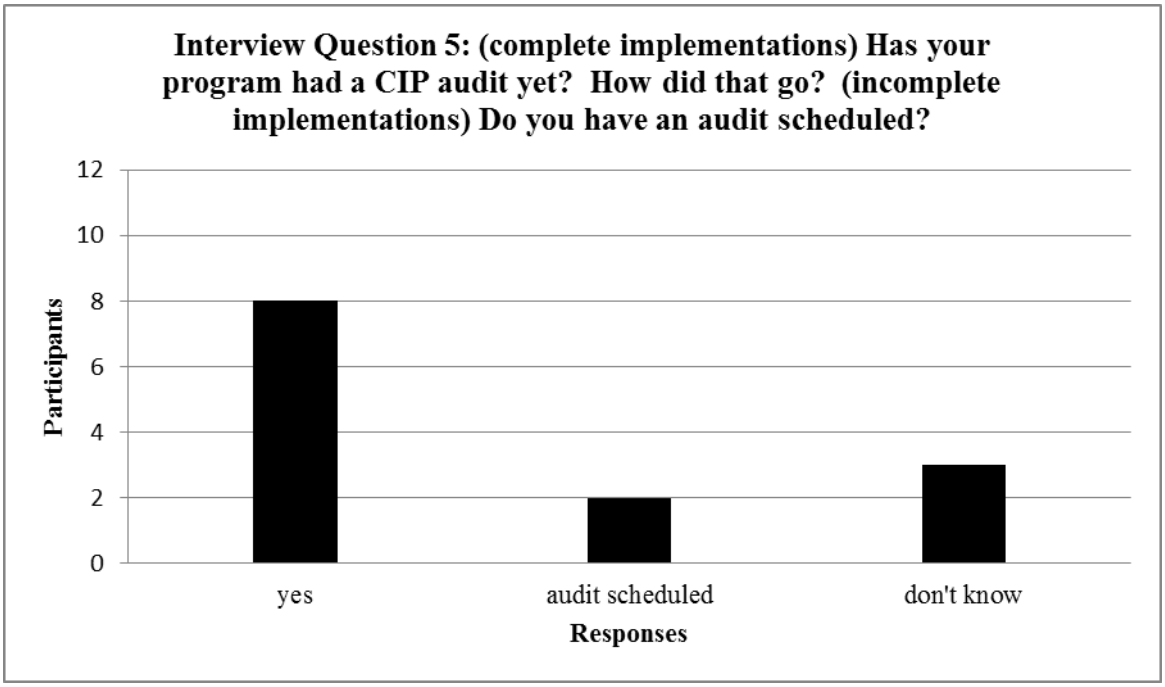


Figure 7. Summary results for Interview Question 5

Two participants responding to Interview Question 5 indicated that the CIP implementations were complete at their entities and an audit was scheduled. Of the participants that indicated they had completed an audit, two participants stated that the auditors defined areas for improvement for the entity but no violations were received. Two participants mentioned violations issued for their entities. Four participants indicated no violations from the auditors for their entities.

P6 had been involved in a number of audits for different entities. P6 expressed frustration with the audits, saying,

> I have felt that the audits that have been done, in large part, have not been very good. The audits in many cases focused simply on documentation and in some cases, nomenclature of the documentation…resulting in fines that were idiotic.

For example, an entity may have written a good document describing how they were providing cyber protection to their equipment but the auditors made them throw those documents away and write new ones that were simply cut and paste verbiage from the CIP standards with no description of how equipment was being protected. P6 expressed that "there is so much ambiguity in those CIP requirements" that it was difficult not only for the entities implementing the standards, but for the auditors auditing them.

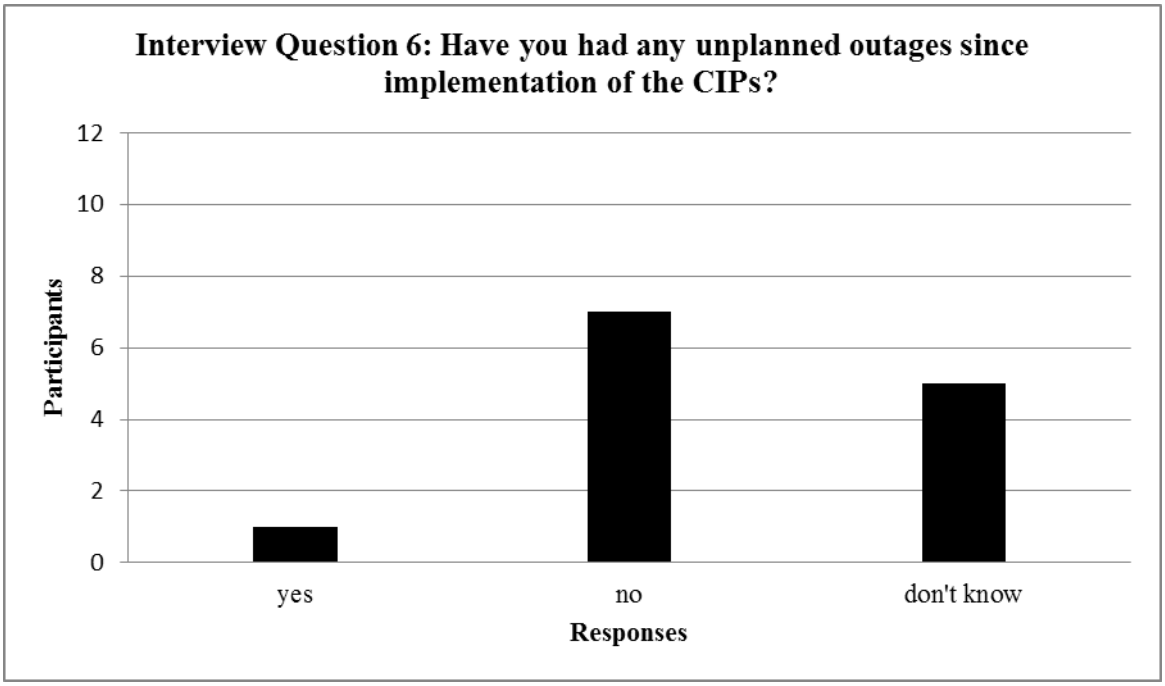


Figure 8. Summary results for Interview Question 6

Interview data for Interview Question 6 indicated that only one entity had experienced an unplanned outage after completion of their CIP implementation program. P5 stated that unplanned outages happen all the time. P5 was not aware of any outages, for any entity, related to CIP standards. One outage P5 referred to was a result of human error, not cyber security, and ended up costing a company over $20 million in fines.

P6 indicated that to date, no cyber events have impacted power delivery. Computer viruses have infected entity systems but none have caused any significant stability issues or loss of power. P7 expressed a statement similar to P5, saying that there is no evidence of any outages at any entity related to CIP implementations. P10 also was unaware of any outages related to the CIPs.

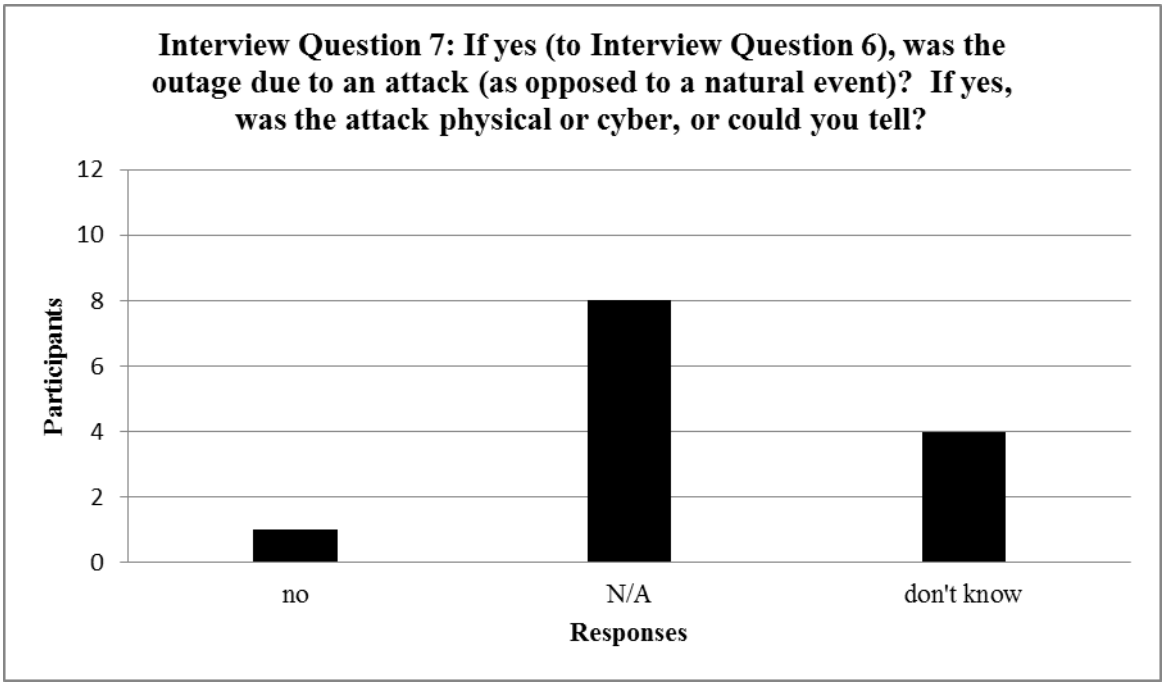


Figure 9. Summary results for Interview Question 7

The one entity that experienced an outage explained that the outage was not related to cyber security or their CIP program implementation but was instead weather related.

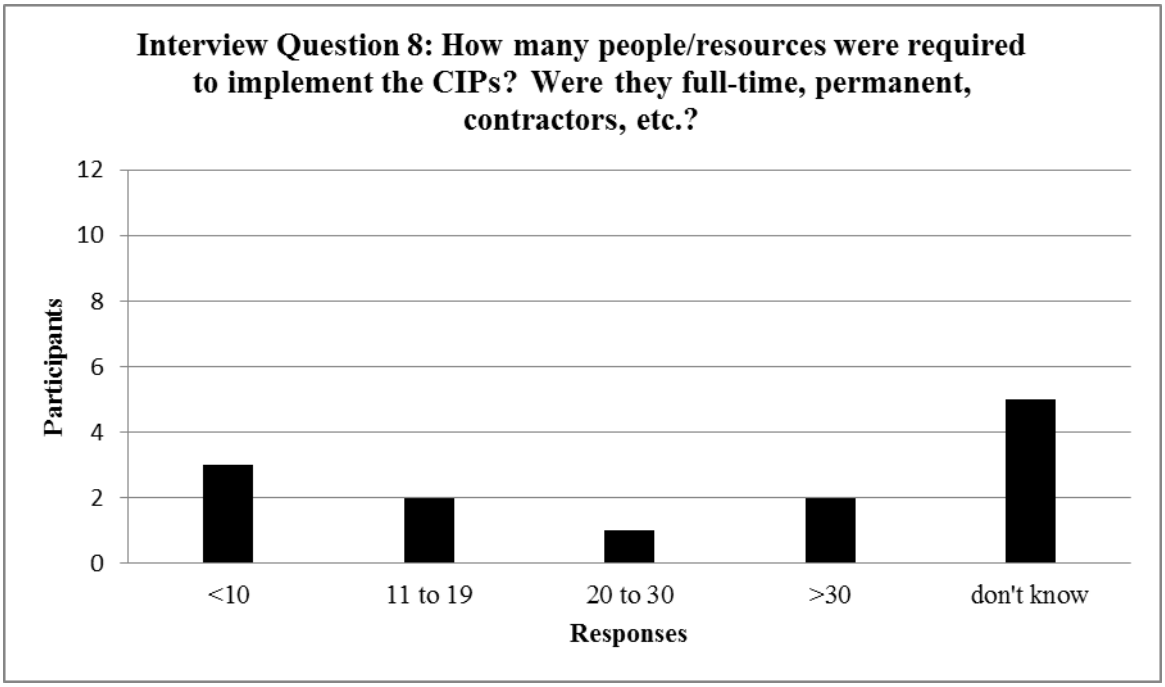


Figure 10. Summary results for Interview Question 8

Participants stated that their CIP implementations were performed by a combination of regular full time entity employees supplemented by contractors and consultants. Some small to medium sized entities re-tasked individuals from positions they had been working in (before the CIPs were a requirement) to positions that supported CIP implementation. According to P5, between the years 2005 and 2008, there was a huge influx of personnel and money to support CIP implementation. P5 also said that personnel required for ongoing maintenance of the program will be different than for implementation.

