

Critical Digital Infrastructure Protection: An Investigatoin Into The Intergovernmental Activities Of Information Technology Directors In Florida Counties

2004

Joah Nicole Devenny
University of Central Florida

Find similar works at: <https://stars.library.ucf.edu/etd>

University of Central Florida Libraries <http://library.ucf.edu>

 Part of the [Public Affairs Commons](#)

STARS Citation

Devenny, Joah Nicole, "Critical Digital Infrastructure Protection: An Investigatoin Into The Intergovernmental Activities Of Information Technology Directors In Florida Counties" (2004). *Electronic Theses and Dissertations*. 86.
<https://stars.library.ucf.edu/etd/86>

This Doctoral Dissertation (Open Access) is brought to you for free and open access by STARS. It has been accepted for inclusion in Electronic Theses and Dissertations by an authorized administrator of STARS. For more information, please contact lee.dotson@ucf.edu.

CRITICAL DIGITAL INFRASTRUCTURE PROTECTION:
AN INVESTIGATOIN INTO
THE INTERGOVERNMENTAL ACTIVITIES
OF INFORMATION TECHNOLOGY DIRECTORS
IN FLORIDA COUNTIES

by

JOAH NICOLE DEVENNY
B.A. University of Central Florida, 1993
M.A. University of Central Florida, 1999

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in the Public Affairs Doctoral Program
in the College of Health & Public Affairs
at the University of Central Florida
Orlando, Florida

Spring Term
2004

Major Professor: Eileen Abel

© 2004 Joah Nicole Devenny

ABSTRACT

As cyber attacks become more sophisticated, the risk to all networked computer systems increases. Whether public or private, whether federal, state, or local, the threat is equally real. Consequently, local governments must respond accordingly to understand the threats, take measures to protect themselves, and determine how to respond in the event of a system breach. Additionally, since cyber criminals do not respect geographic or administrative boundaries, local leaders must be prepared to instantly interact with other governments, agencies, and departments to suppress an attack.

Guided by the theory of intergovernmental management (IGM), this exploratory research investigated how Information Technology (IT) Directors in Florida county constitutional offices use intergovernmental relations and management activities as part of their information security efforts. Specifically, this research sought to determine: 1) which IGM activities do county IT Directors most often perform; 2) do county IT Directors make more use of vertical or horizontal IGM relationships; 3) is there a relationship between office/county demographics and the IGM activities its IT Directors most often perform?

To answer these questions, an electronic survey was distributed to 209 directors, of which 125 responded. Overwhelmingly, the findings indicate that these Directors rarely engage in IGM activities regardless of the purpose or type of government/department contacted. However, when seeking intergovernmental assistance, it is most often horizontally with other Departments within their own

government and least often vertically with Federal offices. The most frequently performed intergovernmental activity is seeking technical assistance, however seeking program/project information is also performed more frequently than the other activities explored in this research. The least frequently performed activities involved seeking to modify established IT partnerships. Further, there was evidence of relationships between certain office/county demographics and IGM activity. The discovery of these patterns and relationships can be used to aid policy and program development, as well as to stimulate deeper inquiry into the intergovernmental dimensions involved in protecting local elements of the U.S. Critical Digital Infrastructure.

For their constant encouragement, support, and understanding,
I dedicate this work to my parents, John and Sue Devenny.

Thank you.

ACKNOWLEDGEMENTS

There are several individuals I would like to thank for their contributions to this research. First and foremost, I extend my most sincerely gratitude to Eileen Abel, the Chair of my committee. From the earliest stages of this work to the final revisions, from late-night phone calls to weekend emails, she consistently provided sound advice, constructive analysis, motivating encouragement, and most enjoyably, she shared her good nature. This research, and my doctoral experience, would not be not have been the same without her.

I would also like to thank my committee members, Stephen Holmes, Ronnie Korosec, and Mary Van Hook for their diligence and commitment to this project. Because of their valuable feedback, this work is stronger. Special thanks go to Margaret Mlachak, Pam Kirby, and Larry Cochran for their support and friendship throughout my doctoral studies.

Next, I wish to thank the respondents who took part in this research. Because of their voluntary participation, we now have a better understanding of the role intergovernmental activities and relationships play in county-level information security in the State of Florida. Finally, I am beholden to the many authors cited throughout this work.

In closing, I wish to note that the opinions, observations, and conclusions presented in this work are mine alone. They do not represent the views of the University of Central Florida, the Public Affairs Doctoral Program, or any other member of the university community.

TABLE OF CONTENTS

LIST OF TABLES.....	x
LIST OF FIGURES.....	xv
I. INTRODUCTION.....	1
II. LITERATURE REVIEW.....	9
The Internet: A Network of Networks.....	9
Borderless and Connected.....	16
The Critical Digital Infrastructure.....	18
Breadth of Criminal Cyber Activity.....	24
Exploiting Vulnerabilities.....	28
Threats and Attacks.....	32
Government and the CDI.....	38
Local Government.....	42
County Government.....	44
Information Security: More than Technology.....	49
III. THEORY OF INTERGOVERNMENTAL MANAGEMENT.....	57
Intergovernmental Relations.....	57
Intergovernmental Management.....	65
Problem Solving.....	69
Networking.....	72
Coping Capabilities.....	75
Vertical and Horizontal Environments.....	79

	Application of Theoretical Ideas.....	83
IV.	METHODOLOGY AND DATA COLLECTION	92
	Observation Unit and Study Population.....	92
	Variable Operationalization	95
	Research Instrument	100
	Data Collection and Response Rate.....	101
	Independent Variable Coding	104
	Dependent Variable Coding	112
	Non-parametric Tests	116
V.	ANALYSIS AND FINDINGS	119
	General Analysis	119
	Question 1: Prevalence of IGM Activity	133
	Question 2: Vertical vs. Horizontal Relationships	136
	Question 3: Demographics and IGM Activity	138
	Office Supervised	139
	Contact with Federal Offices.....	140
	Contact with Another Government in the County.....	145
	Seeking Funding or Resources.....	147
	Overall Relationship Importance.....	149
	Percent Duties Focuses on IT Related Issues	151
	Population with Bachelors Degree or Higher	152
	Adequacy of Funding.....	156
	Non-significant Demographic Variables	156

Summary	162
VI. IMPLICATIONS	167
Theoretical Implications	167
Practical Implications	171
Limitations	176
Future Research	178
Concluding Remarks	180
APPENDIX A: INTRODUCTORY LETTER	183
APPENDIX B: EMAIL	186
APPENDIX C: SURVEY INSTRUMENT	188
APPENDIX D: FIRST FOLLOW-UP EMAIL	197
APPENDIX E: SECOND FOLLOW-UP EMAIL	199
APPENDIX F: UCF INSTITUTIONAL REVIEW BOARD APPROVAL	201
LIST OF REFERENCES	204

LIST OF TABLES

Table 1: Sampling Frame Development.....	95
Table 2: Frequency for Independent Variable: Which zone is the County in	105
Table 3: Frequency for Independent Variable: “OFFICENU” (Number of Offices Supervised).....	105
Table 4: Frequency for Independent Variable: “OFFICE” -Which Office do you Supervise	106
Table 5: Frequencies for Dichotomous Independent Variables for Type of Office Supervised (N’s = 125).....	106
Table 6: Independent Variables Recoded as Ordinal from the U.S. Census and State of Florida	107
Table 7: Percent of Duties Focused on IT Related Tasks	108
Table 8: Number of Employees Supervised (N=124).....	108
Table 9: Questions Used to Create the Independent Index Variable “Adequacy of Budget”.....	110
Table 10: Independent Index Variable for “Budget Adequacy” Recoded as Ordinal ..	110
Table 11: Question Regarding Online Services	111
Table 12: Independent Variables	112

Table 13: Dependent and Index Variables	113
Table 14: Total Percent of Respondents who Contact Each Type of Government only “ A Few Times a Year” or “Never” Regardless of the Activity	120
Table 15: Perceived Overall Relationship Development with Each Contact by Percents	121
Table 16: Perceived Importance of Each Contact to Overall IT Success	122
Table 17: Percent of Respondent who Engage in Each Activity “ A Few Times a Year or Less” Regardless of the Intergovernmental or Interorganizational Contact.....	123
Table 18: Percent of Duties Focused on IT Related Tasks	124
Table 19: Zone by Percent of Duties Focused on IT Related Tasks	124
Table 20: Zone by Number of Offices Supervised.....	125
Table 21: Number of Employees Supervised by Percent of Duties Focused on IT Related Tasks	126
Table 22: Number of Employees Supervised by Zone	126
Table 23: Zone by the Independent Variable “Intergovernmental Revenue	127
Table 24: Zone by the Index variable “Adequacy of Budget”	128
Table 25: Core IT Needs by Percent of Respondent who Indicated that Funding was Inadequate	130
Table 26: Number of Employees Supervised by Type of Office	131

Table 27: Percent of IT Directors who Supervise Two or more Office by Type of Office Supervised	131
Table 28: Percent of IT Director’s Duties Focused on IT Related Issues by Type of Office Supervised	132
Table 29: The Nine Activities with Modes of ‘A Few Times a Year or Less’ rather than ‘Never’	134
Table 30: Five Most Frequent Activities by Percent of Respondents who Perform the Activity Several Times a Year or More	135
Table 31: Five Least Frequent Activities by Percent of Respondents who Never Perform the Activity	136
Table 32: Most Frequent Partner for Each Activity	137
Table 33: Least Frequent Partner for Each Activity	137
Table 34: Kruskal-Wallis Tests Significant at $p \leq .01$ for the Independent Variable “Office Supervised” & the Composite Dependent Variables	139
Table 35: Mann-Whitney Tests for Significant Dependent Index “Frequency of Contact with Federal Offices” by Independent Dichotomous Variables for Type of Office Supervised	140
Table 36: Mann-Whitney Tests for Dichotomous “Board of Commissioners” by Index Factors of “Frequency of Contact w/ Federal Offices”	142
Table 37: Mann-Whitney Tests for Dichotomous “Sheriff’s Office” by Index Factors of “Frequency of Contact w/ Federal Offices”	143

Table 38: Mann-Whitney Tests for Dichotomous “Tax Collector” by Index Factors of “Frequency of Contact w/ FEDERAL Offices” 144

Table 39: Mann-Whitney Tests for Significant Dependent Index “Frequency of Contact with another Government located within the Jurisdiction of Your County” by Independent Dichotomous Variables for Type of Office Supervised 145

Table 40: Mann-Whitney Tests for Dichotomous “Board of Commissioners” by Index Factors of “Frequency of Contact w/ another Government in Your County Jurisdiction” 146

Table 41: Mann-Whitney Tests for Significant Dependent Index “Frequency of Seeking Funding or Resources” by Independent Dichotomous Variables for Type of Office Supervised 148

Table 42: Mann-Whitney Tests for Dichotomous “Board of Commissioners” by Index Factors of “Frequency of Seeking Funding or Resources” 148

Table 43: Mann-Whitney Tests for Significant Dependent Index “Overall Relationship Importance” by Independent Dichotomous Variables for Type of Office Supervised 150

Table 44: Mann-Whitney Tests for Dichotomous “Board of Commissioners” by Index Factors of “Overall Relationship Importance” 150

Table 45: Mann-Whitney Tests for Index “Frequency of Contact w/ State Offices” by Dichotomous Variables of “Percent of County Population, age 25+, which Hold Bachelor’s Degrees or Higher” 153

Table 46: Mann-Whitney Tests for Dichotomous Variable “23% or More of Population Hold Bachelor’s Degrees or Higher” by Index Factors of “Frequency of Contact w/ State Offices”	155
Table 47: Mann-Whitney Test for the Independent Variable “Supervise Only One Office”	157
Table 48: Kruskal-Wallis Tests for “Number of Employees Supervised”	158
Table 49: Kruskal-Wallis Tests for “Number of Office Supervised”	159
Table 50: Kruskal-Wallis Tests for “County Intergovernmental Revenue”	160
Table 51: Kruskal-Wallis Tests for “ Zone”	161

LIST OF FIGURES

Figure 1: Florida Counties with No Representation in this Study	103
Figure 2: Florida Counties by U.S. MARS Zones	104
Figure 3: Frequencies of Index “Contact with Federal Offices” by Dichotomous “Board of Commissioners”, “Sheriff”, and “Tax Collector” Variables	141
Figure 4: Frequencies of Significant Indicator Variables for “Frequency of Contact with Federal Offices” by “Board of Commissioners Versus All Others”	142
Figure 5: Frequencies of Significant Indicator Variables for “Frequency of Contact with Federal Offices” by “Sheriff’s Office Versus All Others”	144
Figure 6: Frequency of Index of “Frequency of Contact w/ another Government in Your County Jurisdiction” by Dichotomous “Board of Commissioners”	146
Figure 7: Indicator Variables for “Frequency of Contact w/ another Government Located within the Jurisdiction of Your County” by “Board of Commissioners” versus All Others	147
Figure 8: Significant Indicator Variables for “Frequency of Seeking Resources or Funding” by “Board of Commissioners Versus All Others”	149
Figure 9: Significant Indicator Variables for Dependent Index “Overall Relationship Importance” by “Board of Commissioners Versus All Others”	151

Figure 10: Frequencies of Index “Frequency of Contact w/ State Offices” by Percent of County Population, age 25+, which Hold Bachelor’s Degrees or Higher” 154

Figure 11: Significant Factors from “Frequency of Contact w/ STATE Offices” 155

I. INTRODUCTION

The aim of this research was to explore the roles intergovernmental management, activities, and communication play in protecting the information systems of our critical infrastructure. As cyber attacks become more sophisticated, the risk to ALL computer systems increases (White House, 2003; Computer Science & Telecommunications Board, and National Research Council, 2002; Information Assurance Advisory Council, 2001; McCarthy, 1998). Whether public or private, whether federal, state, or local, the threat is equally real (Misra, 2003). Consequently, local leaders must respond accordingly to understand the threats, take measures to protect themselves, and determine how they will respond in the event an attack occurs. As such, the focus of this research was to investigate how county-level Information Technology Directors and their staff use intergovernmental relations and management activities in securing critical information systems under their charge.

From maintaining medical records to tax filing, computers and the Internet have come to play a role in most every sphere of modern life (Careless, 2003; Nye, 2003; Long, 2000; Libicki, 1995). As such, it should not come as a surprise that a well-coordinated large-scale cyber attack has the potential to disrupt daily life in America and across the global (White House, 2003; Walker, 2002; Noonan, 2001; Brock, 2000a, 2000b). Given that our social, health, economic, justice, and military systems increasingly depend on networked information systems, any person or group, public or private, regardless of Internet access, would be affected if critical computer systems

were rendered inoperable (Freund, 2003; Hansell, 2003; Reames, 2000; Stanton, 2000; Everett et. al., 1997). In a post-9/11 report to Congress, the Gilmore Commission (2001) clearly made this point when it wrote,

Our banking and finance systems, our just-in-time delivery system for goods, our hospitals, our state and local emergency services... all of these critical services rely upon their information connections and databases... each is critical to the American economy and health of our citizens... and each can be shut down or severely handicapped by a cyber attack (p. 53).

Amid increased global terrorist activity, a growing body of research and intelligence information suggests that the probability of terrorist–orchestrated cyber attacks on U.S. critical information systems is extremely high (Computer Science & Telecommunications Board and National Research Council, 2002; Deibert, 2002; Kremmen, 2002; Verton, 2002; Berkowitz 2001; McWilliams, 2001). Yet, the ability and authority to prevent such a threat surpasses any lone industry or level of government. In testimony before the U.S. House of Representatives Select Committee on Homeland Security the U.S. Comptroller General stated the indisputable need to “...clarify the appropriate roles and responsibilities of federal, state, and local entities and build a framework for partnerships for coordination, communication, and collaboration” (Walker, 2002, p. 4). Per 2001 Executive Order 13231 section 5(a), the President’s Critical Infrastructure Protection Board (CIPB) is charged to work with state and local governments “...to ensure that systems are created and well managed to share threat warning, analysis, and recovery information among government network operation centers...”. Yet three years later, the information security of local and county governments remains a major concern among security experts (Misra, 2003; Barrett,

Greene, & Mariani, 2002; Public Technology Inc., 2002). Adding to this concern is the reality that local governments, such as counties, serve as first responders to crisis (National Association of Counties, 2001A, 2001D; U.S. General Accounting Office, 2001c). As such, county communications and computer systems were rendered inoperable by a cyber attack during a simultaneous physical crisis, the ability for officials to coordinate relief efforts would be severely effected.

In 1999, the Emergency Response and Research Institute conducted a non-scientific survey of local/county/state administrators, supervisor, technology professionals, and first-line responders which revealed that 85 percent believed more research into computer attacks on local government offices needs be conducted (Staten, 1999). Further, 85 percent believed hacking local, county, or state government systems will become more of a problem in the future. Indeed, in the years since this survey local governments, specifically counties, have been increasingly plagued by Internet worms, viruses, and denial of service attacks. Mary Reynolds, Chief Technology Officer for Illinois, states that cyber attacks occur "all the time", noting that some government systems are attacked hundreds of times each month (Perlman, 2002b). She speculates that the majority of local governments remain unsuccessful at fending off attacks and intrusions because they fail to patch software, properly configure firewalls, use intrusion-detection systems, or scan their networks.

Despite the recent efforts of local officials to improve these practices (Barrett, Greene, & Mariani, 2002; Monroe, 2002; Posner, 2002; Gonzales, 2001), poor information security remains rampant in county governments (Kouns, 2003; O'Connell, 2003; Brock, 2000; Dacey, 2001; PDD-63, 1998; Smith, 1998; Crescenzi, 1996). This

reality was made publicly obvious during the summer of 2003 when a series of viruses and worms penetrated county computer systems across the nation. For instance, nearly the entire computer system for the Hillsborough County Florida school system (approximately 10,000 computers) was shut down for several days late August due to a virus (ABC Action News, 2003). In Christian County Kentucky, poor information security forced the shut down of computers at the clerk's office and health department for several days after falling victim to a computer worm known as "Nachi" or "Welchia" (Leazer, 2003). This shut down completely halted numerous services, including motor vehicles registration, voters registration, food stamp benefits, child support, Medicaid, and payroll. Again in August 2003, poor county-level information security proved equally damaging in Maryland where citizens were temporarily unable to renew drivers licenses or register motor vehicles at 23 centers throughout the state (WBAL-TV, 2003). The cause was cited as the "lovsan" or "MSBlaster" worm that exploited a Microsoft vulnerability for which a software patch had been released a month prior as part of a large public campaign to limit potential damage. The MSBlaster worm also forced ill-prepared officials in Riverside County California to shut down county web sites and Internet services while they patched security holes throughout the county's vast network of 12,000 personal computers. For nearly 48 hours, Riverside County employees were unable to access email, the database of court cases was no longer assessable online, and jurors could not check their status online.

Further demonstrating the severe damage and disruption cyber attacks cause county governments, consider the stealthy computer worm "NIMDA" which virtually froze Fairfax County Virginia in the summer of 2001 (Perlman, 2002b; Gilmore

Commission, 2001). For a nearly a week, county officials had to lock network access to the outside world to allow nearly 150 IT technicians to "scrub" the entire network of 9,000 PCs and 300 servers to remove the virus and repair the system. The severity of the worm forced the county to shut down its web site which receives more than a million hits a day as residents log on for a variety of services, from paying fines and purchasing permits, to renewing library books. Making matters worse, county IT professionals believed they had eradicated the virulent worm only to have it resurface and re-infect the system. In an unrelated series of events during March 2002, an unauthorized private information security analyst informed Harris County Texas that its wireless network was completely open leaving sensitive information vulnerable to illicit access (Juhnke, 2002). The independent analyst demonstrated for county officials how easily the system could be tapped using a basic laptop and an inexpensive wireless card. The demonstration prompted the county to disable its entire wireless network (Dornan, 2002).

Numerous aspects of local government depend on communication between citizens and officials. The Internet and network-enabled computer systems have made that process much more efficient (Bowser, 1998). As cyber criminals become more sophisticated, the risk of an attack targeting or at the very least compromising local systems increases (Misra, 2003). As noted earlier, local leaders must respond accordingly to understand the threats and take measures to protect themselves from an attack. A 2002 survey by the National League of Cities reported that cyber attacks are among the top three terrorist related concerns of city governments. In an effort to tend to these concerns, *all* survey respondents indicated that their city had increased intergovernmental cooperation with other cities, counties, state, and federal bodies

since 9/11. Yet the study found that only 43 percent of large cities and 26 percent of all cities have developed strategies to specifically address cyber-terrorism. Speculating on these findings, the National League of Cities noted that federal agencies still provide relatively little direct guidance and training regarding cyber terrorism compared to biological and chemical threats. These disparities suggests that protecting localities from cyber attacks needs more attention at all levels of government.

Despite efforts, this researcher was unable to locate any similar studies focusing on county government. American City & County Magazine (2002) also addressed this research lacuna noting that there is very little available data on county information security efforts. However, without an understanding of county leadership and the pervasiveness of vertical and horizontal communication with regard to information security, our national security remains vulnerable. In a response to this need for understanding and given the importance of critical digital infrastructure protection, this research sought to observe the reality of information technology security as it occurs in the trenches; county government. Again, the focus of this research was to investigate how county-level Information Technology Directors and their staff use intergovernmental relations and management activities in securing critical information systems under their charge.

Due to the breath of issues stemming from safeguarding information technology, information security research is not married to any discipline, let alone one theory. However, in an effort to increase the practical utility and efficacy of this research, this study was guided by the public administration theory of intergovernmental management (henceforth, IGM). This theory was selected because at its core, it focuses on the

degree to which "...officials strategically interact with various actors for the purpose of successfully designing and administering policies" (Agranoff & Lindsay, 1983, p. 5). The concepts, classification schemes, and propositions put forth by this theory were drawn upon to shape definitions, operationalize concepts, and aid in linking variables through the use of its established taxonomies.

Because the of role intergovernmental activities in county level information security had yet to be studied, this investigation was exploratory. As such, this research did not expressly set out to test hypotheses or establish causal relationships. Instead, theory was used to guide research questions in an effort to discover and explain patterns of activity (Chafetz, 1978). To that end, this research sought to answer the questions: 1) which IGM activities do county IT Directors/staff most often engage in on behalf of information security and critical digital infrastructure protection; 2) do county IT Directors/staff make more use of vertical or horizontal IGM relationships on behalf of information security and critical digital infrastructure protection; 3) is there a relationship between office/county demographics and the IGM activities its IT Directors/staff most often engage in on behalf of information security and critical digital infrastructure protection? By uncovering patterns of similarities and differences in the type and use of IGM activities, these preliminary finding can be used to stimulate deeper inquiry and generate dialogue into the intergovernmental and administrative dimensions involved in protecting the U.S. critical digital infrastructure.

While disciplines such as criminal justice, legal studies, and computer science have been actively involved in information security research; the results are often fragmented and discipline-specific. Further, little attention and even less research has

been given to roles intergovernmental relations, communications, and management play in information security. This research, however, recognizes that critical digital infrastructure protection is a complex social, economic, and administrative issue that affects the health, welfare, and security of the citizens in all communities. As such, a unique aspect of this research is that it approaches what is seemingly a technological concern as a public affairs issue where understanding and solutions require an interdisciplinary approach.