The expense required for CIP implementation was not insignificant. P5's entity spent in excess of $15 million on CIP implementation. P6 made reference to large utilities spending tens of millions of dollars over 3 to 4 years to implement their CIP

programs. Third party vendors also contributed to implementation efforts. When the CIP standards were published and the timeline created for compliance requirements, P2 stated that several dozen consulting companies were formed with a single area of expertise in CIP compliance assistance for utilities. Additionally, software packages were developed specifically for CIP documentation and control.

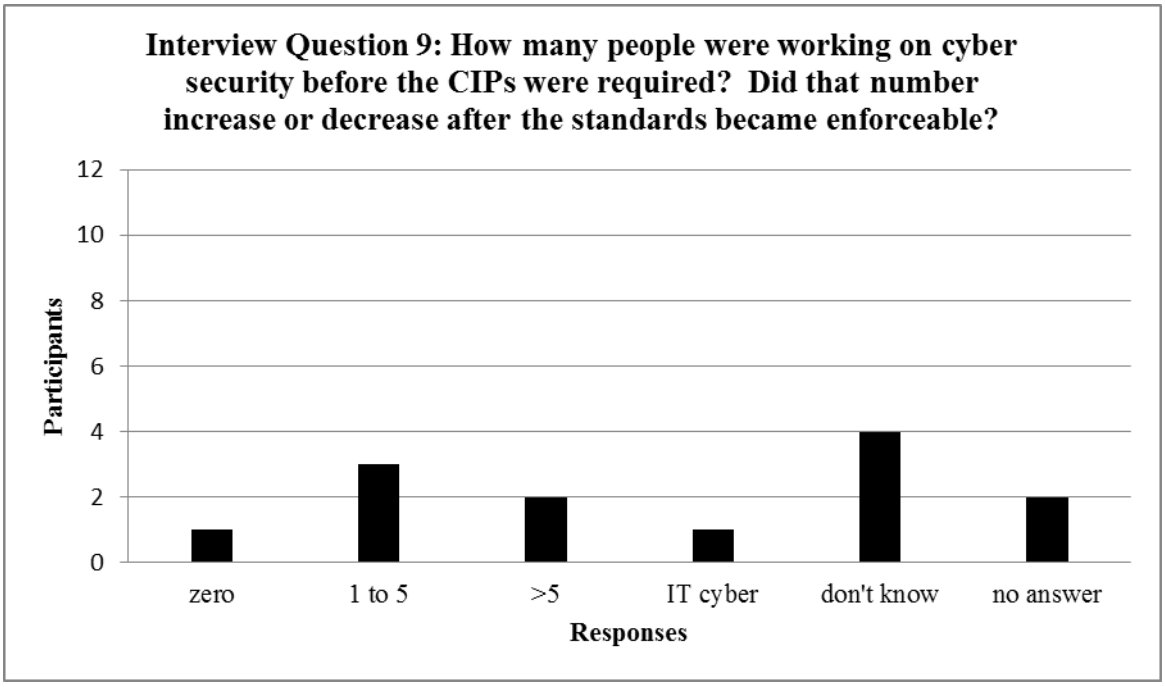


Figure 11. Summary results for Interview Question 9

The number of people working in cyber security positions, pre-CIP standards, was less than after the standards became a regulatory requirement. P5 stated that maintenance personnel for their entities' CIP program are currently just over a dozen. P5 expects that number to increase over time as the complexity of the standards increases, including the addition of new standards. P6 indicated that future upgrades and audits to CIP programs

will likely be performed by contractors and consultants rather than increasing full time employee numbers. P7 explained that it was not uncommon, four to six months prior to an audit, for entities to increase their staff in preparation for the audit.

P12 gave a slightly more detailed picture of the number of personnel employed by entities implementing CIP programs. Small utilities usually employed between three to five individuals that could be a combination of regular full time and contract employees. Medium sized utilities employed from six to eight employees while large utilities commonly employed dozens of individuals. Generally, a core compliance team of three to five people was not uncommon for medium to large utilities. In addition to the individual contributors to the program, there are ties into many other departments in the entity that include supply chain, human resources, operations, and others.

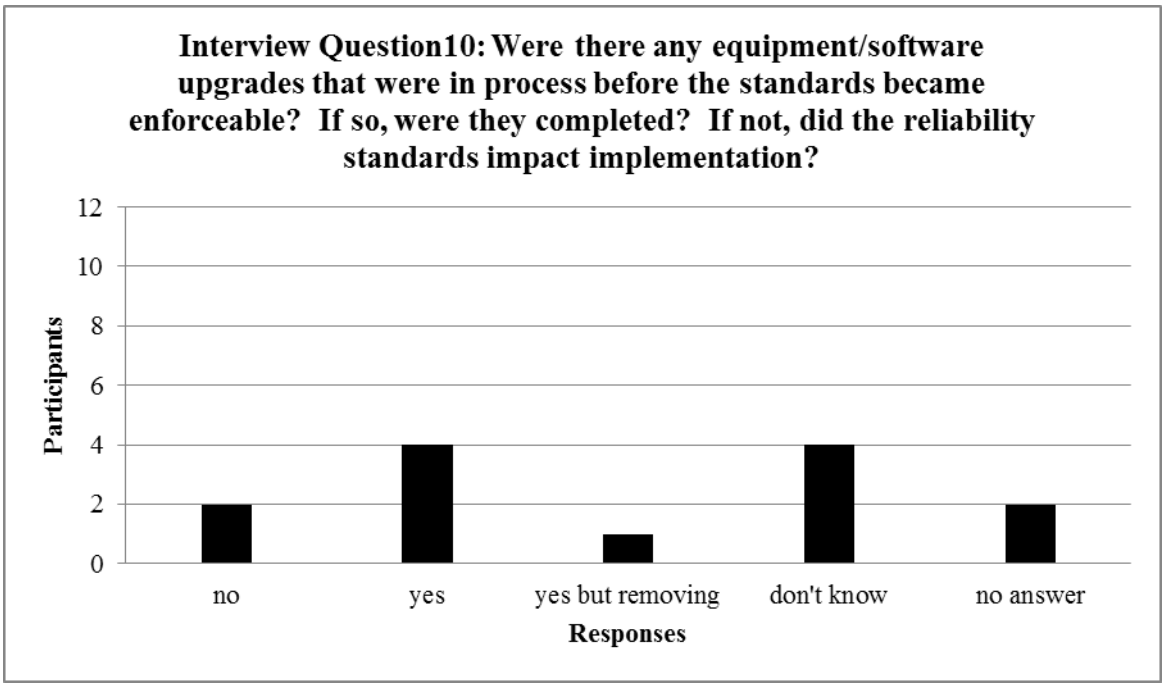


Figure 12. Summary results for Interview Question 10

P4 stated that a SCADA system upgrade was in progress during their utilities' CIP implementation. The upgrade was not impacted by the CIP program. P6 had experienced several large utilities that had implemented upgrades only to tear them out when the CIP standards were implemented. The utilities did not want those upgrades to fall into scope for CIP compliance. Remote access (utilizing TCP/IP) upgrades were removed and serial communication re-installed to ensure CIP compliance was not required for that equipment. P7 echoed the comment from P6, stating that entities took some networking hardware out and replaced it with "serial communications, only trying to skirt CIP compliance. Every entity I know plays the game that way."

P8 described the impact of CIPs on upgrades in a different way. For each critical cyber asset, detailed paperwork must be generated. Diligence must be proved by the entity to the regulator. The extensive paper trail required for compliance was an incentive for entities to minimize the number of assets required to comply, leading to reductions or cancelations of upgrades.

In an entity with a customer base of more than 600,000, equipment installations and upgrades are somewhat constant. P13 discussed the fact that equipment upgrades and projects were in process and ongoing when the CIP requirements became mandatory. It was unknown if any of the projects were related to CIP implementation. P13 indicated that none of the projects were cancelled before, during, or after the CIP regulations were enforceable.

Interview Question 11 was an open ended question asking participants if there was anything else they wished to add to their responses to the questions. Only one participant did not offer a response. The responses from the other participants were

included in the Qualitative Data Presentation section of Chapter 4. Any data from Interview Question 11 that was applicable to other interview questions was included in the analysis of the appropriate question.

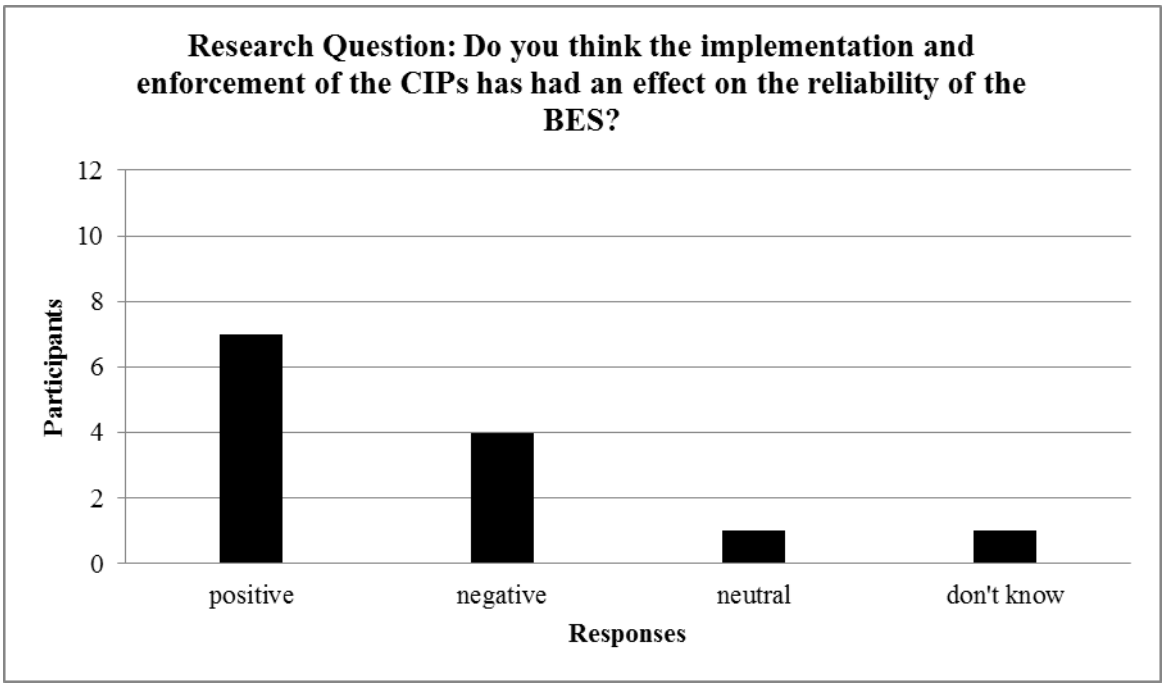


Figure 13. Summary results for the Research Question Interview Question

As figure 13 indicates, seven of the study participants felt that the CIPs have had a positive effect on the reliability of the BES. Four participant opinions indicated there has been a negative effect. One participant felt that the CIPs have had neither a positive or negative effect on the BES. One participant stated that they did not know if the CIPs had any effect on BES reliability.