Again, the aim of this research was to explore the roles intergovernmental management and interorganizational communication in protecting county information systems. To this end, the literature of this study begins by discussing network and information technology and the connections and interdependencies they create. Next, the nature of the U.S. critical digital infrastructure is explained, including why it is vulnerable and to what. Focus then turns to general government use of network systems with specific emphasis on local and county governments. After discussing the inadequate state of these systems, information security and the critical role of management is highlighted.

Following the literature review, the theory of intergovernmental management is explicated. Then a discussion clarifies the intrinsic and critical relationship between information security and intergovernmental management activities. Following is an explanation of the methodology used, the analysis, and a presentation of findings. Finally a discussion of the implications for the public affairs arena complete this research endeavor.

II. LITERATURE REVIEW

The Internet: A Network of Networks

The 2003 National Strategy to Secure Cyberspace released by the White House declared the Internet "...the nervous system of our country" (p. 6). Yet few comprehend how it works or its inherent vulnerabilities. In order to understand these matters, it is first important to have a basic understanding of computer networking. To begin with, a computer, or single system, is usually controlled by a single owner and is located in a known physical location. With the addition of specific software and hardware to provide communication protocols and physical channels, several single systems can be connected to create a network of systems. Individual systems can be added or removed from a network at any time, making it dynamic in structure and operations. The size of a network can range from two systems to thousands of systems and these different systems can be housed in different physical locations, manufactured by different vendors, and even owned by different organizations (Committee on the Internet in the Evolving Information Infrastructure, 2001; U.S. Department of Commerce, 1998).

When a network remains private, as a "closed system of systems", it is called an intranet (Phoha, 2002; Sunshine, 1999). Intranets are most often used to share information between employees as part of day-to-day business operations. This type of network is the most secure as it does not directly connect to the Internet. A variation of

this is an extranet, which occurs when a private network connects to the larger Internet to provide public access to a limited amount of content which is sectioned off from the rest of the main intranet (Jordan, 1997). There are few physical limitations to the scope and breadth of either category of network as they can traverse organizational and national boundaries if resources are available. However, it is the joining of extranets and public networks into a “network of networks” which serves as the foundation of the Internet (Miller & Gregory, 2002).

Linking computers from distant locations to share information was only brought to fruition in the early 1960s (Everett, Dewindt, & McDade, 1997). The RAND proposal, written by Paul Baran in 1964, outlined principles of a non-local network designed to be robust and flexible (Mayr, 1995). The original impetus for this project was to preserve the integrity of the military command and control network under warlike conditions, even a nuclear attack. This new network would have no central authority, all the ‘nodes’ would be equal in status, and each node could send and receive messages. In principle, if one node was destroyed, the rest of the nodes would still be able to communicate.

The Defense Advanced Research Projects Agency (DARPA) funded the first test of the concept in 1969 and the first nodes were installed at UCLA, Stanford, University of California at Santa Barbara, and University of Utah at Salt Lake City (Lipson, 2002; Sewell, 2002). The network was fundamentally simple, consisting of scientists at these remote locations passing findings and research notes back and forth. ARPAnet, as it was initially known, was successful and rapidly adopted. By the end of the first year, it was increasingly being used like a data mailbox and in the years to follow its uses continued to evolve and expand. In 1983, the military and nonmilitary elements were

split apart and the nonmilitary section grew into what is now called the Internet (Sunshine, 1999; Everett, Dewindt, & McDade, 1997).

The Internet is a collection of thousands of networks linked by a common set of technical protocols which make it possible for users on any one of the networks to communicate with, or use specified services of any of the other networks (Committee on the Internet in the Evolving Information Infrastructure, 2001; Fraser, 1997). To operate, the Internet requires several layers of technology, some of which are obvious and physical; while others are logical and operational. As such, the Internet is the sum of all of the information and communication technologies that support its sundry protocols. This includes such elements as computers, peripheral components, telephone lines, fiber optic cables, satellites, hosts, users, Internet Providers, data standards, applications, protocols, routers, code, servers, hubs, and of course, the information content contained therein.

Information sent across the Internet from one computer to another is broken into small packets of data that contain information regarding the origin/destination of the data, as well as a portion of the total data (ISC2.com, 2003; Zakon, 2003; Phoha, 2002; Smart Computing, 2001). These packets travel separately through telecommunication channels which connect the Internet and then are reassembled at the destination or receiving computer. There are two primary protocols, referred to collectively as TCP/IP, that enable these data packets to traverse the complex networks and arrive in an understandable format (Lipson, 2002; Miller & Gregory, 2002). First, Transmission Control Protocol (TCP) decomposes the data into packets. Next, Internet Protocol (IP) guides or routes the data packets across the Internet. Upon arriving at the final

destination, TCP ensures that all of the necessary packets are properly reassembled. However, TCP and IP are but two of the many protocols that govern the network transfer of digital information (Collins, 2001; Fraser, 1997; Ruthfield, 1995). Others include File Transfer Protocol (FTP), Post Office Protocol (POP3), Simple Mail Transfer Protocol (SMTP), Wireless Application Protocol (WAP), to mention a few. Yet it was the 1990 development of an experimental protocol known as Hyper Text Transfer Protocol (HTTP) that transformed the Internet into the social and economic backbone of modernized nations in less than a decade (Roos, 1998).

HTTP works by the use of web enabled pages (i.e. files written in Hyper Text Markup Language or HTML), web servers (which “serve up” or deliver the web enabled pages), and web browsers (which present the “served pages” to the end user) (Zakon, 2003; Phoha, 2002). The key to the World Wide Web is “hyperlinks” which are embedded in web enabled documents. The advent of hyperlinks provided a new way of conceptualizing and organizing information and enabled users to exchange documents regardless of the protocol they were using (Bowser, 1998). Webpages accessed using a web browser or client, such as Netscape Navigator or Internet Explorer, proved an easier way to navigate the Internet than older protocols such as gopher and FTP (U.S. Department of Commerce, 1998). Both computer programmers and the public quickly embraced the combination of user-friendly web browsers and the easy to learn coding language HTML. In 1992, the World Wide Web was comprised of only 50 web servers, by 2003, just a decade later, there were over 35.5 million (Smart Computing, 2001).

The Internet and World Wide Web continue to grow and recent numbers estimate that globally 500 million people go online in a given month (CyberAtlas.com, 2003;

Digital Divide Network 2003; Nielsen NetRatings, 2002). While this is a staggering number, it actually represents less than 10 percent of the world's entire population. Yet of those half-billion users, 41 percent are located in the United States and Canada. Perhaps this is not entirely surprising considering that the United States operates more computers than the rest of the world combined (Digital Divide Network, 2003). A national telephone survey conducted by Pew Internet and the American Life Project (2003) found that U.S. Internet penetration rates have remained around 60 percent since late 2001. Of this population, 49 percent use the Internet at least once a day either from home, work, or both. This means that on an average day, about 61 million Americans go online to do such things as send email, read the news, and make purchases. With so many users, there is much potential for irresponsible use, abuse, and exploitation (Doddrell, 1996).

To demonstrate the global presence and dominance of the U.S. Internet infrastructure, consider some of the following numbers. According to the Organization for Economic Cooperation and Development (henceforth, OECD) (2002a), the relative development of a country's Internet infrastructure can be measured by the number of its Internet hosts per 1,000 inhabitants¹. In late 2000, the United States far outpaced any other OECD country² by maintaining more than 234 hosts per 1,000 inhabitants (OECD,

¹ A host is a domain name that has an IP (Internet Protocol) address associated with it. In an internet-network environment, a host is any computer with full two-way access to other computers on the Internet, or a computer that runs a web server for one or more web sites (Phoha, 2003; Sans.org; 2003). Since some systems can not be detected because of the use of firewalls, an estimate of hosts should be thought of as an indicator of the minimum size of the public Internet (OECD, 2002a).

² The 30 member countries in the Organization for Economic Cooperation and Development (OECD) are Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece,

2002a). The average for the European Union was only 37.4 hosts per 1,000 inhabitants. Additionally, of the 90 million Internet hosts registered to OECD countries in 2000, a full 70 percent were registered to the United States. The second largest concentration of registered hosts was in Japan, which maintained only 4.6 percent of the OECD total, followed by the United Kingdom with 3.5.

While the number of Internet hosts gives an indication of the size of a country's Internet infrastructure, the number of active web sites provides information on a country's relative development of Internet content. Again, the United States leads web site hosting with 12.6 million sites hosted as of July 2000 (OECD, 2002a). This figure translates into 46.5 web sites per 1,000 U.S. inhabitants. Germany and the United Kingdom were the only other OECD countries hosting more than one million sites, with 1.8 million and 1.4 million hosted sites respectively. Collectively the European Union only maintains 12.7 web sites per 1,000 inhabitants.

Another measure of the depth of a nations' information and communication infrastructure is the use of the Internet as a transaction channel for electronic commerce (henceforth, e-commerce). While e-commerce has revolutionized economic activity, it has taken off more slowly than predicted (Council for Excellence in Government, 2002; Denby, 2000; Reames, 2000; Sager et al, 2000; Litt, 1997). Despite the turbulence resulting from collapsed "dot.coms" in the late 1990s, the U.S. Department of Commerce (2003) reported that domestic Internet retail trade (the general focus of e-commerce attention) grew rapidly both in volume and share of total U.S. retail trade

Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States (OECD, 2003).

from 1999 to 2001. Its share increased from 0.7 percent in the fourth quarter of 1999 to 1.3 percent in the fourth quarter 2001. During 2001, approximately 38 percent of U.S. Internet users ordered products online (OECD, 2002b) which translated into \$35 billion in sales (U.S. Department of Commerce, 2003)³. In terms of both dollar value and share of economic activity, e-commerce varies markedly among key U.S. economic sectors. For example, manufacturing leads all industry sectors with e-commerce shipments that account for 18 percent (\$725 billion) of total manufacturing shipments. Merchant wholesalers rank second with e-commerce sales that represent 10 percent (\$270 billion) of their total sales. Forrester Research (Global Reach, 2001) predicted that by 2004, global e-commerce would reach \$6.8 trillion and that 47 percent of that could be attributed to the U.S.

Much of the success of e-commerce depends on the security of cyber transactions. Yet the more the Internet is used to transfer funds, the more likely data transmissions and the underlying infrastructure itself will become targets (Moteff, 2002; Rathmell, 2000; Reames, 2000). Both industry and government appear aware of this growing threat as the number of secure servers in OECD countries increased by 223 percent from July 1999 to January 2002 (OECD, 2002b). However, a full 65 percent of all OECD secure servers are located in the United States. To put that number in perspective, the United Kingdom boasts the second largest concentration of secure servers with only six percent of the total. This disparity is quite alarming as the Internet

³ The total value of on-line retail sales should be considered as a lower bound, as certain categories that are included in other surveys, such as on-line travel services, financial brokers and dealers and ticket sales agencies, are excluded.

is borderless and the vulnerabilities of one system can adversely affect the security of all others to which it is connected (Moore, 1997). As such, no one nation or government can alone secure cyberspace (White House, 2003; Institute for Information Infrastructure Protection, 2003; Frank, 2002; Hecker, 2002; Sewell, 2002; Tritak, 2001b; Rathmell, 2000).

Borderless and Connected

Cyberspace, a term coined by William Gibson in his 1984 sci-fi novel *Neuromancer*, is a metaphor to describe the non-physical terrain created by networked computer systems (Zakon, 2003). In the topography of cyberspace, national boundaries have little meaning (Institute for Information Infrastructure Protection, 2003; Tyrrell, 2002). Supported by information and communication technologies, the Internet seamlessly links nations across the globe (Held et al, 1999). Yet as Everett, Dewindt, and McDade (1997) ominously point out, “History has given evidence to the fact that when some new technology brings mankind brightness, a shadow is cast simultaneously”. The Internet has proven no exception. For while it is highly efficient; it is alarmingly vulnerable. Recent history has proved that a well-executed cyber attack can breach computer systems globally in a matter of hours, in some cases minutes, with no regard for organizational or sovereign borders (White House, 2003; Freund, 2003; Lipson, 2002; Tritak, 2001b; Vatis, 2001; U.S. General Accounting Office, 2001c; Transition Office of the President’s Commission on Critical Infrastructure Protection &

the Critical Infrastructure Assurance Office, 1998; Litt, 1997). As such, by using the Internet, a malicious actor can compromise literally millions of systems, thousands of miles away, at very little cost.

Case in point, in January 2003, the SQL Slammer worm (also known as “Sapphire”) exploited a known Microsoft vulnerability for which a repair patch had been available for six months prior to the attack (Fisher, 2003a; Associated Press, 2003). Due to widespread neglect for installing the patch in such countries as South Korea, the worm caused considerable damage internationally via cascading network outages, canceled airline flights, and automated teller machine failures. The worm infected more than 90 percent of vulnerable computers worldwide within 10 minutes of its release on the Internet. The U.S. General Accounting Office (Dacey, 2003a) reported that the worm doubled in size every 8.5 seconds and achieved its full scanning rate (55 million files scanned per second) after about 3 minutes, making it the fastest computer worm to date.

The ease with which this worm spread was directly due to the rampant presence of vulnerable systems within larger networks, demonstrating the adage “security is only as strong as its weakest link” (U.S. Department of Commerce, 1999, p. 4). Doddrell (1996) expands on this adage by offering a likely scenario whereby a government office, for instance, within a larger network implements security measures such as a firewall, while another office within the same network simply connects to the Internet with no protection. A hacker could theoretically enter the network via the insecure office and navigate to the more secure office rendering the best efforts ineffective. This plausible situation leaves governments in a precarious position; each one can do only so much to

secure its own presence in cyberspace as the connectedness of the Internet presents vulnerabilities that cannot always be controlled, let alone foreseen.

In the wake of the attacks of 9/11, there has been a greater awareness of importance of network security, not only for each individual organization, but also for the vitality of the nation as a whole. As Charles McQueary, Undersecretary for Science and Technology at the Department of Homeland Security pointed out, "September 11 didn't make us more vulnerable, but made us more aware of our vulnerabilities" (Amarelo, 2003). However, the United States' increasing dependency on the Internet and information technologies to manage and operate its critical infrastructures provides terrorists with a tactical target (Vatis, 2001).

The Critical Digital Infrastructure

The US Critical Infrastructure (henceforth CI) consists of public and private physical and cyber assets that are considered vital to society, commerce, and national security (White House, 2003; Isenberg, 2002; Allor & Lindley, 2000; Dearth, 2000; Tyrrell, 2000). The President's Commission on Critical Infrastructure Protection (PCCIP, 1997) declared that the critical infrastructure constitutes the life support system of the United States and Presidential Decision Directive 63 (PDD-63, 1998) referred to it as the structural foundation of a society. A well-executed physical and/or virtual attack on major infrastructure elements could affect millions of people, both domestically and abroad.

Specifically, the U.S. Critical Infrastructure consists of eight sectors, namely, information and communications; electrical power systems; gas and oil transportation and storage; banking and finance; transportation; water supply systems; emergency services; and government services (Moteff, 2002; Tritak, 2001a; PDD63, 1998). While identified as separate sectors, they are highly interdependent. For example, the banking and finance sector relies on the telecommunications and computer sector, which in turn relies on electrical power systems, which are dependent on oil & gas transportation and so on. In an interview with *The New Atlantis* (2003), a journal for technology and society, former vice chairman of the White House's Critical Infrastructure Protection Board, Howard Schmidt discussed the complex interrelationship between the information and communication sector and seemingly disparate elements of the national CI. He gave the following scenario to illustrate the critical linkages,

For example, if a computer system is down for the national rail system, you could still physically move trains, but you wouldn't want to, because you won't know where perishable items are supposed to be delivered. Or perhaps chemicals that need to be moved to help water treatment plants won't get there—so within a matter of time, water treatment facilities would be having problems. The underpinning of all these critical infrastructures are computers that must be protected (The New Atlantis, 2003).

Increasingly, each sector is reliant upon networked computers, the Internet, and the larger information and communication infrastructure to provide CI services (White House, 2003; Institute for Information Infrastructure Protection, 2003; Lipson, 2002; Moteff, 2002; Executive Order 13231; Death, 2000; Long, 2000; Tyrrell, 2000). As a result, the Department of Justice (1998) recognized the Internet as the single most important critical infrastructure element today. The information and communication

sector, also referred to as the critical digital infrastructure (henceforth, CDI) consists of and connects many different elements, systems, and networks, which are owned by an array of governmental, private, and commercial entities. These networked elements play an instrumental role in the day-to-day operations of both public and private organizations with regard to such tasks as managing payroll; tracking inventory and sales; as well as research and development activities (Executive Order 13231; Dacey, 2001). Yet, our reliance on information technology is far more profound than just the use of spreadsheets or network-enabled communications like telephones, fax, and e-mail (U.S. Department of Commerce, 2003; Critical Infrastructure Assurance Office, 2002; Lipson, 2002; Rathmell, 2000). For years, computer systems have been used to manage and operate such essential CI components as power grids; gas and oil distribution pipelines; water treatment and distribution systems; nuclear power plants; hydroelectric and flood control dams; oil and chemical refineries; air traffic control system; elements of the financial infrastructure; and other physical systems (Dacey, 2003a; Computer Science & Telecommunications Board and National Research Council, 2002). Further, the last decade has seen the control and execution of numerous critical functions and procedures shift to publicly networked computers without a great deal of thought for security (White House, 2003; Nye, 2002; Collins, 2001). Additionally, in an effort to reduce costs, SCADA systems (supervisory control and data acquisition systems) have been widely adopted (Graham-Rowe, 2003; Transition Office of the President's Commission on Critical Infrastructure Protection & the Critical Infrastructure Assurance Office, 1998). These programs, which allow supply systems to be managed from a central and often remote control point, used to be

custom-built software for isolated systems. Increasingly however, they are now largely stock versions which are internationally available. On discussing this shift, Bill Flynt, former director of the Homeland Infrastructure Security Threats Office for the US Army, noted that it has "...left us with generic SCADAs gateways to the companies operating on publicly accessible networks. These days, one cyber-attack fits all" (Graham-Rowe, 2003). This likelihood is not lost on terrorist groups. In early 2002, the FBI's National Infrastructure Protection Center issued a bulletin stating it believed members of al Qaeda were trying to gain remote control of U.S. water supplies and wastewater treatment plants (Isenberg, 2002).

By networking vital control systems via the CDI, organizations have been able to reduce operational costs by supporting remote maintenance, control, and update functions (Dacey, 2003a; Graham-Rowe, 2003). Yet these efforts have created many interdependent architectures that cross organizational boundaries such that often no single entity has sole control or responsibility for security (Sewell, 2002; Anderson, 1999). Because of the highly connected nature of intranets, extranets, and the Internet, unrelated networks and systems have potential access to one another which increases access points for would-be attackers (Tyrrell, 2000; Jordan, 1997). The United States' increasing dependency on information technology to manage and operate such a wide array of critical infrastructure services from power supplies to health and social services, provides terrorists with a tactical target and has inadvertently created a national Achilles' heel (Computer Security Institute, 2002; Isenberg, 2002; Moteff, 2002; Dearth, 2000). Operating in such an unsecured environment presents tremendous challenges when one considers that our economy and society rely on the secure transmission of

data, whether command, control, proprietary, intellectual property, financial, or otherwise.

Although U.S. governments only control roughly 15 percent of all U.S. infrastructure systems, they nevertheless perform essential services that rely on the CDI -whether to interface with the other infrastructure elements or the public (Sarkar, 2003; Institute for Information Infrastructure Protection, 2003; Sewell, 2002; Worthen, 2002; Bettelheim & Adams, 2001; Tritak, 2001a). As such, national debate has emerged over where to focus security efforts; on physical structures or on cyberspace (Council for Excellence in Government, 2002; Nye, 2002; National Infrastructure Protection Center, 2002). As the tragic events of 9/11 demonstrated, physical attacks can result in massive damage and loss of life in a very short period of time. Although the damage from a cyber attack is unlikely to manifest in such a manner, the potential damage is high (Computer Science & Telecommunications Board and National Research Council, 2002; U.S. General Accounting Office, 2001a). For example, military officials are acutely aware that a compromised computer system could kill people just as effectively as bombs or bullets (Krebs, 2003). Consider that an enemy could infiltrate a vulnerable military network to inject misleading information about the location of allied and enemy forces, leading to friendly fire casualties or an ambush. Further consider that the U.S. military's use of networked and satellite communications increased by more than 3,000 percent from the first Gulf War to the second (Shachtman, 2003).

While an isolated cyber attack can be severely damaging (Computer Security Institute, 2002; Moore, 1997), the impact of a successful attack on CDI elements is likely to have a global reach (Stanton, 2000; Anderson, 1999; Roos, 1998; Everett et al.,

1997). Evidence has shown that a cyber attack can spread so rapidly through the nation's networks that many victims rarely have a chance to respond (Drogin, 2000; Clarke, 1998). Even when forewarned, it is unlikely that networked organizations would have sufficient time to protect themselves as effective defenses can take months, even years, to develop, test, and implement (White House, 2003).

An attack targeting the CDI would likely cost lives by interfering with medical information systems and devices; rendering communications and electric distribution difficult or impossible by disabling control systems; compromising financial transactions; and disrupting transportation and shipping (National Infrastructure Protection Center, 2002; Nye, 2002). Fire, EMS, police, and others might be unable to communicate to one another at the scene of critical incidents. Dangerous fugitives or potential terrorists could unknowingly be admitted into the country or released from custody because police are unable to access databases containing criminal histories. Overall, numerous daily functions could grind to a halt which would likely impact both local and global economies. As such, the question presents itself; is the nation prepared and capable of operating "off-line" on short notice?

While the impact of a CDI attack could be shocking, simultaneous cyber and physical attacks, referred to as swarming attacks, would endanger lives directly-affecting both physical safety and well-being (Dacey, 2003a; Hennessy, Patterson, & Lin, 2003; National Infrastructure Protection Center, 2002; Verton, 2002; U.S. General Accounting Office, 2001a). A swarming attack would be used to worsen the effects of a physical attack. For instance, a cyber attack could be used to trigger the release of fuels or gas from a pipeline in the area of a planned physical attack thus stalling or even

stopping emergency efforts. If the airline hijackings of 9/11 were accompanied by a successful cyber attack on the air traffic control system efforts to clear the skies and scramble fighter jets would not have been as effective. Had those terrorists launched a coordinated cyber attack on communications channels, rescue teams would not have been able to coordinate responses or evacuate first responders from the towers. General panic among the public would have been even more likely.

While an increase in malicious cyber activity in recent years has been widely reported (White House, 2003; Department of Homeland Security, 2003; Freund, 2003; Deibert, 2003), the issue remains whether national leaders believe that cyber attacks are truly a threat to national and economic security. They may feel that we should stay focused on protecting the physical security of our citizens from terrorism believing that future threats will most likely take similar forms. However, if anything, these recent events point to the need for us to be prepared for the unexpected; to recognize that our enemies have the will and ability to coordinate large scale sophisticated attacks.

Breadth of Criminal Cyber Activity

A national telephone survey conducted by Pew Internet and the American Life Project (2001) found that Americans are deeply worried about criminal activity on the Internet. While their revulsion at child pornography is by far their biggest concern (92 percent of Americans say they are troubled by child pornography on the Internet), 87 percent of Americans say they are concerned about credit card theft online; 82 percent are concerned about how organized terrorists can wreak havoc with Internet tools; 80

percent fear that the Internet can be used to commit wide scale fraud; 78 percent fear hackers getting access to government computer networks; 76 percent fear hackers getting access to business networks; and 70 percent are anxious about criminals using computer viruses to alter or wipe out personal computer files. The question arises: how realistic are these fears?