Of the participants in the positive category, one participant provided a caveat to their answer, explaining that the reliability of the BES had been improved "assuming the

standards have been written properly." They continued, "If the standards are requiring that the folks do, you know, hardening and surveillance, and focus on the ability to recover critical elements of the system, then in theory, they're responding to a need that wasn't previously attended to." Another participant indicated that the CIPs had "drastically increased awareness of cyber security and the importance of proper cyber security in the electric industry", leading to a positive effect on the reliability of the BES.

One participant agreed with two others, emphasizing that the BES is more secure because facilities have more security equipment, processes and procedures, and common security practices that were not available before the CIPs were required. They felt that, unquestionably, the CIPs have had a positive cyber and physical impact on the reliability of the BES, stating that "the CIP program has done a real good job of…helping organizations become secure from a cyber perspective." However, they added that determining if the CIPs have had an effect on the reliability of the BES was "a real, real hard question. For what I will call the common man,…all they care about is when they flip the switch in their bedroom, the light comes on. That is all the general public cares about." This participant also emphasized that people working in the electricity industry talk about reliability and availability in different terms than the general public.

Another participant agreed that the CIPs have had a positive effect on the reliability of the BES. They stated that the CIPs have been a foundation that has pulled the electricity industry together. About the CIPs, they said the standards "do provide…some reliability and control for the industry to have a gauge to work toward." Yet another participant indicated a positive effect by reducing cyber risk in the BES. The CIPs require entities to implement technical remediation including intrusion detection

and electronic security perimeter protection, among others. The CIPs increased the ability for an entity to detect attacks on their systems and also increased the level of effort required by an attacker to successfully attack systems. The CIPs have also forced entities to put firewalls where previously, there were none.

This participant continued, explaining that the CIPs have empowered the small utilities to protect themselves and not be a weak link in the BES anymore. They expressed that people have argued, insisting that the CIPs are not having any effect on the BES, but that those people are the ones that have done a poor job of implementing the standards. From a cyber-attack perspective, when an attacker enters a network, they are able to move around, to go places, explained this participant. The CIPs, when implemented strategically, protect networks.

Of the four participants who felt the CIPs have had a negative effect on the reliability of the BES, each expressed a different reason. One said, "In general, NERC CIP has made our country less secure because the systems are less reliable because the best people are being pulled off [of their equipment or systems] to fill out paperwork." It was the opinion of this participant that the CIP standards require a very high degree of documentation and that this documentation is being performed by people who were, prior to CIP implementations, working as experts on their equipment in the field.

This participant continued that there are many organizations that have to be involved in the documentation process including legal, documentation groups, engineering and operations, to name a few. Additionally, the fine structure applied to violations of CIP standards can be very formidable. Fines have been levied against entities for inadequate CIP documentation. Therefore, entities have removed individuals

from the equipment and systems they have been supporting in the field in order to write CIP documentation, thereby increasing the vulnerability of the equipment or systems to compromise if they are not adequately supported.

Another of the four participants expressed the opinion that the CIPs have had an adverse impact on the reliability of the BES because money being spent on the CIPs is money being taken away from reliability and customer services. This participant felt that this was detrimental to the entities and the industry and as a result, the CIPs have taken away from the reliability of the BES. The money that has been spent on complying with CIPs may have been used to upgrade systems or harden (increase the security of) existing equipment. Especially for smaller utilities, implementing the standards combined with upgrading equipment is simply cost prohibitive.

One participant, in agreement with two others on the negative effect of the CIPs on the reliability of the BES, had a different story to tell. This participant felt that cyber security attacks are not going to be effective tools to compromise the BES. Severe weather events are the biggest threat to the BES, in their opinion, stating "there is a risk but it's not….something that I would lose sleep over" they said, explaining that the smart grid, which is under construction, may be more susceptible to cyber-attacks. However, the smart grid will not be completely integrated but will operate in sections. The current power grid is more analog than the smart grid will be. According to this participant, "I think the *fear* about the risk to the grid based on cyber-attacks is far more significant than the *actual* risk to the grid from cyber-attack."

The fourth participant answering that the CIPs have affected the BES negatively added that "it's hard to say." They felt that the standards did not drive entities to increase

cyber security. It was the growing cyber security threat environment that propelled this participant's entity to implement security improvements when the CIP requirements emerged. This participant expressed that their entity was in the process of upgrading their cyber security posture anyway, prior to CIP standards requirements.

A participant expressing a neutral position regarding reliability effects on the BES from the CIPs cited positive attributes. From an engineering perspective, improvements in entities have definitely been made, and the BES has benefited. For example, 10 to 15 years ago, entity corporate and control networks were largely mixed together. Currently, separation of the networks resulting from CIP requirements has culminated in a huge improvement in reliability over previous years.

From a negative reliability perspective, implementation of the CIP standards has resulted in people making "intentional choices in how they construct their systems in order to avoid compliance", this participant said. An example of a choice was evident in routable protocol exceptions. IP connectivity has been removed or not installed in electrical substations in order to avoid compliance obligations. This participant explained that these choices have had a negative impact on reliability because some modern systems depend on that architecture to operate.

The participant expressing a neutral position on the CIP standards affecting the BES felt that the standards have had an unintentional consequence of a reduction in the reliability of the BES. As a result of entities choosing to avoid compliance requirements by not installing equipment or removing equipment that would require CIP compliance, entities would be unable to take advantage of the additional protections that may be offered in new installations. Removing equipment, such as routable protocols in favor of

serial communications may allow entities to avoid CIP compliance for that equipment but limits organizations to antiquated equipment and the associated detriments. This participant's opinion was that the positive and negative attributes cancelled each other, ultimately resulting in the participant's neutral opinion.

Considering out of date equipment operating the BES, one participant explained that "in general, the electric system is in fact vulnerable and it will always be vulnerable." With the equipment and technology currently in place, this participant felt that the grid cannot be completely secured. Entities that choose not to upgrade legacy equipment in favor of avoiding CIP compliance may unwittingly be playing a role in the insecurity of the BES.

One participant explained that the electricity industry had been trying to integrate cyber security when the CIP standards were under development. When the standards became a requirement, entities "budgets are largely directed toward meeting compliance objectives due to regulatory fines" that may be imposed by NERC for non-compliance. This participant emphasized that "the fines are the driver" to implementing the CIPs, not increasing an entities security posture. This participant felt that utilities want to be secure but the fine structure drives them to NERC CIP compliance rather than holistic cyber security. In the end, this participant was unsure if the CIPs had a negative or positive effect on the reliability of the BES.

**Themes**

With no preconceived theories (Jebreen, 2012) on which this study was based, the data from the interviews defined the themes. Each interview was transcribed by the researcher upon completion. Once all interviews were complete, thematic inductive

analysis of the data began. During the data analysis, themes started developing. Metathemes (Guest et al., 2006) emerged after Interview 8 and data saturation was achieved after Interview 13.

Once the analysis was complete, the data was entered into NVivo to triangulate the themes. In addition to confirming the themes generated from the thematic inductive analysis, NVivo also illuminated a hierarchy to the themes. Table 6 illustrates the themes by the number of items coded and organized hierarchically. The strongest theme was listed first, followed by the next strongest theme, and so on. The number of items coded refers to the number of participants and coding references refers to the number of times a theme became evident in the interviews. It was not uncommon for one participant to discuss a particular theme multiple times during the interview, which is reflected by a higher number in the coding references column than the number of items coded column.

The strongest theme, Entities Removing Equipment to Avoid CIPs, was mentioned by seven participants and the theme was referenced a total of nine times. As the number of coding references column indicates, there were multiple instances of participants discussing a theme several times during their interview. Figure 14 is a graphical representation of the data in Table 6. Figure 14 was generated in NVivo software. Figure 14 shows the strongest theme on the left of the figure and themes of lesser strength continuing toward the right.

Table 6. Nodes (themes) Organized by Number of Items Coded

| Nodes | Number of items coded | Number of coding references |
|---|---|---|
| Entities Removing Equipment to Avoid CIPs | 7 | 9 |
| CIPs Positive Effect on BES | 7 | 8 |
| NERC Fines Influencing Implementation | 6 | 10 |
| Removing SMEs to do CIP Paperwork | 6 | 9 |
| Compliance versus Security | 5 | 12 |
| CIPs Negative Effect on BES | 4 | 6 |
| Lack of Common Vocabulary | 4 | 4 |
| Inconsistent Auditors or Auditing | 3 | 9 |
| Cyber Security Always in Response Mode | 3 | 5 |

In Figure 14, the NVivo software did not include a word wrap or editing function for figures generated in the software, resulting in some words in the figure being truncated. The themes expressed in Figure 14 are identical to those presented in Table 6.


Figure 14. Summary figure of themes generated from NVivo

**Theme 1: Entities Removing Equipment to Avoid CIPs**

For Theme 1, the strongest theme, seven participants discussed entities removing equipment, in particular networking equipment, to avoid the requirement to apply CIP standards to that equipment. Two participants referenced equipment modification or removal twice in their interviews, explaining that for some entities, it was more economical for them to spend money removing or modifying equipment than spending the amount of money required to apply the CIP standards. Another participant explained that entities were extremely motivated by the potential fines for non-compliance with regard to routable protocols. Rather than spend the money to ensure the routable protocols were CIP compliant, returning to serial communications ensured that they would not be required to apply CIPs to that equipment and the possibility of being fined for non-compliance was negated.

All entities defined their assets according to their risk based assessment methodology as required by CIP-002. With a lack of risk assessment standardization throughout the industry, assessment methodologies were inconsistent across regions so assets that may have come into scope for the CIP standards for one entity may have been

scoped out in another entity. One participant stated that some utilities sold assets in order to avoid CIP compliance. In some instances, as another participant mentioned, larger utilities that had recently completed equipment upgrades chose to remove them when the CIPs became a regulatory requirement, thereby eliminating compliance requirements for the equipment.

**Theme 2: CIPs Positive Effect on the BES**

Theme 2, the second strongest theme, developed out of input from seven participants also with eight coding references. General statements ranged from the CIPs reducing cyber risk and making the power grid more secure, to the increase in cyber security awareness as a result of the regulation and enforcement of the CIPs. A participant expressed the opinion that BES reliability has increased as the importance of proper cyber security in the electricity industry increased due to the regulatory requirement of CIP standards implementation. In other words, cyber security awareness has increased and is a positive consequence of CIP implementation.

In addition to increased awareness, another participant expressed that the implementation of the CIPs has reduced the damage that could have been done by a cyber incident. For example, consider the introduction of hostile code from a portable device. Measures put in place to satisfy CIP compliance should reduce the efficacy of that type of attack.

**Theme 3: NERC Fines Influencing Implementation**

The third strongest theme to emerge from the interviews involved regulatory fines and the effect of potential fines for non-compliance on how entities implemented their CIP programs. During the interviews, the discussion of fines elicited emotional

responses from some participants. Some felt that the potential million dollars per day per occurrence non-compliance fine is exorbitant. While the possibility of incurring a million dollar fine for willful and blatant non-compliance is remote, it does exist. According to data provided by the participants, entities are influenced by regulatory fines with regard to CIP implementations.

Entity managements developed different approaches for CIP implementation depending on their appetites for different risk circumstances. Some entities based their CIP programs on the need to avoid regulatory fines above all else. Other entities crunched the numbers and discovered that they could accept the risk that they may receive a fine for non-compliance. Included in their calculations was public information regarding fines received by other similar entities. Other entities included additional factors in their risk based decisions for implementation, such as the potential damage to an entities reputation if they were caught in a non-compliance situation that would become public information.

**Theme 4: Removing SMEs to do CIP Paperwork**

The fourth strongest theme involved entities removing subject matter experts (SMEs) from equipment they supported in order to complete paperwork required for CIP compliance. Similar to Theme 3, Theme 4 elicited strong responses from some participants. The over-arching concern expressed by six participants was the removal of people directly responsible for equipment supporting the reliability of the BES in order to generate CIP paperwork. If the equipment the SME had been supporting needed an upgrade or suffered a failure of some kind, a potential reduction in BES reliability may exist depending on the significance of the equipment to the reliability of the BES. While

a participant explained the regulator expectation that entities replace SMEs that have been re-tasked with CIP compliance duties, financial restraints may complicate an entities ability to fulfill that expectation, particularly in small or medium sized entities.

Another participant stated that roles have shifted with regard to equipment SMEs. The SMEs assist in improving security by continuing to support their equipment. With the requirement of the CIP standards, SMEs are finding themselves filling out paperwork and not providing support for their systems. Yet another participants' opinion was that the energy critical infrastructure sector degrades when people that know how to maintain critical systems have been pulled away to do CIP paperwork.

**Theme 5: Compliance versus Security**

Theme 5 arose in interviews as participants debated the concept of the NERC CIPs simply being a regulatory compliance exercise over actually improving cyber security in support of the reliability of the BES. During the NVivo coding process, attributes shared between Theme 4 and Theme 5 became apparent. In Theme 4, participants discussed the decisions by entities of re-tasking SMEs to complete CIP paperwork as an exercise in compliance and not in support of cyber security. Theme 5 echoed elements of Theme 4 while including additional insight from participants.

Several participants referenced compliance with NERC CIP standards not equating a more secure entity. However, complying with the standards should have a side effect of an entity becoming more secure. Some participants expressed the opinion that entities may have done the minimum requirements to satisfy compliance with the CIPs and that the minimum level may not be satisfactory to protect an entity from cyber-attacks. One participant explained that security must constantly evolve in order to

combat ever emerging threats in the cyber community. Compliance with the standards fulfills static regulatory requirements, potentially introducing gaps or vulnerabilities that may be exploited if security is not constantly keeping pace with new developments.

Participant opinions in Theme 5 included feelings that entities have completed what the standards have required and have not gone beyond the requirements. Entities have done what they needed to do to check the compliance box but they have not done what they need to do to help secure the BES. One participant worked with clients that were more concerned with compliance than security and while they may have completed the requirements for compliance, they had not necessarily become more secure in the process. This participant indicated that entities have applied "window dressing to make the auditors happy" and pass their audits, illustrating their compliance, but not necessarily resulting in a secure infrastructure.

**Theme 6: CIPs Negative Effect on the BES**

The participants that felt the CIPs had a negative effect on the reliability of the BES voiced varying opinions why they felt that way. One participant felt that there was higher probability of a physical attack on the BES than a cyber-attack. In saying so, this participant did not imply that there was no risk of a cyber-attack but in comparison with a physical attack, cyber was a lower probability. They cited the current, predominately analog, configuration of the BES as the reason a successful cyber-attack would be difficult. They also stated that once the digital smart grid is fully implemented, the success of a cyber-attack would be more probable compared with the current analog BES.

Other opinions given in support of the CIPs having a negative effect on the BES included entities spending money on compliance efforts in lieu of strengthening their

cyber security posture. In addition to money being spent on compliance instead of securing systems, time spent on completing paperwork for CIPs was disproportionate to system maintenance and security improvements. Considerably more time was required for CIP paperwork. In consideration of those entities that had chosen not to install or upgrade equipment that would then require compliance with the CIPs, those entities may have inadvertently created security weaknesses in their equipment or networks. There exists a possibility that those weaknesses may have the potential to threaten the reliability of the BES.

**Theme 7: Lack of Common Vocabulary**

Theme 7 included the vocabulary in the CIP standards, vocabulary used by auditors across regions and interpretations of those vocabularies. Participants echoed concern within entities regarding differences in interpretations of terms and the confusion with vocabularies. How NERC auditors understood the standards was not necessarily consistent with what the entities understood. With these variations in understanding came a wide variety of CIP implementations from the entities.

Ambiguity in the CIPs contributed to misunderstandings, not only between entities and auditors, but between the auditors themselves. A common result of a communication gap between entities and auditors was regeneration of paperwork. Entities found themselves changing words in their documents to satisfy the auditors. There were instances where entities experienced such frustration that they simply rewrote their procedures with copy and paste verbiage from the CIP standards. Unfortunately, often times those documents ended up being satisfactory for the audits, resulting in entities that were compliant but not necessarily secure.

**Theme 8: Inconsistent Audits or Auditing**

Participants that were regular full time entity employees voiced the frustration they felt with inconsistent NERC audits. Participants performing contract work, research or consulting activities for entities expressed their customers' exasperation with the inconsistencies surrounding audits throughout the NERC regions. The rules for auditing CIP programs seemed to differ between regions; what was important in an audit for one region may not have been important in another region. This was particularly vexing for large entities operating in more than one NERC region.

Two participants made nearly identical statements concerning auditors' desires to take entity documents with them at the conclusion of an on-site inspection. The rules regarding removal of documents differed between auditors. There was no published uniformity guiding audit requirements. Therefore, some entities experienced audits where the auditors removed documentation from their site while other auditors stated that taking documents from sites was not permitted by NERC. In these instances, NERC requirements for documentation appeared divergent.

Another area of audit inconsistency existed in the objectives of audits. One participant noted that some auditors looked only at titles of documents and what words were used in the documents, paying no attention to the intent of the document. This participant stressed that across the NERC regions, auditors do not seem to be looking for the same things in cyber programs. These inconsistencies are evident intra region between the entities as well as between NERC regions. An auditor may be concerned with how procedures are titled and the formatting of the procedure, not the technical applicability of the procedure for its intended use.

### Theme 9: Cyber Security Always in Response Mode

The BES is not a singular target of attack. Hackers and cyber criminals are constantly coming up with new ways to try to compromise systems anywhere. Cyber threats are not limited to attempts to break into systems or networks from the outside. Insider threats are people who have access to systems, software, networks, and other equipment as trusted individuals, commonly employees of a company or entity.

Whether the threat is from an insider or someone on the outside, cyber security protections cannot predict how the next compromise will happen, what it will look like or when it will occur. Several participants agreed that cyber security must continually adapt to the changing threat environment to remain a viable protective force against cyber criminals. Adversaries do not announce their attacks. Protecting the BES requires vigilance and awareness that cyber security will never move ahead of the attackers but will always be responding to and recovering from the attacks.

## Summary

Qualitative exploratory inquiry was the research design chosen for this study. A lack of research and literature on the subject of the effect of the implementation of the NERC CIPs on the reliability of the BES made exploratory research the best research design choice. According to Bacchetti (2002), new research needs to have a starting place. Zikmund et al. (2012) noted that exploratory research can be an appropriate starting point for a topic, emphasizing that performing an exploratory study can help reduce the chance of initiating future research on ambiguous, spurious or otherwise misleading research goals.

Chapter 4 included a description of the sample frame implemented in the study followed by the methodological approach applied to the data analysis. Data and results from the semi-structured interviews were detailed including a qualitative data presentation followed by a quantitative summary of the results (Mays & Pope, 1995). The quantitative summary expounded upon the interview questions which were expressed in figures 3 through 13. The 9 themes followed the quantitative summary generated from the interview data. Chapter 4 concluded with the summary.

# CHAPTER 5. DISCUSSION, IMPLICATIONS, RECOMMENDATIONS

## Introduction

The goal of this chapter was to summarize and discuss the results of the study in relation to the research question and outline recommendations for further research. Additionally, implications and suggestions for management and operations groups in entities responsible for implementation of the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards in the electricity critical infrastructure were presented. A summarization and discussion of the results of the study followed by implications of the results and limitations of the research were included. This chapter, as well as the study, culminated in the last section of the chapter, the conclusion.

From an academic perspective, the results and recommendations from this research should be enlightening and beneficial to those continuing to research the effectiveness of the CIPs on the reliability of the Bulk Electric System (BES). From the vantage point of businesses and BES entity managements, including the regulator, the synopsis of recommendations outlined in the interventions section of Chapter 5 should contribute to a more thorough understanding of opinions surrounding the CIP standards coming from a range of subject matter experts (SMEs) who have been performing the implementation of the CIPs or assisting others that have been doing the implementing at their facilities. There is absolutely no hesitation in stating that complying with the CIP standards has been a monumental undertaking, regardless of the size of the utility; small, medium or large. As one participant conveyed, the CIPs have given people pain and suffering. Of that, there is no doubt.

## Summary of the Results

After the September 11, 2001 terrorist attacks, physical and cyber security in the United States experienced increased attention (Hobijn, 2002). Compliance with NERC standards, which support the reliability of the BES, was required as of March, 2007 (Zhang & Stern, 2010) with the exception of the CIPs. In December, 2009, conformance with the CIP standards (Kaun, 2010) was obligatory. The CIPs were intended to increase the reliability of the BES by strengthening cyber security postures of the entities in NERC regions (Staggs, 2008).

Data from this study indicated that implementations of CIP programs in NERC regions have been concluded and many audits completed. Prior to this study, documented evidence of the effect of the CIP standards on the reliability of the BES was unavailable. As a result, and similar to a clean energy study in Colorado and Montana (Davis & Hoffer, 2010), this study utilized qualitative exploratory research methodology. The purpose of this study was to research the effect that the implementation of the NERC CIPs has had on the reliability of the BES.

Data collection was performed via semi-structured interviews (Drever, 1995) with 13 SMEs experienced with CIP implementations throughout the NERC regions. Seven participants were direct full time employees of NERC entities. Six participants were indirect employees. Data from 11 interview questions resulted in the generation of 9 themes with data saturation (Guest et al., 2006) confirmed after Interview 13.

## Discussion of the Results

The problem that motivated this research was change in the reliability of the BES. The purpose of this study was to identify a theme or themes regarding changes in the

reliability of the BES as a result of the NERC CIP standards implementation. The study included a single research question: has the reliability of the North American Bulk Electric System been affected by the implementation of the North American Electric Reliability Corporation's Critical Infrastructure Protection Standards?

**Research Question Discussion**

Participant responses to the research question (RQ) resulted in seven participants expressing the opinion that the CIPs have improved the reliability of the BES. Four participants felt that reliability had not been improved. One participant expressed a neutral opinion regarding positive or negative change in BES reliability. One participant did not know if reliability of the BES had changed.

**CIPs Positive Effect on the BES**

One of the opinions that participants discussed regarding why they felt the reliability of the BES had improved included an increased awareness of cyber security as a result of the regulatory requirement to implement the CIP standards. For example, prior to the CIPs requirement, it was not uncommon for entities to have connectivity between their corporate and control systems networks (King, 2009). This configuration could render the control systems on the control network vulnerable to cyber-attack. If an attacker were able to compromise the corporate network and find a path to the control systems network, the control systems could be at risk.