For the last seven years, the Computer Security Institute has teamed up with the Federal Bureau of Investigation's Computer Intrusion Squad to conduct a nationwide survey of computer crime and security (Computer Security Institute, 2002). This longitudinal effort has helped researchers and industry alike understand the baseline of such activities. The numbers released for 2002 found that for the fifth year in a row, more respondents cited their Internet connection as the point of attack (74 percent) versus their internal systems as a point of attack (33 percent). Forty percent detected either Denial of Service attacks and/or outside penetration attacks on their systems. Seventy-eight percent detected employee abuse of Internet access privileges (for example, downloading pornography, use of pirated software, or inappropriate use of e-mail) and a full 85 percent detected computer viruses.

Computer Security Institute further reported that during 2002, 90 percent of respondents (primarily large corporations and government agencies) detected some form of computer security breach and 80 percent acknowledged that they suffered financial losses as a result. Of the 44 percent of respondents willing to quantify their losses, the total figure eclipsed \$455 million for 2002 alone. Yet only 34 percent of those that experienced a security breach reported the intrusion to law enforcement. Figures released by the Computer Emergency Response Team at Carnegie Mellon University

stated that nearly 35,000 attacks were reported in the first 10 months of 2001 alone. This proved a 60 percent increase over the entire previous year (McWilliams, 2001). Further, a 2001 study by researchers at the University of San Diego found that Denial of Service attacks, such the one that froze Internet traffic in 2000 to such large sites as CNN.com and Ebay.com, are currently being launched at a rate of nearly 4,000 per week (Costello, 2001). Collectively these findings indicate that there is much more unauthorized and criminal activity going on in cyberspace than commonly acknowledged.

Further, an overwhelming number of sources (Department of Homeland Security, 2003; Costello, 2001; Vatis, 2001; U.S. General Accounting Office, 2001c; European Committee on Crime Problems, 2000; Reames, 2000; Stambaugh et al., 2000; Stanton, 2000; Triagaux, 1998; Center for Strategic and International Studies, 1998) note that the speed, virulence, and maliciousness of cyber attacks have increased dramatically in recent years. Criminals have used the Internet to penetrate such high profile organizations as the Pentagon, the White House, the FBI, the Department of Defense, NASA, Los Alamos, Microsoft, and AT&T (Computer Security Institute, 2002; Bettelheim & Adams, 2001; Costello, 2001; Dacey, 2001; Vatis, 2001; Cheney, 1999). Additionally, in recent years powerful worms and viruses have been used to launch numerous cyber attacks globally including the widely publicized 'Melissa virus', 'I Love You virus', 'SirCam worm', 'Code Red I/II worm', 'Nimda worm', 'SQL/Sapphire worm', to name a few (Symantec.com, 2003; Dick, 2001; McDonald, 2001; Rhodes, 2001). According to the National Strategy to Secure Cyberspace (White House, 2003) the Code Red worm infected 150,000 computer systems in just 14 hours. Conservative estimates of 2001

corporate losses from the Code Red and Nimda worms are over \$3 billion due to lost productivity and costs to disinfect systems (Freund, 2003). The SQL Slammer worm (IT-ISAC, 2003; Fisher, 2003a), infected over 200,000 computers and generated more than 7 million error events in North America alone. Worldwide it affected between 400,000 and 700,000 computers, clogged networks, and stalled Internet-enabled devices.

Despite the evidence, some critics (Koerner, 2003; Deibert, 2003; Shachtman, 2002; Verton, 2001; Roos, 1998; Smith, 1998) still speculate that the actual threat to the critical digital infrastructure is over inflated, much like the dot.com technology market of the late 1990s. Indeed, attacks targeting the CDI itself remain rare (Computer Science & Telecommunications Board and National Research Council, 2002). However, in October 2002, NIPC reported that the 13 root-name servers that provide the primary roadmap for almost all Internet communications were targeted in a massive Denial of Service” attack (Dacey, 2003a; Associated Press, 2002). Seven of the servers failed to respond to legitimate network traffic, and two others failed intermittently during the attack.

Howard Schmidt, former vice chairman of the White House’s Critical Infrastructure Protection Board, avers that the threat is undeniably real and indeed serious, stating, “...the more we depend on the critical infrastructure being run by IT systems, the harder we’ll have to work to make sure we don’t fall into the situation where these threats become more than just an inconvenience” (The New Atlantis, 2003). So what exactly are the threats to CDI elements and who is vulnerable to them?

Exploiting Vulnerabilities

In order for a threat to exist two conditions must be present. First, there must be the capability for a threat to occur, such as the presence of a vulnerability. Second, it must be possible to exploit the vulnerability (Anderson, 1999). As a principle of computer security risk management, a vulnerability is “the absence or weakness of a safeguard in an asset that makes a threat potentially more harmful or costly, more likely to occur, or likely to occur more frequently” (Miller & Gregory, 2002). As such any information and communication technology element from information systems and internal controls, to implementation methods and design could potentially contain an exploitable vulnerability (Phoha, 2002; U.S. General Accounting Office, 1996b). Often even the best security systems are unknowingly vulnerable. Only a few years ago a private research and development company was hired to covertly determine the security of the U.S. Department of Defense’s (DoD) network systems (Goodman, 1997). Within the first week, the ‘hacking team’ successfully broke into 65 percent of all DoD systems. Further, the DoD only detected 4 percent of the occurrences.

According to many sources (White House, 2003; Department of Homeland Security, 2003; Computer Science & Telecommunications Board and National Research Council, 2002; Noonan, 2001; Wulf, 2001), vulnerabilities are surfacing faster than the country's ability and willingness to respond. Between 1995 and 2003, Computer Emergency Response Center (CERT) at Carnegie Mellon University documented over 10,000 computer technology vulnerabilities. While certainly an alarming number, remedies known as “patches” or “fixes” have been made widely available to correct

many of these vulnerabilities (Fisher, 2003a; Computer Science & Telecommunications Board and National Research Council, 2002). Even still, the technology research firm, the Gartner Group (Associated Press, 2002) projected that through 2005, 90 percent of computer attacks will continue to succeed by exploiting known vulnerabilities for which a corrective patch is available but simply not installed.

The most recent *Internet Security Threat Report* (2003) released by Symantec Corporation, a global leader in Internet security technologies, states that approximately 60 percent of all documented vulnerabilities remain easily exploitable either because exploit tools are widely available or are not required at all. The report further notes that of the vulnerabilities newly identified during 2002, a full 85 percent were recognized as moderate or severe. It has been estimated that as much as 95 percent of today's successful attacks exploit these commonly known flaws using widely available automated tools (Forman, 2003). As such, a savvy attacker with a modest degree of sophistication can easily exploit numerous vulnerabilities found in today's commercial software products. Addressing this state of affairs, a security bulletin on the Microsoft website (2003) offered a somewhat bleak and condescending suggestion to network administrations "...don't hold your breath waiting for a patch that will protect you... sound judgment is the key to protecting yourself...".

The Internet Security Threat Report suggests a trinity of events has led to the dramatic increase in system vulnerabilities of recent years. First, the IT industry has come under increased pressure from media coverage of high-profile attacks which has creating a push for responsible disclosure of known flaws. Second, researchers are using new methods to discover software bugs and fix vulnerabilities before would be

attackers exploit these defects. Finally, the report along with other research (Verton, 2003a; 2003b; Institute for Information Infrastructure Protection, 2003; Computer Science and Telecommunications Board, and National Research Council, 2002; Denning & Baugh, 2000) suggest that a significant portion of software and hardware flaws can be squarely attributed to vendors, who, in the rush to get commodities to market, fail to make security a priority during product development.

The critical digital infrastructure is dependent on the availability of reliable and secure networks (Anderson, 1999). Yet it is well documented that many of the features that make the underlying information systems so successful, such as distributed networking and plug-and-play compatible software/hardware, make the CDI inherently vulnerable to attack (Dacey, 2003b; Information Assurance Advisory Council, 2001; Public Technology, 2000; Sunshine, 1999). For example, consider that electronic mail systems, commonly referred to as email, have long been a source for intruder break-ins (Rhodes, 2001; Fraser, 1997). This is because by its very nature, an email system requires access to the outside world and most email servers accept input from any source. A 1999 study found that 84 percent of respondents admitted to regularly sending and receiving personal email at work (Naughton, 1999). By digitally interacting with so many potentially unsafe sources, employees unknowingly introduce threats into otherwise protected networks- and would be attackers know this. For instance, concerns about instant messaging security were heightened by the recent disclosure of six vulnerabilities in America Online Inc.'s instant messaging software 'Mirabilis ICQ'. Cnet.com (Lemos, 2003) reported that the most recent version this software has been downloaded from its site more than a quarter of a billion times; no doubt a countless

number of these were onto government computers. If left unpatched, exploiting these ICQ vulnerabilities could create dangerous holes in enterprise firewalls, leaving sensitive data exposed on public networks resulting in the unprotected transfer of files (Vijayan, 2003).

Another seemingly innocuous technology is the Domain Name System (DNS) that is used to match and verify network names to host addresses (Phoha, 2002; Fraser, 1997). This one system is absolutely vital to the secure operation of any network. An attacker who is able to successfully control or impersonate a DNS server can re-route or divert network traffic to a compromised system. Likewise, they could trick users into providing confidential information such as passwords or credit card information. Finally, consider wireless technologies that are being widely adopted because they allow users to move handheld devices or laptops from location to location without wires and without losing network connectivity. Forecasts made by IBM and Symantec at the 15th Annual Canadian IT Security Symposium warned that by the decade's end viruses, hacking, and security breaches of wireless-based systems will be a top problem for IT administrators (Careless, 2003). The inherent vulnerability and risk to wireless technologies lies in the underlying communication medium, the airwaves, which is virtually open to snooping intruders. This makes wireless communication more prone to loss of confidentiality and integrity. Among the biggest challenges of wireless connectivity is that an infected device can upload viruses or malicious code directly into an organization's network whenever it is synced (NetScreen Technologies, 2003b).

Threats and Attacks

Just as each technology has inherent weaknesses as well as distinct security safeguards, each is also accompanied by an array of unique threats (Institute for Information Infrastructure Protection, 2003; Fraser, 1997). In other words, means and methods of exploiting vulnerabilities have become as diversified and specific as the targets. For instance, email servers are highly vulnerable to viruses and worms. Commonly used threats and techniques include sniffers, backdoors, DoS, worms, logic bombs, social engineering, probing, false authentication, tunnels, spoofing, Trojan horses, malicious applets, war dialing, password crackers, et cetera (Hansell, 2003; Freund, 2003; Hobbs, 2000; Sager et al, 2000; U.S. Department of Justice, 1999; Trigaux, 1998).

The same as the means of each threat differs, so do the aims. Yet fundamentally, there is a limited number of archetypal threats to information security, namely, denial of service; unintended disclosure of information; unauthorized disclosure of information; and unauthorized access to resources/information (Center for Strategic and International Studies, 1998; Moore, 1997; Fraser, 1997). Depending on intentions, compromises due to threats can be either observable, such as an active virus, or clandestine, such as espionage in search of classified information. Would be attackers could use a combination of both to plot future cyber strikes or swarming attacks by mapping U.S. information systems, identifying key targets, and lacing infrastructure elements with back doors and other means of access (Goldberg, 2003).

Additionally, threats can either be deliberate or accidental (Computer Science & Telecommunications Board and National Research Council, 2002; McWilliams, 2001; Moore, 1997; Mills, 1995). Accidental compromises occur because of either natural causes, such as a lightning surge that causes part of a network to fail, or human error, such as a programming mistake that creates a weakness in a network or unintentionally cutting a communications cable during excavation. However, deliberate compromises are the result of conscious human action. Security experts often refer to the efforts of these malicious actions as attacks.