Network separation was not the only awareness benefit the CIPs provided. P10 discussed how the CIPs necessitate that entities installed firewalls where, prior to CIP regulations, there may have been none. Installation of firewalls added another layer of protection to critical equipment which could offer additional layers of security, provided

the firewalls were configured properly. If the CIPs had not become a regulatory requirement, the additional firewall protection may not have been installed.

Increased awareness levels have not been limited to medium and larger sized entities. The CIP requirements have been especially helpful to smaller utilities that may have been ill informed concerning cyber security threats and vulnerabilities. Bolstering cyber awareness and protection in these entities has strengthened their position regarding BES reliability, according to P10. The small utilities are, now, not necessarily the fragile intersections in the BES that they may have been prior to CIP regulation.

**CIPs Negative Effect on the BES**

Participants who felt the CIPs have had a positive effect on the BES shared similar reasons for their opinions. In contrast, the participants that felt the CIPs have had a negative effect on the BES had different reasoning. Each of the four participants described somewhat differing viewpoints that led them to their opinions. Physical attacks possibly presenting a more immediate threat (compared with cyber-attacks) was one opinion. Paperwork requirements and rerouted funds were other issues conveyed as contributing to a negative impact of the CIPs on the reliability of the BES.

Prior to the CIP standards becoming a regulatory requirement (Kaun, 2010), there was a lack of consistency in the electricity industry with regard to cyber security. Complying with CIPs, entities must have implemented the standards according to the requirements and may not simply have chosen if they wanted to comply or not. As a result, increased reliability of the BES should be the benefactor through standardized equipment, configurations, processes and procedures. However, a cyber security program is only as effective as its implementation. Incorrect equipment configurations or

poorly written processes and procedures would not be conducive to increased BES reliability.

While one participant stated that the CIPs have had a positive effect on the reliability of the BES, this conclusion was reached under the assumption that this positive effect was a result of the CIP standards having been properly written. This statement was not expanded upon; however, data resulting in the formulation of Theme 7 offered additional insight. Theme 7 included opinions from participants regarding the widespread lack of a common vocabulary with respect to the NERC CIPs.

Misunderstandings included auditors to entity members. Inconsistent vocabularies have led to confusion between those implementing the standards and those enforcing them, resulting in questionable or confounding violations and fines. Data generated in this study did not offer any indication that the CIP standards were written properly or improperly. Additionally, data defining what would constitute properly written standards was absent in this study.

A participant explained that fluctuating vocabularies between NERC regions was exceptionally confusing for entities spanning multiple regions. This participant continued, "People in [the] SPP [region] were told to do things totally different than people in [the] WECC [region]." Often, the rules would conflict, causing one region to implement their program under one interpretation of the regulation while another region could be performing the exact opposite implementation under completely different guidance for the same standards.

## Implications of the Study Results

There is evidence of a growing cyber security threat environment through the increase in successful attacks on organizations (Order, 2013). Stuxnet was a detailed attack on a very specific target (Falliere et al., 2011) located in control system architecture and was the first of its kind. One participant indicated that there are no meaningful metrics available regarding cyber-attacks. A review of NERC public records summarizing entity cyber security violations and fines are inconclusive with respect to cyber-attack trends.

The signing of Executive Order 13636 (2013), Improving Critical Infrastructure Cybersecurity, exemplifies the continued commitment of the United States to support increasing cyber security for critical infrastructure sectors. The issues articulated by the participants in this study may not cause significant concern, singularly, regarding a threat to the reliability of the BES. When considered cumulatively, however, these factors have the potential to negatively impact the BES which may possibly create an attractive target for an adversary. Moreover, one participant succinctly stated that "CIP implementations will never be complete. Security has to constantly evolve to match the threats."

Theme 5 consisted of participant opinions concerning entities' compliance with the NERC CIP requirements not necessarily equating with successfully achieving appropriate cyber security. The NVivo results from the data examination elucidate five participants stipulating that utilities have complied with CIP requirements but may not have attained sufficient security to protect their assets. This theme was the fifth strongest of the 9 themes yet contained the highest number of coding references (number of times mentioned by the five participants) of all themes. Comments from the participants

included, “they [entities] have done what was required to become NERC CIP compliant. They have not done what they needed to do…to secure their systems”; “they are compliant, not necessarily secure”; and one participant’s five compliance versus security comments regarded having worked with clients that were not nearly as concerned about true cyber security as they were about being compliant with the standards.

Implications from this study include another perspective to examine with respect to BES reliability: smaller entities in the NERC regions. Data from the interviews suggested that large utilities are generally equipped with sufficient budgets and personnel to adequately implement the requirements of the CIPs. Cyber awareness has increased across all entity members but smaller entities may have struggled, on several levels, with the implementation requirements. Regulations should be consistent across entities, regardless of their size, but regulators might consider the impact of their requirements on small entities and offer assistance or incentives to help them achieve compliance.

## Limitations

An unfortunate but not unexpected limitation surfaced at the onset of the study. When participant recruitment began, several potential participants expressed interest in the study and began dialog with the researcher, but ultimately did not return invitations to interview. Still other potential interviewees returned consent forms but then contacted the researcher at a later date and withdrew from participation. Reasons for opting out included an interested person who received legal advice not to participate and other individuals who said they “had better not” participate.

It was clearly understood, when this study was being developed, that people in the highly regulated electricity critical infrastructure fear repercussions, both real and

perceived, from regulators, legal departments, management, and even peers. For that reason, special consideration was given when developing participant consent forms and researcher scripts that explained protections to potential and confirmed participants. In spite of detailed explanations of anonymity and confidentiality, some participants withdrew before beginning their interview. None of the participants that began their interviews withdrew from the study.

## Recommendations for Further Research or Interventions

This section of the chapter was divided into two parts: the scholastic section including recommendations for further research, and the management and operations section including recommended interventions intended for NERC entities as well as the regulator. The recommendations for further research were derived from the study data which resulted in the generation of 9 themes and the limitation that arose during the study. The interventions intended for management and operations were also attained from study data.

### Recommendations for Further Research

The limitation this study encountered offers an opportunity for further research. A case study into reasons why this study's sample frame individuals were reluctant to participate in this research may be valuable to entities in the electricity industry as well as the regulator. The sensitivity of this topic cannot be overstated. A study of this type may be appropriate for researchers in the field of psychology or business.

Theme 1, Entities Removing Equipment to Avoid CIPs, and Theme 3, NERC Fines Influencing Implementation, may be correlated. Theme 1 was the strongest theme in this study with seven participants providing data. Theme 3 was the third strongest

theme with six participants contributing opinions. Development of hypotheses and research into a correlation between these two themes may result in conclusions that could be beneficial to not only the research community but the energy critical infrastructure. An opportunity for causality research may also exist.

An additional correlational/causality research opportunity may exist between Theme 4, Removing SMEs to do CIP Paperwork, and Theme 5, Compliance versus Security, from this study. Hypotheses could potentially be developed regarding SMEs that are unavailable to support their systems after being re-tasked to complete paperwork required for CIP compliance. As a result, entities may become less secure but appear compliant with regulations. The importance of BES reliability as it relates to regulatory compliance is in need of further investigation.

This exploratory study did not delineate between small, medium and large utilities. Research opportunities are available regarding how the CIPs have affected these entities by comparing them with each other: small utilities with other small utilities, and so on, a true apples-to-apples comparison. This study gathered data from large entities required to comply with all of the CIP standards as well as small utilities responsible for only CIP-002 compliance. Narrowing the scope of a study may offer deeper insight into the effects of the CIPs on like entities.

Quantitative opportunities for additional research include studies into BES reliability affected by human error. A cause and effect relationship between BES disturbances related to human error may also offer data of interest to the regulator and management of entities. Additional detail in a cause and effect study may include reasons for the human error. How the CIP standards relate to the human error and were

standards not adhered to, resulting in an effect on BES reliability could be additional components to the study.

**Recommendations for Interventions**

Theme 7, Lack of Common Vocabulary, and Theme 8, Inconsistent Auditors or Auditing, offers opportunities for both entity management as well as the regulator. A starting point may include conversations between entity management individuals and NERC regions to confirm that a consistent vocabulary exists. Definitions of terms should be made clear. Interpretations of standards should be transparent.

Participants in this study were straightforward regarding the lack of clarity between entities, regions, auditors and the regulator. Expectations and guidance coming from the regulator and regions and going to the entities (as well as intra-entity) should also be transparent. One participant confirmed the lack of openness in the industry, saying that utilities "clammed up" around the time the audits began.

This management and organizational recommendation may tie into the recommendation for further research into why people in the electricity industry seem to be unwilling to communicate on regulatory topics. A suggestion for management and the regulator includes communication with scholastic research in the area investigating why utilities are reluctant to talk. There may be enlightenment that could benefit both sides; the entities and the researchers.

Similar to confusing vocabularies throughout the regulatory component of the electricity critical infrastructure, identifying what constitutes properly written standards would assist entities in their compliance efforts. In an effort to avoid verboseness, a standard for the CIP standards may be appropriate. Management and the regulator should

again strive for transparency in the publication of the standards. This recommendation should not be limited to the CIPs but be applicable across all of NERCs reliability standards.

Reliability and resiliency are not the same, as stated by P9. Resiliency supports reliability. Resiliency is especially appropriate when considering a combined physical/cyber-attack. The Metcalf electrical substation in California that was attacked in 2013 could serve as an introduction into the realm of combined attacks. A recommendation for entity management personnel as well as the regulator includes consideration of the potential for a combined attack and evaluating the BES against such an attack. If not already done so, evaluations of mitigations should be completed.

Finally, as the smart grid continues development and implementation, CIP standards will require retrofitting or revision to keep pace with technology. Currently, the CIP standards support a primarily analog BES. As the analog technology is replaced with digital and the smart grid comes online, NERC should have a plan in place to support with appropriate cyber security standards. Theme 9 in this study summarized participant data regarding cyber security always being in a response mode with regard to cyber-attacks. The smart grid becoming fully integrated in the BES with a lack of cyber security standards to protect it is an undesirable place for the United States to be.

## Conclusions

A lack of published literature on the research topic for this study prompted the choice of a qualitative exploratory inquiry research methodology (Davis & Hoffer, 2010) to perform this study. A single research question was posed regarding the effect of the implementation of the NERC CIP standards on the reliability of the BES. 11 semi-

structured interview questions elicited participant responses which resulted in the generation of 9 themes and data applicable to the research question. From a scholastic perspective, suggestions for further research were developed from the themes. From a business and technology perspective, suggested implications for management and operations, in addition to the regulatory body, NERC, arose from the themes.

To answer the research question "Has the reliability of the North American Bulk Electric System been affected by the implementation of the North American Electric Reliability Corporation's Critical Infrastructure Protection Standards?" data from the research question revealed 7 of the 13 study participants expressing an opinion that the CIPs have had a positive effect on the reliability of the BES. Four participants conveyed an opinion that the CIPs have had a negative effect on reliability. One participant had a neutral opinion and one participant did not know if the CIPs have affected BES reliability in either a positive or negative manner.

Prior studies and previous literature on the topic of CIP standards' effectiveness on the reliability of the BES were undocumented and, therefore, unavailable to link this research with. This inaugural study has presented multiple opportunities for continued research in several areas related to the CIPs effect on the reliability of the BES. Suggestions for qualitative and quantitative methodologies were proposed. Case studies, correlational research and cause and effect analyses were a few of the proposals that would be appropriate follow-on research to this study.