As the number of individuals with computer skills has increased, so to have the number of readily available and relatively easy to use intrusion and hacking tools. Security experts note that there are thousands of websites that offer free digital tools that let people snoop, crash, modify, or even hijack computers (Dacey, 2003a; Tritak, 2001a; Bissett & Shipton, 2000; Center for Strategic and International Studies, 1998). As such, a person's technical skills do not have to be very sophisticated to cause damage (Wulf, 2001; Sager et al, 2000). However, in recent years it seems the goals, methods, and means of attacks have been changing (Computer Science & Telecommunications Board and National Research Council, 2002; Anderson, 1999). During the 1990s, most hackers operated like vandals,

...attacking vulnerable targets with an experimental, shotgun approach. Malicious hackers concentrated their efforts on destructive viruses and swiftly spreading worms that crawled haphazardly across the Internet, infecting individuals and corporations indiscriminately (Freund, 2003).

Today there are far more dangerous and targeted attacks carried out by highly skilled hackers motivated by financial gain and armed with the expertise to cause

serious damage (Freund, 2003). Hackers have moved beyond basic tools like viruses and port scanners to more sophisticated techniques that use such tools in concert (Hobbs, 2000). For instance, there are now computer worms that can remotely open back doors on networks. These mechanisms monitor traffic, intercept passwords, and establish secret communication channels for the hacker to use to pluck sensitive information at will. Additionally, recent attacks involve 'rapid mutation', where the level and source of cyber-threat changes rapidly in unpredictable ways. This is generally combined with the characteristic of 'diverse origin' where an attacker need not be localized in relation to the target. As such an attack can be orchestrated by any number of globally distributed actors. While attacks have always exhibited this quality, greater experience combined with more sophisticated attack strategies and techniques have made the identity of cyber-attackers increasingly difficult to ascertain (McDonald, 2001). Further, attacks are increasingly utilizing stealthy attributes of criminal espionage to launch more effective and destructive attacks with minimal warning. As such, not all attacks are created equal as some are more destructive than others.

Despite the real and growing threat from cyber attacks, most cyber offenses fit under the umbrella of "internet fraud" (Cheney, 1999). These offenses involve "any type of fraud scheme that uses one or more components of the internet, chat rooms, message boards, Web sites, or e-mail, to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme" (Department of Justice, May 8, 2000, p. 1). In 2002, 47 percent of all fraud complaints filed with the Federal

Trade Commission were Internet-related, up 16 percent from just three years earlier (Shim, 2003).

Until recently, the majority of computer fraud and network intrusions were committed by current or former employees, referred to as insiders (Nash, 2003; Computer Security Institute, 2001; McCarthy, 1998; Goodman, 1997; Charney, 1994; Hurewitz & Lo 1993). Katz and Carter (1998) state that the reason for this is that "...insiders are familiar with their employers' data processing operations and the type of data each system and application is storing and processing... and therefore know exactly where to look for information" (p. 224). These criminals often act because they feel the company owes them something. As such, motivation could be for profit by stealing and selling intellectual property or the offender might feel that the organization wronged them and thus destroying data and software would be revenge (Dacey, 2001; Dick, 2001). Additional motivation exists as mere opportunity.

Upon addressing the threat of insiders, the National Manager of NITSSC, Michael Hayden, reminds how information systems contain "...vast amounts of sensitive and classified mission critical data. The potential for abuse is obvious" (NSTISSAM INFOSEC, 1999, forward). Yet criminals continue to obtain sensitive IT jobs because organizations, including elements of the US government, often fail to require background checks on new technology workers. For instance, the leader of an international hacking ring credited with a series of attacks against U.S. computer security organizations between 2000 and 2002 was found working as a support technician in a U.K. office of Siemens Communications (Roberts, 2003). While currently

it is not know whether the man compromised his employer or client systems, the point is criminal hackers work right under our nose within the information infrastructure.

The 1997 report of the President's Commission on Critical Infrastructure Protection recommended allowing limited exemptions for private employers to request consensual background checks and to administer polygraphs to employees in sensitive positions. Yet background checks and polygraph examinations are not the industry standard. In an interview for Computer World Magazine (Verton, 2003a), the CEO of a U.S. executive search firm remarked, "I'm surprised at how few of my clients actually do background checks on their information security professionals... at most, they require me to do a reference check." This alarming habit demonstrates the potential ease with which ill-intending individuals can get hired into sensitive positions.

Complicating the issue, consider the serious challenges and vulnerabilities accompanying the growing reliance the U.S. software industry has on overseas developers in such countries as India, Pakistan, Russia, and China. A recent study by Gartner Inc. predicted that by 2004, more than 80 percent of U.S. companies will consider outsourcing critical IT services, including software development to foreign companies. Opportunistic foreign employees could potentially program backdoors into vital software that can later be exploited. In light of recent changes in the global security environment, this scenario poses a very real threat (Verton, 2003a).

While insiders will continue to pose a threat to information security for these and other reasons, a recent study by Deloitte & Touche found that 90 percent of network and system attacks are now coming from external forces and only 10 percent from inside sources. This shows a marked change from recent years were 60 to 70 percent

of attacks were internally sourced. When asked about this shift, a spokesperson with Deloitte & Touche commented, "As organizations become more connected there are more doors people can rattle to get in" (Nash, 2003, online). According to Symantec Corporation (2003) attacks originating from within the United States accounted for more than 35 percent of all of the attacks reported during 2002. Rounding out the top five sources of cyber attacks were South Korea, China, Germany, and France. Launching 23.7 attacks per 10,000 Internet users, South Korea appears to have the most attackers per capita among countries with large online populations. The U.S. is not in the top 10 of this list.

The FBI (Dacey, 2003a) notes that increasingly terrorists, transnational criminals, and foreign intelligence services are using information exploitation tools to destroy, intercept, degrade, or deny access to data. As of yet, the White House (2003), does not believe that any traditional terrorist group has used the Internet to launch an assault on the US infrastructure. However, former White House cyber-security czar Richard Clarke recently said, "...[information technology] has always been a major interest of al-Qaeda. We know that from the laptops... we've recovered that have hacking tools on them. It is a huge mistake to think that al-Qaeda isn't technologically sophisticated, a fatal one" (Fisher, 2003b).

Government and the CDI

Increasingly, government units at all levels are turning to information and communication technologies to improve and increase the services they provide (Council for Excellence in Government, 2003; Dunn, 1999; National Research Council, 1999; Center for Technology in Government, 1997a). A certain extent of this technical migration is mandated by federal legislation (Committee on the Internet in the Evolving Information Infrastructure, 2001; Government Electronics and Information Technology Association, 2001; McDonald, 2001; Tritak, 2001a), for example, the Federal Paperwork Reduction Act (44 U.S.C. §3501) and more recently, the Government Information Security Reform Act (NetScreen Technologies, 2003a). In some instances, state legislatures impose their own technical mandates on subunits of government, as is the case in Florida with statute 282.5004 which required Y2K compliance; statute 943.08 which mandates the coordinated sharing of criminal justice and other public safety system data; and statute 408.913 which requires the development of a comprehensive health and human services eligibility access system (Florida Statutes, 2002). By and large, however, updating services and procedures through the implementation of advanced digital and communication technologies remains at the voluntary discretion of each individual government, often at the departmental level (Council for Excellence in Government, 2002).

One of the more publicly touted government uses of IT is known as “electronic government” (henceforth, e-government). E-government is “...the use of technology, particularly web-based Internet applications, to enhance the access to and delivery of

government information and services to citizens, business partners, employees, agencies, and other entities” (Intergovernmental Advisory Board, 2003, p.6). The wide-ranging goal of e-government is to seamlessly integrate back-end business processes involving suppliers, contractors, and partners with front-end processes aimed at clients and customers (FTAA, 2002; Anderson, 1999). Such efforts often necessitate the creation of new departments and procedures; hiring IT and security experts; and regularly call for multi-year initiatives (Kayyem & Howitt, 2002). When these matters are successfully addressed, e-government can provide citizens and businesses with 24/7 self-serve access to services in the areas of income taxes, social security, un/employment, official records, passport applications, drivers licenses, car registration, building permits, public libraries, and more (Arrison, 2002; Dacey, 2001; Deloitte Research, 2000; Dunn, 1999). Electronic services to businesses are equally vast and generally deal with permits, records, taxes, licenses, declarations, and procurement, among other services. In 2002, the Center for Digital Government predicted that state and local governments would spend \$78.1 billion on IT in that year alone (Pratt, 2002).

The benefits of e-government are numerous and documented (FTAA, 2002; Council for Excellence in Government, 2002; Rathmell, 2000; National Research Council, 1999). For example, a 2003 report released by Intergovernmental Advisory Board found, "States that implemented E-government programs for grants management streamlined their processes, eliminated paperwork, reduced application processing time and saw their staff costs reduced by as much as 35%" (p. 13). However, incorporating networked information and communication technologies into government is far from a service-delivery panacea as it introduces numerous issues pertaining to data privacy,

accessibility, and of course security. For example, in a recent report prepared for the House of Representatives, the U.S. General Accounting Office revealed that a review of Internet security of the Internal Revenue Service (IRS) exposed almost 900 weaknesses across the 11 IRS organizations (Dacey, 2003a). The report stated that while most of the weaknesses were in the areas of access and authorization, all of the weaknesses could be traced to the incomplete implementation of an agency-wide security program. Corroborating these findings was former White House cyber security czar Richard Clark (Fisher, 2003b) who criticized that the government is actually less capable of securing its networks that it was a year ago and additionally it is doing an unacceptable job of helping the private sector lock down critical infrastructures.

Perhaps the most disconcerting account of the state of overall government computer security is the annual congressional report card on computer security conducted by the House Government Reform Subcommittee on Government Efficiency, Financial Management & Intergovernmental Relations in conjunction with the General Accounting Office (Dacey, 2002). The 2002 analysis reported that the computer security of nearly two-thirds of the federal government's 24 major agencies earned failing marks. Among the failing department were the Justice Department, State Department, Office of Personnel Management, Treasury Department, Energy Department, Defense Department, Interior Department, Agriculture Department, Federal Emergency Management Agency, and Transportation Department. The analysis concluded:

...federal systems were not being adequately protected from computer-based threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations (p 12).

Commenting on the report, Rep. Stephen Horn (R-CA) stated "September 11 taught us that we must be prepared for attacks. We cannot allow government operations to be compromised or crippled because we failed to heed that lesson" (Krebs, 2002). Indeed these attacks have spurred a detailed re-evaluation of many spheres of life as Americans have become acutely aware of how vulnerable and interconnected all of infrastructure systems are (Hecker, 2002; Kayyem & Howitt, 2002; Bettelheim & Adams, 2001; U.S. General Accounting Office, 2001c).

As outlined in Presidential Decision Directive 63 (1998), the basic federal approach to critical digital infrastructure protection has remained a strong policy preference for consensus-building and voluntary cooperation rather than regulatory actions (Tritak, 2001a). Yet experts have long warned that local, state, and national agencies have yet to fully achieve consensus or truly function in the spirit of cooperation (Whitehouse, 2003; Dacey, 2003a; Monroe, 2002; Posner, 2002; Collins, 2001; Willemssen, 2001; McCarthy, 1998; Dalrymple, 1998; Center for Technology & Government, 1997a; 1997b). Further, they do not share enough information and generally lack a working plan to deal with cyber attacks (Bettelheim & Adams, 2001). Among the challenges is that the nature of security concerns for the federal government, local governments, the military, and industries differ. This has led to problems since these sectors often share infrastructure elements for reasons of efficiency and economy (Schumacher & Ghosh, 2000).