Study participants emphasized that cyber security is constantly changing to adapt to the sustained threat environment that is ever present in society. Currently, NERC entities are operating under revision 3 of the NERC CIP standards. Revision 4 was

cancelled and revision 5 will require entities to update their cyber security programs to comply with the new revision. New CIP standards have been developed and are subject to future enforcement: CIP-010, Configuration Change Management and Vulnerability Assessments, and CIP-011, Information Protection (NERC, 2013).

Executive Order 13636 (2013) is undergoing implementation. The order contains requirements that will be in addition to the NERC standards for the BES. Cyber security challenges will constantly increase in complexity, standards requirements notwithstanding. Considering the changes on the horizon for the energy critical infrastructure, and as suggested by P12, the continued applicability and effectiveness of the NERC CIPs on the reliability of the BES is a question that should be answered definitively, sooner than later.

## REFERENCES


Abell, J., Locke, A., Condor, S., Gibson, S., & Stevenson, C. (2006). Trying similarity, doing difference: The role of interviewer self-disclosure in interview talk with young people. *Qualitative Research, 6*(2), 221-224.

Abbotts, N., Anderson, P. J., & Kari, D. G. (2010). Is your organization prepared for compliance with NERC reliability standards? *Mondaq Business Briefing*. Retrieved from http://www.perkinscoie.com/news/pubs_detail.aspx?op=updates&publication=2487

Amin, M., & Schewe, P. F. (2007). Preventing blackouts. *Scientific American. 296*(5), 60-67.

Anderson, R., & Fuloria, S. (2010). Security economics and critical national infrastructure. In T Moore, D. J. Pym & C. Ioannidis (Eds.), *Economics of Information Security and Privacy* (pp. 55-66). New York, NY: Springer.

Anfara Jr, V. A., & Mertz, N. T. (Eds.). (2006). *Theoretical frameworks in qualitative research*. Thousand Oaks, CA: Sage.

Apt, J., Lave, L. B., Talukdar, S., Morgan, M. G., & Ilic, M. (2004). Electrical blackouts: A systemic problem. *Issues in Science and Technology*, *20*(4), 55-61.

Bacchetti, P. (2002). Peer review of statistics in medical research: The other problem. *BMJ: British Medical Journal*, *324*(7348), 1271.

Bariball, K., & White, A. (1994). Collecting data using a semi-structured interview: A discussion paper. *Journal of Advanced Nursing, 19*(2), 328-335. doi: 10.1111/j.1365-2648.1994.tb01088.x

Bartol, N., Dunn, D., Glantz, C., Goff, E., Jereza, K., Lee, A., . . . Seader, M. (2014). *Cybersecurity procurement language for energy delivery systems.* Energy Sector Control Systems Working Group. Washington, D.C. Retrieved from http://energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf

Battaglia, M. (2008). Purposive sample. In P. Lavakas (Ed.), Encyclopedia of survey research methods. (p. 646). Thousand Oaks, CA: Sage. doi: 10.4135/9781412963947.n419

Bell, D. S. (1964). Jurisdiction of the Federal Power Commission under the Natural Gas Act-Commingled Gas. *Louisiana Law Review, 24*(3), 600.

Benoit, J. (2008). Meeting IED integration cyber security challenges (conference). Presented at the Eskom Southern Africa Power System Protection Conference. South Africa.

Berkeley III, A. R., Gallegos, G. G., & Grayson, M. E. (2008). Critical infrastructure partnership strategic assessment final report and recommendations. *National Infrastructure Advisory Council, 64,* 3.

Billson, P. (2010). Qualitative research. *Supply Management, 15*(1), 37. Retrieved from http://search.proquest.com.library.capella.edu/docview/1354059737?accountid=27965

Blanton, M. (2010). *Nuclear energy: Protecting the nation's infrastructure-safety and security*. Section of Public Utility, Communications, and Transportation Law. Report of Nuclear Energy Committee 2010 Fall Council Meeting, 1.

Bloomberg, L. D., & Volpe, M. (2008). *Completing your qualitative dissertation: A roadmap from beginning to end.* Thousand Oaks, CA: Sage. doi: 10.4135/9781452226613.n1

Boin, A., & McConnell, A. (2007). Preparing for critical infrastructure breakdowns: The limits of crisis management and the need for resilience. *Journal of Contingencies and Crisis Management*, *15*(1), 50-59.

Bowen, G. A. (2008). Naturalistic inquiry and the saturation concept: A research note. *Qualitative Research, 8*(1), 137-152. doi: 10.1177/1468794107085301

Bowman, D. (2004). *Experience effects on brand choice.* Zyman Institute of Brand Science. Retrieved from http://www. zibs.com/bowman1.shtml

Boyatzis, R. E. (1998). *Transforming qualitative information: Thematic analysis and code development*. Thousand Oaks, CA: Sage.

Burns, N. (1989). Standards for qualitative research. *Nursing Science Quarterly, 2*(1), 44-52. doi: 10.1177/089431848900200112

Byres, E., & Lowe, J. (2004). The myths and facts behind cyber security risks for industrial control systems (conference). *Proceedings of the VDE Kongress*, *116*.

Cachia, M., & Millward, L. (2011). The telephone medium and semi-structured interviews: A complementary fit. *Qualitative Research in Organizations and Management, 6*(3), 265-277. doi: http://dx.doi.org/10.1108/17465641111188420

Caelli, K., Ray, L., & Mill, J. (2008). 'Clear as mud': Toward greater clarity in generic qualitative research. *International Journal of Qualitative Methods*, *2*(2), 1-13.

Camm, M., & Fox, C. (2010). The regulatory environment. *Under Control* (pp. 123-142). Retrieved from http://link.springer.com/chapter/10.1007/978-1-4302-1593-6_9

Cardenas, A. A., Amin, S., & Sastry, S. (2008). Secure control: Towards survivable cyber-physical systems. *System*, *1*(a2), a3.

Carpentier, D. (2011). Demonstrating compliance with North American Electric Reliability Corporation (NERC) reliability standards. *Natural Gas & Electricity*, *27*(9), 1-8.

Carspecken, P. F. (1996). Critical ethnography in educational research: A theoretical and practical guide. London, England: Routledge.

Chance, J. E. (2013). Preparing for a North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Audit. *Power, 157*(4), 28-35.

Childers, L. (1989). Credibility of public relations at the Nuclear Regulatory Commission (NRC). *Journal of Public Relations Research*, *1*(1-4), 97-114.

Church, R., & Scaparra, M. P. (2007). Analysis of facility systems' reliability when subject to attack or a natural disaster. *Advances in Spatial Science*. 221-241. doi: 10.1007/978-3-540-68056-7_11

Cohen, D., & Crabtree, B. (2006). Qualitative research guidelines project. *Robert Wood Johnson Foundation.* Retrieved from http://www.qualres.org/HomeSemi-3629.html

Coll-Mayor, D., Paget, M., & Lightner, E. (2007). Future intelligent power grids: Analysis of the vision in the European Union and the United States. *Energy Policy*, *35*(4), 2453-2465.

Congress, U. S. (1977). Department of Energy Organization Act. Washington, D.C: Public Law, 95-91.

Conrad, C. F., & Serlin, R. C. (2006). *The Sage Handbook for Research in Education.* Thousand Oaks, CA: Sage. doi: 10.4135/97814129760939.n26

Copeland, T. (2001). Is the "new terrorism" really new? An analysis of the new paradigm for terrorism. *Journal of Conflict Studies*, *21*(2).

Creswell, J. W. (2012). *Qualitative inquiry and research design: Choosing among five approaches*. Thousand Oaks, CA: Sage.

Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches*. Thousand Oaks, CA: Sage.

Creswell, J. W., Hanson, W. E., Clark Plano, V. L., & Morales, A. (2007). Qualitative research designs: Selection and implementation. *The Counseling Psychologist, 35*(2), 236-264.

Davies, P. (2006). Exploratory Research. In V. Jupp (Ed.), *The Sage dictionary of social research methods.* (pp. 111-112). London, England: Sage. Retrieved from http://srmo.sagepub.com.library.capella.edu/view/the-sage-dictionary-of-social-research-methods/SAGE.xml

Davis, C., & Hoffer, K. (2010). Energy development in the Rockies: A role for counties? *Publis: The Journal of Federalism, 40*(2), 296-311.

Dearnley, C. (2005). A reflection on the use of semi-structured interviews. *Nurse Researcher, 13*(1), 19-28.

Derene, G. (2009). How vulnerable is U.S. infrastructure to a major cyber attack? *Popular Mechanics*. Retrieved from http://www.popularmechanics.com/technology/military/4307521

Directive, P. P. (2013). PPD-21, Critical Infrastructure Security and Resilience. *Washington, DC: The White House*, *12*, 6.

Drever, E. (1995). Using semi-structured interviews in small-scale research. A teacher's guide. Retrieved from http://eric.ed.gov/?id=ED394990

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review, 45*(1), 67-87.

Eccleston, C., & Stuyvenberg, A. (2011). The perfect electrical storm? *Environmental Quality Management,* 20, 43-49. doi: 10.1002/tqem.20288

Ellis, A., Nelson, R., Von Engeln, E., Walling, R., McDowell, J., Casey, L., . . . & Kirby, B. (2012). *Reactive power interconnection requirements for PV and wind plants–recommendations to North American Electric Reliability Corporation (NERC)*. Albuquerque, NM: Sandia Corporation.

Eto, J. H., & LaCommare, K. H. (2008). *Tracking the reliability of the U.S. electric power system: An assessment of publicly available information reported to state public utility commissions.* Ernest Orlando Lawrence Berkeley National Laboratory. Berkeley, CA. Retrieved from http://escholarship.org/uc/item/2jq5z0m7

Evans, R. P., Carlson, R., Dagle, J., Scown, V. S., Shamsuddin, S., Shaw, G., . . . Schmidt, J. (2006). Process control system cyber security standards-an overview (symposium). Idaho National Laboratory. 52nd International Instrumentation Symposium.

Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. Stuxnet dossier. *White paper,* Symantec Corp., v1.4. Security Response.

Farrell, A., & Lave, L. (2002). Regulating and restructuring the U.S. electric power industry: Where we are and how we got here (invited talk). Consumer Energy Council of America. Washington, D.C.

Gallant, E. (2011). The SCADA worm threat to mission critical infrastructure. *Mission Critical,* (4)1, 30-35.

Gent, M. R. (1995). Inter-firm cooperation: Maintaining reliability of electricity supply. C. J. Andrews (Ed.). *Regulating regional power systems*, 149.

Given, L. M. (2008). *The Sage encyclopedia of qualitative research methods.* Thousand Oaks, CA: Sage. doi: 10.4135/9781412963909

Gleick, P. H. (2006). Water and terrorism. *Water Policy*, *8*(6), 481-503.

Glenn, J. C. (2010). Handbook of Research Methods. Jaipur, IN: Oxford.

Government Accountability Office (GAO) (2013). *Critical infrastructure protection: DHS could strengthen the management of the regional resiliency assessment program* (GAO Publication No. GAO-13-616). Washington, D.C: Government Accountability Office.

Green, J., Willis, K., Hughes, E., Small, R., Welch, N., Gibbs, L., & Daly, J. (2007). Generating best evidence from qualitative research: the role of data analysis. *Australian and New Zealand Journal of Public Health*, *31*(6), 545-550.

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field Methods, 18*(1), 59-82. doi: 10.1177/1525822X05279903

Haase, J. E., Heiney, S. P., Ruccione, K. S., & Stutzer, C. (1999). Research triangulation to derive meaning-based quality-of-life theory: Adolescent resilience model and instrument development. *International Journal of Cancer*, *83*(S12), 125-131.

Hamaker, C. (2006). What's next for cyber-security? *Public Utilities Fortnightly, 144*(8), 34-37.

Hancock, B., Windridge, K., & Ockelford, E. (2007). An Introduction to Qualitative Research. The National Institute for Health Research. Birmingham, UK: NIHR RDS EM / YH.

Hand, H. (2003). The mentor's tale: A reflexive account of semi-structured interviews. *Nurse Researcher, 10*(3), 15-27.

Hardcastle, M, Usher, K., & Holmes, C. (2005). Carspecken's five-stage critical qualitative research method: An application to nursing research. *Qualitative Health Research, 16*(1), 151-161.

Harkins, M. (2013). Emerging threats and vulnerabilities. *Managing Risk and Information Security* (pp. 71-85). Retrieved from http://link.springer.com/chapter/10.1007/978-1-4302-5114-9_6#page-1.

Hart, S., & Ramsay, J. (2011). A guide for homeland security instructors preparing physical critical infrastructure protection courses. *Homeland Security Affairs*, *7*(1), 1.

Henrie, M. (2013). Cyber security risk management in the SCADA critical infrastructure environment. *Engineering Management Journal, 25*(2), 38-45.

Hobijn, B. (2002). What will homeland security cost? *Federal Reserve Bank of New York Economic Policy Review*, *8*(2), 21-33.

Holloway, I., & Biley, F. C. (2011). Being a qualitative researcher. *Qualitative Health Research*, *21*(7), 968-975.

Holmes, C. A., & Smyth, W. (2011). Carspecken's critical methodology - A theoretical assessment. *International Journal of Multiple Research Approaches, 5*(2), 146-154.

Hoover, J. B. (2000). The changing world of power monitoring (conference). *Telecommunications Energy Conference, 2000.* INTELEC. Twenty-second International, 103-108. doi:10.1109/INTLEC.2000.884235

Hulme, G. V. (2011). SCADA insecurity. *Information Security, 13*(1), 38-44.

IESO_GDE_0364 (2013), Part 11.1: Applicability criteria for compliance with NERC reliability standards and NPCC criteria, *2*. Retrieved from http://www.ieso.ca/Documents/ircp/IESO_Applicability_Criteria_for_Compliance_with_NERC_Standards_and_NPCC_Criteria.pdf

Inslee, J., Larsen, R., & McDermott, J. (2006). Letter to the Federal Energy Regulatory Commission. Office of External Affairs, Congress of the United States. Retrieved from http://elibrary.ferc.gov/IDMWS/common/opennat.asp?fileID=11076068

Irvine, A., Drew, P., & Sainsbury, R. (2013). 'Am I not answering your questions properly?' Clarification, adequacy and responsiveness in semi-structured telephone and face-to-face interviews. *Qualitative Research, 13*(1), 87-106.

Jackson, S. J., Edwards, P. N., Bowker, G. C., & Knobel, C. P. (2007). Understanding infrastructure: History, heuristics and cyber infrastructure policy. *First Monday*, *12*(6).

Jebreen, I. (2012). Using inductive approach as research strategy in requirements engineering. *International Journal of Computer and Information Technology, 01*(02).

Jindra, M. (2005). The market for Internet domain names. *Policy*, *24*(6-7), 553-563.

Joffe, H. (2011). *Thematic analysis.* 209-223. Chichester, UK: John Wiley & Sons.

Jones, R. O. (2007). An examination of tenant evolution within the UK factory outlet channel. *International Journal of Retail & Distribution Management*, *35*(1), 38-53.

Jones, S. A. (2013). Illustrating the narrative process through career stories. *School Libraries Worldwide*, *19*(2), 37.

Kajornboon, A. B. (2005). Using interviews as research instruments. *E-Journal for Research Teachers, 2*(1). Retrieved from http://www.culi.chula.ac.th/e-Journal/bod/Annabel.pdf

Kaptein, M., & Schwartz, M. S. (2008). The effectiveness of business codes: A critical examination of existing studies and the development of an integrated research model. *Journal of Business Ethics, 77*,111-127. doi: 10.1007/s10551-006-9305-0

Kaun, R. (2010). Changing the way we think (whitepaper). Matrikon. Retrieved from http://www.matrikon.com/portal/downloads/industrial_Security/ISC_changingthewaywethink.pdf

Kerr, P. K., Rollins, J., & Theohary, C. A. (2010). *The Stuxnet computer worm: Harbinger of an emerging warfare capability,* 1-9. Congressional Research Service. Washington, D.C.

Keogh, M., & Cody, C. (2013). *Resilience in regulated utilities.* The National Association of Regulatory Utility Commissioners (NARUC). Retrieved from http://www.naruc.org/Grants/Documents/Resilience%20in%20Regulated%20Utilities%20ONLINE%2011_12.pdf

Kim, C. J., & Obah, O. B. (2007). Vulnerability assessment of power grid using graph topological indices. *International Journal of Emerging Electric Power Systems*, *8*(6). doi: 10.2202/1553-779X.1738

Kim, C. L., Hall, M. E. L., Anderson, T. L., & Willingham, M. M. (2011). Coping With Discrimination in Academia Semi-Structured Interview [database record]. Retrieved from PsycTESTS. doi: 10.1037/t08577-000

King, J. (2009). The new ground zero in internet warfare. *Computerworld, 43*(17), 30-32.

Krefting, L. (1991). Rigor in qualitative research: The assessment of trustworthiness. *The American journal of occupational therapy*, *45*(3), 214-222.

Lambrechts, R. J. (2011). The U.S. electrical grid: Surviving cyber-terrorism and solar flares. *Natural Resources & Environment, 25(*42).

Larence, E.R. (2007). *Critical infrastructure protection: Sector plans and sector councils continue to evolve*. Washington, D.C: United States Government Accountability.

Lawson, F. H. (2004). Grave new world: Security challenges in the 21st century. *Perspectives on Political Science*, *33*(1), 52.

Lerner, E. J. (2005). What's wrong with the electric grid? *Gravitational, Electric and Magnetic Forces: An Anthology of Current Thought*. Available from http://books.google.com/books?hl=en&lr=&id=wogh8Bvs9cwC&oi=fnd&pg=PA41&ots=p2mWO6K-1F&sig=xoZQwZP0XUJsme5YpSjNFri2i4E#v=onepage&q&f=false

Lewis, J. (2010). The electrical grid as a target for cyber attack. *Center for Strategic and International Studies*.

Li, J., Yamashita, K., Liu, C-C., Zhang, P. & Hofmann, M. (2008). Identification of cascaded generator over-excitation tripping events (conference). 16th Power Systems Computation Conference. Glasgow, Scotland.

Lincoln, Y. S., & Guba, E. A. (1985). *Naturalistic inquiry.* Thousand Oaks, CA: Sage.

Lindstrom, J. (2005). Inside the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards. Retrieved from http://www.symantec.com/resources/articles/article.jsp?aid=IN_091105_inside_nerc_cip_standards

Long, T., & Johnson, M. (2000). Rigour, reliability and validity in qualitative research. *Clinical effectiveness in nursing*, *4*(1), 30-37.

Lyons, C., Jacobi, J., & Starkweather, R. (2008). North American Electric Reliability Corporation (NERC) standards and standards compliance: Still a work in progress? *The Electricity Journal*, *21*(3), 29-39.

Marnay, C. (2007). Microgrids and heterogeneous security, quality, reliability and availability (conference). Power Conversion Conference, April 2-5, 2007. Nagoya. doi: 10.1109/PCCON.2007.373031

Mason, M. (2010). Sample size and saturation in PhD studies using qualitative interviews. *Forum: Qualitative Social Research*, *11*(3).

Massoud Amin, S., & Wollenberg, B. F. (2005). Toward a smart grid: power delivery for the 21st century. *Power and Energy Magazine, IEEE*, *3*(5), 34-41.

Mays, N., & Pope, C. (1995). Rigour and qualitative research. *BMJ: British Medical Journal*, *311*(6997), 109.

Mazanec, B. M. (2009). The art of (cyber) war. *Journal of International Security Affairs*, *16*, 84.

McAllister, L., & Dawson, K. L. (2010). Restoring faith in the bulk-power system: An early assessment of mandatory reliability standards. *The Electricity Journal*, *23*(2), 18-28.

McClelland, J. (2012). Testimony of Joseph McClelland, Director, Office of Electric Reliability, Federal Energy Regulatory Commission. Before the Committee on Energy and Natural Resources, United States Senate. Washington, D.C.

McKay, B. (2011). Lessons to learn for U.S. electric grid critical infrastructure protection: Organizational challenges for utilities in identification of critical assets and adequate security measures (conference). *System Sciences (HICSS), 2011 44th Hawaii International Conference, IEEE.*1-9.

McLoughlin, D. (1985). A framework for integrated emergency management. *Public Administration Review*, *45*(special issue), 165-172. doi: 10.2307/3135011

Messmer, E. (2006). Energy firms race to meet security rules. *Network World, 23*(38), 15-16.

Minkel, J. R. (2008). The 2003 northeast blackout--five years later. *Scientific American.* Retrieved from http://www.scientificamerican.com/article/2003-blackout-five-years-later/

Moot, J. S. (2006).Testimony of John S. Moot, General Counsel. Electric Power Reliability. Docket No. RM05-30-000 – Order No. 672 and 672A.

Morse, J. M., Barrett, M., Mayan, M., Olson, K., & Spiers, J. (2002). Verification strategies for establishing reliability and validity in qualitative research. *International journal of qualitative methods*, *1*(2).

Moteff, J., Copeland, C., & Fischer, J. (2003). *Critical infrastructures: What makes an infrastructure critical?* (Report for Congress CRS-17). Washington, D.C: Congressional Research Service, the Library of Congress.

Moteff, J., & Parfomak, P. (2004). *Critical infrastructure and key assets: definition and identification.* Washington D.C: Library of Congress, Congressional Research Service.

Murray, B. L. (2003). Qualitative research interviews: Therapeutic benefits for the participants. *Journal of Psychiatric and Mental Health Nursing, 10*(2), 233-236.

Naedele, M. (2005). Standardizing industrial IT security-a first look at the IEC approach (conference). In *Emerging Technologies and Factory Automation, 2005. ETFA 2005.* 10th IEEE Conference, vol. 2, 863-870. doi: 10.1109/ETFA.2005.1612763.

Newman, I., & Benz, C. R. (1998). *Qualitative-quantitative research methodology: Exploring the interactive continuum*. Southern Illinois: University Press.

Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of cyber-warfare. *Computers & Security*, *31*(4), 418-436.

Nicholson, T. (2009). Protecting critical cyber assets through North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) mandates. *Electric Power and Light, 87*(3), 16-17.

Nicol, D. M. (2011). Hacking the lights out. Computer viruses have taken out hardened industrial control systems. The electrical power grid may be next. *Scientific American*, *305*(1), 70.

North American Electric Reliability Corporation (NERC) (2002). 1997 system disturbances: Review of selected 1996 disturbances in North America. Retrieved from http://www.nerc.com/files/disturb96.pdf

North American Electric Reliability Corporation (NERC) (2011). 2010 Annual Report. Retrieved from http://www.nerc.com/files/2010_Annual_Report.pdf

North American Electric Reliability Corporation (NERC) (2011). Glossary of terms used in NERC reliability standards. North American Electric Reliability Corporation. Retrieved from http://www.nerc.com/files/Glossary_of_Terms_2011October26.pdf

North American Electric Reliability Corporation (NERC) (2013). United States mandatory standards subject to enforcement. Retrieved from http://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20States

Nugent, J. H., & Raisinghani, M. S. (2002). The information technology and telecommunications security imperative: Important issues and drivers. *Journal of Electronic Commerce Research*, *3*(1), 1-14.