The U.S. General Accounting Office (Dacey, 2003a) reports the need for federal agencies to provide outreach efforts to state and local government to increase their infrastructure protection efforts. The current Homeland Security initiative designed to

meet this need is The National Strategy to Secure Cyberspace, which endorses partnership, exchange, as well as local and private buy-in, which are all seen as essential to success (White House, 2003). Supported in large part by the newly created Department of Homeland Security, the strategy calls for coordination and outreach to state and local governments through collaborative public-private activities, such as sharing best practices; evaluating and implementing new technologies; raising cybersecurity awareness; increasing criminal justice activities; and developing national security programs to deter future cyber threats (Hecker, 2002; Walker, 2002).

Billed as a strategy rather than a plan it calls for a change in thinking on the part of computer security professional and the public. Yet realizing this strategy will involve more than jargon. It will call for grants, regulations, tax incentives, regional coordination, and accountable partnerships. It will require the systematic identification of the unique resources and capacities of each government unit followed by an accurate matching between these capabilities and specific tasks (Posner, 2002; National Research Council, 1999). It will also entail identifying and then tackling weaknesses.

Local Government

So in war, the way is to avoid what is strong and to strike at what is weak (-Sun Tzu, The Art of War).

Typically, local government information systems are not directly attacked because they do not yield enough valuable information commiserative with the effort and risk involved (Hennessy, Patterson, & Lin, 2003; Public Technology, 2000). Yet as

local governments continue to connect more systems to the Internet and offer more services via these networked systems the amount of “exploitable information” will increase. Conversely, so to will the return from breaching these systems. Currently, however, local systems are generally attacked because successful breaches create media attention, and/or quite simply, because these systems are generally weak (Gartner Consulting, 2000).

According to Symantec Corporation (2003), opportunistic attackers often locate and strike any vulnerable system connected to the Internet regardless of who owns the system or the specific function of the system. In this situation a victim is not targeted but rather selected after being recognized as vulnerable. Targeted attacks, however, are directed at a specific organization. In theory, individuals who launch these types of attacks have identified a target and have made a deliberate attempt to gain access to its network. In this situation, an attacker looks for ANY weakness that will enable him/her to gain access to the targeted organization (Institute for Information Infrastructure Protection, 2003; Center for Strategic and International Studies, 1998). Therefore, in both cases weak systems are targeted.

State and local government information systems and security procedures have increasingly come under fire for being weak links in the larger national infrastructure protection efforts (Dalton, 2002, Yim, 2002a; Davies, 2001). A study by Gartner Consulting (2000), noted that for most small and medium size local governments information security is not approached as a full time job thus leading to the creation of significant security issues. Public Technology Inc. (2000) also noted that local jurisdictions often have either inadequately trained staff or simply lack an adequate

information security staff. This, in combination with insufficient security budgets, creates vulnerable systems.

Weak information security efforts among local governments have been documented for years and continue to be highlighted (Brock, 2000; Dacey, 2000; PDD-63, 1998; Smith, 1998; Crescenzi, 1996; U.S. General Accounting Office, 1996a; Solomon, 1995; Toffler & Toffler, 1993). As a case in point, the “2002 State of America’s Cities Survey” revealed that only 26 percent of city officials (n=725) indicated that cyber threats were addressed in their city’s planning; even though 85 percent indicated that they were concerned or very concerned about cyber attacks as a form of terrorism (Hoene, Baldassare, & Brennan, 2002). Several reasons are regularly cited for why the information security of local governments continues to lag behind including smaller budgets, lack of available skilled personnel, entrenched cultures, parochial concerns, general inertia, and fragmentation of local and state governments among others (Hecker, 2002; Yim, 2002b; Davies, 2001). Like many small organizations, local governments often lack the experience to adequately inform themselves about cyber threats to their networks and systems. Operating from this uninformed position, they often cannot justify allocating the resources for protective measures (Information Assurance Advisory Council, 2001).

County Government

Among those facing these challenges are county governments (Gonzales, 2001; U.S. General accounting Office, 2001c). Often called ‘invisible governments’, counties

are generally responsible for maintaining such diverse services and programs as natural resources; fire protection; water supply; housing and community development; sewerage; cemeteries; libraries; parks; roads and highways; hospitals; education; airports; utilities; and records (National Association of Counties, 2001c; Altshuler, et al. 1999). More than states or cities, counties interact with differing levels of government on a day-to-day basis (Barrett, Greens, & Mariani, 2002). With limited power, counties are continually squeezed by the governments above and below them. According to the 2002 Local Government Directory released by the U.S. Census Bureau there are 87,849 units of local government identified as being either general-purpose (3,034 counties, 19,431 municipalities, and 6,506 townships) or special purpose (13,522 school districts and 35,356 special districts). As such, an average county has 28 general/special purpose sub-county governments operating within its jurisdiction.

All but two U.S. states (Connecticut and Rhode Island), and the District of Columbia have operational counties governments⁴ (National Association of Counties, 2001c). The number of counties per state ranges from three in Hawaii to 254 in Texas. Geographically, counties span an equally broad range varying in size from just 67 square kilometers (Arlington County, Virginia) to the 227,559 square kilometers of North Slope Borough, Alaska. The mean county population is just under 80,000 people yet three-fourths of all counties have populations smaller than 50,000. Despite the averages, counties remain as diverse as the populations they serve. For instance, Loving County, Texas, serves approximately 150 inhabitants, while Los Angeles

⁴ Alaska and Louisiana refer to their counties as boroughs and parishes respectively.

County, California, serves more than 9 million. In addition to the 3,034 traditional U.S. counties, 31 are chartered to operate as city-county governments where functions are consolidated (i.e., Duval/Jacksonville, Florida; San Francisco, California; and New York, New York). Regardless of charter distinctions, administrative rights and responsibilities are generally vested by state constitution or statute (U.S. Census Bureau, 2002a; Altshuler, et. al. 1999).

According to the National Association of Counties (2001c), there are three main types of county governance, Commission/Administrator, Council Executive, and Commission. The commission form of government, the oldest form of government in America, remains the most widespread (72 percent). A descendent of the old English shire-moot system (Iowa State Association of Counties, 2003), counties are characterized by an elected governing board, usually comprised of three to seven members, which holds both legislative and executive powers. The board serves as the governing body for the county and is responsible for the budget, passing resolutions, and enacting locally relevant ordinances and regulations.

Strained interorganizational communication and cooperation are commonplace within county government, whether between officials, departments, or municipalities (International City/County Management Association, 2002). These relationships can be difficult and even acrimonious. Among the greatest challenges is the structural reality that counties are run by numerous elected officials who do not have to report to the Board of Commissioners or single county administrator. For in addition to the board, several constitutional posts are filled through general elections to head major county offices. These often include Sheriff, Property Appraiser, Supervisor of Elections, Tax

Collector, and Clerk of Court, though this varies considerably from county to county. These department officials often claim that their mandate comes directly from the voters and as such they do not need direction from an external administrative body (Barrett, Greene, & Mariani, 2002). This is especially true with regard to IT related issues where it is common for agencies to invest in solutions aimed specifically at meeting only their needs without general thought to the interplay between the agencies themselves (National Research Council, 1999). For example, in Palm Beach County Florida, the Property Appraiser, Tax Collector, Clerk of the Court, State Attorney, Sheriff, Public Defender, and Supervisor of Elections all have their own autonomous IT staffs and systems (Governing.com, 2002). Compounding these IT challenges are the barriers which exist between local, state, and federal governmental bodies. According to one county official,

Inter-jurisdictional coordination and cooperation is a major challenge. Many government services and work processes transcend jurisdictional boundaries. Despite the willingness of the parties, it is often difficult to align the focus, priorities and capabilities of the agencies (Governing.com 2002).

Many counties are beginning to assess how to restructure relationships among contiguous local entities to take advantage of economies of scale; promote resource sharing; and improve coordination of preparedness and response on a regional basis (Monroe, 2002, Posner, 2002). Counties are also rethinking roles and responsibilities with regard to information security as they are becoming increasingly aware of the vulnerabilities of their information technology systems (Kouns, 2003; O'Connell, 2003; Barrett, Greene, & Mariani, 2002; Gonzales, 2001). In recent years, counties across the nation have created steering committees and appointed information security executives

(known as Chief Information Officers, Chief Technology Officers, or Chief Information Security Officers) to work towards greater IT security (Lee, 2001; West & Berman, 2001; Intergovernmental Advisory Board, 1998). These information security executives are generally brought in to provide technological vision and management. In addition, they are often responsible for technology planning such as sponsoring collaborative planning processes; establishing strategic partnerships; coordinating divisional initiatives; general infrastructure and application development; ensuring ongoing investment; and outsourcing (Gartner Group, 2002; Frazer, 1997).

Along side national and state leaders, county IT directors work on the front lines to balance public demands and entrepreneurial growth with cyber security and national defense. An online survey conducted by CIO Magazine (2002) revealed that the majority of IT executives spend more of their time engaged in strategic planning than pure technology. While they take an obvious leadership role in terms of the organization, systems, and the underlying IT infrastructure; they dispense a considerable amount of energy attempting to steer knowledge management and the valuation of intellectual capital. It is often the case that IT directors report to senior executives, commissioners, and elected officials who do not necessarily have a great deal of technology-related knowledge (Sarkar, 2002; National Research Council, 1999). As Gartner Consulting (2000) reported in a recent study, "The cold hard fact is that most elected officials, city managers, and chief administrative officers do not understand the internet or its profound influence on government operations and citizen demands" (p. 9). As such, part of the job of an IT director is selling not only the value of technology but also the value of security (Forman, 2003; Perlman, 2002a).

Information Security: More than Technology

Attaining one hundred victories in one hundred battles is not the pinnacle of excellence. Subjugating the enemy's army without fighting is the true pinnacle of excellence (-Sun Tzu, The Art of War).

The nature of the Internet is an intrinsic trade-off between utility and security (Computer Science & Telecommunications Board and National Research Council, 2002; Information Assurance Advisory Council, 2001; McCarthy, 1998). As a rule (Collins, 2001), the best and most secure systems are the ones built with security in mind from the ground up. However, security is not built into the Internet itself, thus, as a society we are now tasked with retroactively securing a living system that was designed to be open for easy connectivity with few controls (Bettelheim & Adams, 2001; Cohen, 2000). Consequently, information security remains an unpredictable circle of action and reaction (Doddrell, 1996). When vulnerabilities are corrected, attackers look for new paths to exploit and so on. Yet security is still practiced only half-heartedly throughout much of the government and corporate America (Dacey, 2001; Willemsen, 2001). In the journal *Issues in Science and Technology*, author George Smith (1998) frankly suggested, "If organizations don't intend to be serious about security, they simply should not be hooking their computers to the Internet". While undoubtedly a valid suggestion, this option is simply not realistic.

To understand information security, it is important to note that information systems, both automated and manual, are composed of three basic elements: information transfer links, information processing nodes (including storage), and human

factors (Phoha, 2002; Transition Office of the President's Commission on Critical Infrastructure Protection & the Critical Infrastructure Assurance Office, 1998). Fundamentally, information security is the protection of information systems, whether transfer or processing, against unauthorized access, modification, or denial of service to authorized users (Schumacher & Ghosh, 2000). Information security includes those measures necessary to prevent, detect, document, counter, and mitigate such threats (Guel, 2001; Center for Technology in Government, 1997a). It involves "...determining what you need to protect, what you need to protect it from, and how to protect it. It is the process of examining all of your risks, then ranking those risks by level of severity" (Fraser, 1997, p. 4). The more complex a system is, the more likely critical vulnerabilities will exist and potentially be overlooked (Collins, 2001).