Oliver-Hoyo, M., & Allen, D. (2006). The use of triangulation methods in qualitative educational research. *Journal of College Science Teaching*, *35*(4).

Order, E. (1996). 13010. Critical infrastructure protection. *Federal Register*, *61*(138), 37347-37350.

Order, E. (2013). 13636. Improving critical infrastructure cybersecurity. *Federal Register*, *78*(33), 11739.

O'Rourke, T. D. (2007). Critical infrastructure, interdependencies, and resilience. *Bridge-Washington-National Academy of Engineering*, *37*(1), 22.

Osofsky, H. M., & Wiseman, H. J. (2013). Hybrid energy governance. *University of Illinois Law Review, Forthcoming*, 12-49.

Pekrun, R., Goetz, T., Titz, W., & Perry, R. P. (2002). Academic emotions in students' self-regulated learning and achievement: A program of qualitative and quantitative research. *Educational Psychologist, 37*(2), 91-106.

Petit, F. D. P., Bassett, G. W., Black, R., Buehring, W. A., Collins, M. J., Dickinson, D. C., . . . Peerenboom, J. P. (2013). *Resilience measurement index: An indicator of critical infrastructure resilience* (Report No. ANL/DIS-13-01). Argonne National Laboratory, Chicago, IL. doi: 10.2172/1087819

Plakhotnik, M. S., & Rocco, T. S. (2009). Literature reviews, conceptual frameworks, and theoretical frameworks: Terms, functions, and distinctions. *Human Resource Development Review, 8*(1), 120-130.

Pollak, D. (2007). SD Warren and the erosion of federal preeminence in hydropower regulation. *Ecology Law Quarterly*, *34*(3).

Pollet, J., Sikora, W., & Batug, J. (2009). Helping power plant control systems achieve North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) compliance. *Power, 153*(3), 68-71.

Prezant, D. J., Clair, J., Belyaev, S., Alleyne, D., Banauch, G. I., Davitt, M., . . . Kalkut, G. (2005). Effects of the august 2003 blackout on the New York City healthcare delivery system: A lesson for disaster preparedness. *Critical Care Medicine*, *33*(1), S96-S101.

Ralston, P. A., Graham, J. H., & Patel, S. C. (2006). Literature review of security and risk assessment of SCADA and DCS systems. University of Louisville, Louisville, Kentucky.

Risley, A., & Carson, K. (2006). Low-or no-cost cybersecurity solutions for defending the electric power system against electronic intrusions. *Schweitzer Engineering Laboratories Inc.* Pullman, WA.

Roberto, J. B., & de la Rubia, T. D. (2007). Basic research needs for advanced nuclear energy systems. *Journal of the Materials, Metals and Materials Society, 2*(4), 16-19. doi: 10.1007/s11837-007-0048-x

Rowland, K. (2011). Federal Energy Regulatory Commission (FERC) versus the North American Electric Reliability Corporation (NERC): A cyber security showdown? *Intelligent Utility, 3*(4), 14-18.

Salem, P. J. (2012). The use of mixed methods in organizational communication research. *Online Instruments, Data Collection, and Electronic Measurements: Organizational Advancements*. Available from http://www.igi-global.com/chapter/use-mixed-methods-organizational-communication/69732 doi: 10.4018/978-1-4666-2172-5.ch002

Schiff, D. (2007). Taking a wide-angle view of the U.S. electric power grid. *IEEE-USA Today's Engineer*, *09.07.*

Schaffer, G., Keil, T. M., & Mayer, R. (2010). *Communications Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*. Homeland Security.

Schneider, J. D. (2013). NERC on a wire. *Public Utilities Fortnightly, 151*(2), 32-38.

Seale, C. (1999). Quality in qualitative research. *Qualitative inquiry*, *5*(4), 465-478.

Sergel, R. P., Cook, D. N., & Counsel, G. (2006). *Application for recognition as the Electric Reliability Organization.* North American Electric Reliability Council and North American Electric Reliability Corporation. Alberta, Canada.

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information*, *22*(2), 63-75.

Shin, B. C. G., Gibson, P. F., Wangen, B. R., & Perez, L. A. (2011). Wide-area DTS implementation in the Western Electricity Coordinating Council (meeting). *Power and Energy Society General Meeting, 2011 IEEE,* 1-8.

Silverman, D. (2009). *Doing qualitative research.* Thousand Oaks, CA: Sage.

Silverman, D., & Marvasti, A. (2008). *Doing qualitative research: A comprehensive guide*. Thousand Oaks, CA: Sage.

Staggs, K. (2008). Meeting North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) requirements. *Power Engineering, 112*(9), 74-80.

Stamp, J., Campbell, P., DePoy, J., Dillinger, J., & Young, W. (2003). *Sustainable security for infrastructure SCADA* (SAND2003-4670C). Albuquerque, NM: Sandia National Laboratories.

Stamp, J. E., Laviolette, R. A., Phillips, L. R., & Richardson, B. T. (2009). *Final report: Impacts analysis for cyber attack on electric power systems* (SAND2009-1673). Albuquerque, NM: Sandia National Laboratories National SCADA Test Bed.

Stanhouse, D. W. (2003). Ambition and Abdication: Congress, the Presidency, and the Evolution of the Department of Homeland Security. *NCJ Int'l L. & Com. Reg.*, *29*, 691.

Stanton, J., Sampson, D., & Bloch, H. P. (2008). Grid reliability. *Power, 152*(3), 18-23.

Stanton, J. (2011). North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) update. *Power, 155*(6), 16-19.

Stapleton, P. (2009). North American Electric Reliability Corporation (NERC) drives development of sustainable compliance programs. *Power, 153*(2), 61-63.

Stouffer, K., Falco, J., & Scarfone, K. (2011). *National Institute of Standards and Technology (NIST) Special Publication 800-82, guide to industrial control systems (ICS) security*. Gaithersburg, MD: National Institute of Standards and Technology, Computer Security Division and Intelligent Systems Division.

Streeter, L. A., MacDonald, N. H., Apple, W., Krauss, R. M., & Galotti, K. M. (1983). Acoustic and perceptual indicators of emotional stress. *Journal of the Acoustical Society of America, 73*, 1354. doi: 10.1121/1.389239

Swanson, R. A., & Holton III, E. F. (2005). Research in organizations: Foundations and methods of inquiry. San Francisco, CA: Berrett-Koehler.

Swanstrom, D., & Jolivert, M. M. (2009). DOE transmission corridor designations & Federal Energy Regulatory Commission (FERC) backstop siting authority: Has the Energy Policy Act of 2005 succeeded in stimulating the development of new transmission facilities? *Energy Law Journal*, *30*(2).

Symbol, C. N. P., & Year, F. (2014). Annual Report. Centerpoint Energy Inc. Available from http://publish.generationhub.com/document/2014/02/26/CenterPoint%20Energy%202014%2010K,%20Feb%2026%202014.pdf

Taylor, L. Y. (2009). Update on development of North American Electric Reliability Corporation (NERC) requirements for verification of generator dynamic models (meeting). In *Power & Energy Society General Meeting, 2009. PES'09. IEEE*, 1-7.

Teddlie, C., & Yu, F. (2007). Mixed methods sampling a typology with examples. *Journal of Mixed Methods Research*, *1*(1), 77-100.

Thessin, J. (2003). Department of Homeland Security. *Harvard Journal on Legislation, 40,* 513-579.

Thilmany, J. (2012). SCADA security? *Mechanical Engineering, 134*(6), 26-31.

United States Congress House Committee on Science (2006). *Cyber security: U.S. vulnerability and preparedness: Hearing before the committee on science, House of Representatives, One Hundred Ninth Congress, first session, September 15, 2005*. Washington, D.C: U.S. Government Printing Office.

U.S. House of Representatives (2013). *Electric grid vulnerability: Industry responses reveal security gaps*. Washington, D.C: Staff of Congressmen Edward J. Markey and Henry A. Waxman.

Vaughan, R., & Pollard, R. (1984). *Rebuilding America: Planning and managing public works in the 1980's.* Washington, D.C: Council of State Planning Agencies.

Venkatasubramanian, V., & Li, Y. (2004). *Analysis of 1996 Western American electric blackouts.* Cortina d'Ampezzo, Italy: Bulk Power System Dynamics and Control-VI.

Wang, Y., Ruan, D., Xu, J., Wen, M., & Deng, L. (2010). Computational intelligence algorithms analysis for smart grid cyber security. In *Advances in Swarm Intelligence*. 77-84. Berlin, Heidelberg: Springer.

Weiss, J. (2010). *Protecting industrial control systems from electronic threats.* New York, NY: Momentum Press, LLC.

Whiting, L. S. (2008). Semi-structured interviews: Guidance for novice researchers. *Nursing Standard, 22*(23), 35-40.

Wollenberg, B. F. (2004). In my view-from blackout to blackout-1965 to 2003: How far have we come with reliability? *Power and Energy Magazine, IEEE*, *2*(1), 88-86.

Zhang, Y., & Wildemuth, B. M. (2009). *Qualitative analysis of content.* Applications of social research methods to questions in information and library science. 308-319.

Zhang, Z., & Stern, M.S. (2010). NERC today and tomorrow: Living in the new world of mandatory reliability standards. *Public Utilities Fortnightly, 14*(4).

Zikmund, W., Babin, B., Carr, J., & Griffin, M. (2012). *Business research methods.* Available from http://books.google.com/books?hl=en&lr=&id=ydcKAAAAQBAJ&oi=fnd&pg=PR6&dq=%22Business+research+methods%22+%22Zikmund%22&ots=Y5DpO0fd3z&sig=hjbSIceF6nLIuGsTrebQ013qLvs#v=onepage&q=%22Business%20research%20methods%22%20%22Zikmund%22&f=false

# APPENDIX A. INTERVIEW QUESTIONS

The structure of the interview questions used in this study was modeled after a survey instrument designed and implemented by Kim, et al. (2011). The survey instrument is available in the Capella University library which includes permission for research/teaching. The questions from Kim, et al. (2011) were modified, as outlined in Appendix A, to apply to this study.

Overview

1. (Q1) Has your organization completed implementation of the NERC CIP standards? If not, do you have an expected completion date?
2. (Q2) (for those who have completed implementation) How long has your CIP implementation program been complete?
3. (Q3) (for those who have not completed implementation) How many of the CIP standards do you have implemented at this time? Which ones?
4. (Q4) Which of the eight CIP standards were the most difficult to implement?
5. (Q5) (complete implementations) Has your program had a CIP audit yet? How did that go? (incomplete implementations) Do you have an audit scheduled?

Impact of the Critical Infrastructure Protection standards on the reliability of the Bulk Electric System

1. (Q6) Have you had any unplanned outages since [partial or full] implementation of the CIPs?
2. (Q7) If yes, was the outage due to an attack (as opposed to a natural event like a winter storm, for example)? If yes, was the attack physical or cyber, or could you tell?
3. (RQ) Do you think the implementation of the CIPs has had an effect on the reliability of the Bulk Electric System? Please explain what makes you feel that way.

Resources for Implementation

1. (Q8) How people/resources were required to implement the CIPs? Were the people full-time, permanent, contractors, etc.?
2. (Q9) How many people were working on cyber security before the CIPs were required? Did that number increase or decrease after the standards became enforceable?

Other

1. (Q10) Were there any equipment/software upgrades that were in process before the standards became enforceable? If so, were they completed? If not, did the reliability standards impact implementation?
2. (Q11) Is there anything else you would like to add to your responses to these questions?