If for a moment one assumed that all technological holes could be secured today, there would still be the introduction of new vulnerabilities at some future point and of course human error (Wulf, 2001). Many compromises result from improper configuration (Hennessy, Patterson, & Lin, 2003; Computer Science & Telecommunications Board and National Research Council, 2002). For example, a system firewall may be improperly configured to allow web access when, in fact, the system should only transmit and receive e-mail or an operating system may lack a critical "patch" because the system was restored from a backup tape that did not include the patch in the first place. In light of the numerous points for error, information security is best approached holistically bearing in mind how technological, managerial, organizational, regulatory, economic, and social aspects interact (Institute for Information Infrastructure Protection, 2003; National Institute of Standards and Technology, 2003; Everett, Dewindt, and

McDade, 1997; Korzyk & Wynne, 1997). With so many aspects involved in executing even the simplest functions, points for error are potentially innumerable. Consequently, maintaining a holistic vantage to information security is vital as one weak link can topple even the strongest systems.

At the heart of information security are three ideas commonly referred to as the information security triad (Miller & Gregory, 2002; Wulf, 2001; Fraser, 1997). These ideas are confidentiality, integrity, and availability. Confidentiality can be thought of as privacy, secrecy, or control of information. When a system lacks confidentiality, there can be a “leak” of information and resources. Integrity commonly refers to the quality and reliability of data. When integrity is lacking, system data can easily be corrupted or modified by attackers. Data integrity includes protecting data/systems from unauthorized modification and ensuring that transferred data is safely sent/received between known reliable sources. Availability is simply that; having systems and functions available when needed by those authorized to use them. The opposite of availability is commonly referred to as denial of services, denial of use, denial of information, or simply denial. Taken collectively, an IT manager is therefore concerned with the level of risk associated with loss of privacy (i.e. unauthorized individuals reading of confidential information), loss of data (i.e. corruption or loss of information), and the loss of service (e.g. running out of data storage space; denial of network access; or overburdening computational or processing resources).

To simultaneously achieve these three qualities, information security is layered whereby some layers are designed to protect, some to detect, and others offer fail-safes (Collins, 2001). Additionally, security is compartmentalized, like a honeycomb with trap

doors, where flexible layers are set up as defense barriers to contain breaches to the smallest area possible. The “Common Body of Knowledge” (henceforth, CBK), also referred to as the “ten domains of information security”, encompasses the breadth and base of knowledge deemed necessary for information security professionals to successfully apply and integrate these vital layers (Miller & Gregory, 2002). The CBK, maintained and amended by the nonprofit organization International Information Systems Security Certifications Consortium (ISC2), is the international compilation and distillation of security material relevant to IT security professionals. Briefly described, the 10 areas are (ISC2.com, 2003):

1. Access Control Systems and Methodology: Mechanisms that work together to create a security architecture for protecting information system assets.
2. Applications and Systems Development: Security as it applies to application software development.
3. Business Continuity Planning: Preservation and recovery of business operations in the event of outages.
4. Cryptography: Principles, means, and methods of disguising information to ensure its confidentiality, integrity, and authenticity.
5. Law, Investigation and Ethics: Computer crime laws and regulations as well as technologies used to investigate computer crime incidents.
6. Operations Security: Controls for hardware, media, and the operators/administrators with access privileges to said resources.
7. Physical Security: Protection techniques for an entire facility from the outside perimeter to inside office space, including all information system resources.
8. Security Architecture and Models: Concepts, principles, structures, and standards to design, monitor, and secure operating systems, equipment, networks, applications, and controls used to enforce confidentiality, integrity, and availability.

9. Security Management Practices: Information assets and definitions for the development, documentation, and implementation of policies, standards, procedures, and guidelines.
10. Telecommunications, Network, and Internet Security: Network structures, transmission methods, and transport formats used for transmissions over private/public communications network.

Staying on top of each of these knowledge areas is a near Herculean task for IT professionals. Yet, the Computer Science & Telecommunications Board together with the National Research Council (2002) report that isolated human error is usually not the cause of security problems, rather it is management practice. Indeed, faced with ever-dynamic technology innovations, IT managers are frequently pressured to make quick decisions based on incomplete information, limited staff, short budgets, and imposing demands from executive management. Common decisions involve trade-offs between services offered, ease of use, and costs on one hand, and security, confidentiality, integrity, and availability on the other. In the end, security administrators must not only be adept with all areas of the CBK but must also be knowledgeable of government regulations, physical security, public-private sector partnerships, and management practices (Hennessy, Patterson, & Lin, 2003; Radcliff, 2002; Cohen, 2000).

Overwhelmingly, the information security literature emphasizes the importance of methodical and meticulous management as the key to information security and homeland defense (Whitehouse, 2003; Perlman, 2002a; Posner, 2002; Collins, 2001; Willemsen, 2001; Anderson, 1999; McCarthy, 1998; Dalrymple, 1998; Center for Technology & Government, 1997a; 1997b). For example, the U.S. General Accounting Office (1996a) cautioned that the “introduction of newer, faster, cheaper technology is

not a panacea for flawed management practices or poorly designed business processes” (p. 5). The Accounting and Information Management Division of the U.S. Governmentwide and Defense Information Systems (Brook, 2001; 2000) avers that the underlying problem with government information security is poor management. Research by Public Technology Incorporated (2000) found that effective information security is not just a technology issue to be left to the ‘technology people’ but rather requires strategic and business acumen on the part of IT management. Research by West and Berman (2001) conclude that IT officers need to combine their technical expertise with management savvy to successfully work across departments and functional areas to achieve strategic objectives. Further, the Institute for Information Infrastructure Protection (2003) determined that well-designed information security “...require[s] expertise in information management and security technologies, as well as an understanding of policy requirements, business models, and organizational processes” (p. 24).

Fundamentally, information security management involves ensuring that adequate information security tools are properly in place; that staff is trained to use these tools; that enough time is available to use them properly; and that all personnel are held accountable for their information security practices (Computer Science & Telecommunications Board and National Research Council, 2002). Yet it is ultimately more complex as administrators are required to interface with processes and organizations beyond their immediate functional areas. IT security managers must possess a unique understanding of information-related risk and the ability to make prudent decisions on the interaction of many divergent elements, often with incomplete

information (Cohen, 2000). Mark Forman, Chief of Information Technology for the Bush administration, affirms that government IT leaders need to possess three distinct knowledge and skill areas, namely, an understanding of the business of government, an ability to effectively manage resources, and the possession of solid management skills (Frank, 2001). The task then for these individuals is to understand this balance, to understand how to leverage the technology, to understand how to instigate change, and to be able to motivate action up and down the organization. As such, information security strategies lean toward managed progress, rather than natural growth in an attempt to control influences (Mintzberg and Lampel, 1999).

Literature on information management (Cowings, 2001; Center for Technology in Government, 1997a; Moore, 1997; NIST Bulletin, 1995; August, 1994) highlights three responsibilities unique to IT managers, (1) anticipating and understanding technological change, (2) anticipating and understanding information security, and (3) maintaining effective communication between IT and non-IT divisions. Merging these ideas, Everett, Dewindt, and McDade (1997) suggest that managers strategically approach information security as a mosaic, whereby each piece, or element, is understood in terms of the effect on the sum total. This also includes a mindfulness of elements which exist outside of a manager's immediate area of responsibility or authority, such as other organizations with which relations take place. This is perhaps most especially true with regard to government information systems, for as the Center for Technology and Government (1997a) points out, "No government information system stands completely on its own. Each system is implemented in a work environment that includes people, processes, organizational relationships, and other systems" (p. 36). Indeed, the

Intergovernmental Advisory Board (1998) has noted that current approaches to managing governmental information technology are evolving and key among the new approaches is intergovernmental management. Further, Frank McDonough (2002), Deputy Associate Administrator of the U.S. General Services Administration, firmly states that intergovernmental management will be *the* challenge for information security in the next 20 years. He notes several converging conditions which support this position including a Presidential administration focused on improving information security; a demonstrated need to integrate distinct databases to meet homeland security needs; the presence of program overlap between numerous agencies in a time of budget deficits; and the need to acquire/train IT staff after a decade of personnel freezes. Collectively, these conditions point toward the growing importance of integrated systems and collaboration which are at the heart of intergovernmental management.

To appreciate the interplay of these activities as they relate to governmental information security, it is essential to comprehend the nature and theory of intergovernmental management (henceforth, IGM). As such, it is necessary to first understand intergovernmental relations (henceforth, IGR) as they are the bedrock of intergovernmental management. Therefore, the next chapter discusses IGR as an identifiable organizational endeavor at the heart of IGM before presenting contemporary applications of the theory of intergovernmental management in the context of information security.

III. THEORY OF INTERGOVERNMENTAL MANAGEMENT

Intergovernmental Relations

The American system of government is a delicate balance of partnerships between national, state, local, and private bodies (Carlson, 1988; Elazar, 1964). Since inception, this system has been marked by an undercurrent of shared powers and responsibilities rather than merely their separation (Stenberg, 1984). In practice, the distinctions between governments are often blurred whereby no unit truly operates independently (Ellison, 1998). This degree of interdependence requires not only increased levels of transparency and accessibility but also the skillful use of compromise, negotiation, and coordination on the part of intergovernmental partners (Governments Without Boundaries, 2002; Nelson, 2001; Luke & Caiden, 1999; Stenberg, 1984). As such, inherent to the American system of government is the practice of intergovernmental management; however, as a theory IGM is relatively new (Agranoff & McGuire, 2001).

The origins of IGM can be traced to the notion of intergovernmental relations that rose to prominence in the 1930s when the federal government undertook this initiative to reduce the turmoil of the Great Depression via innovative intergovernmental programs introduced as part of the New Deal (Wright, 1992; Macaluso, 1984). Consequently, the term “IGR” came to be associated with liberal, progressive, and

active government ideas that defined that era. However, the first official (statutory) use of the term IGR did not occur until 1953 when Congress created the temporary Commission on Intergovernmental Relations (Wright, 1983). Over time, the subtleties and distinctions of intergovernmental relations continued to evolve and reflect the political movements and events of the day; proving the scope of IGR to be broader than its early characterization.

Differing from traditional federalism, which emphasizes independent levels of government and divided functions (Agranoff & Lindsay, 1983), IGR focuses on relationships between governments which develop in the pursuit of a common goal. However, a review of the literature reveals no singular definition of intergovernmental relations. Therefore, a sampling of several definitions will help to provide a framework from which to begin this discussion. According to Denhardt (1995), IGR encompass “...all the complex and interdependent relationships among those at various levels of government as they seek to develop and implement public programs” (p. 75). Cooper et al. (1998) aver that IGR consists of the connections and competition which characterize the way public sector managers deal with one another and with the body politic. Frederickson (1997) contends that IGR is “the wide range of types of organizations and institutions that are linked together and engaged in public activities” (p. 84). Regardless of how they are defined, intergovernmental activities and partnerships permeate the national landscape as they are utilized to deliver an array of federal, state, and local programs for everything from food stamps to hazardous waste cleanup.

While the breadth of situations for which intergovernmental solutions are employed is vast (Allen, 1994), often, the legal and political incentives for government

units to operate separately are much stronger than the incentives to cooperate. According to interorganizational theory, which focuses on the relations between organizations by looking at interdependencies and strategies (Kickert, Klijn, & Koppenjan, 1997), there are six general drives for relationship formation, namely, out of necessity, to balance asymmetry, for reasons of reciprocity, to increase efficiency, to foster stability, and to produce legitimacy (Oliver, 1990). The decision to pool resources and share authority with another organization is largely based on weighing risks against returns (Powell, Koput, & Smith-Doerr, 1996). The resolution to proceed requires that both the structure and dealings of a proposed intergovernmental relation will respect existing jurisdictional boundaries (Agranoff & Lindsay, 1983). Yet, even when agreements on such matters are reached, Turner (1990) suggests that tension between governments may remain problematic for power sharing near guarantees that relations will remain unstable.

Schiavo-Campo and Sundaram (2001) note that there are only four ways in which IGR are actually created. They are; 1) through formal constitutional change, which redefines the roles and responsibilities; 2) through non-statutory agreements that set out obligations and commitments for specific policy areas, such as the environment; 3) via statutory and binding obligations, such as intergovernmental transfers; and 4) the final way in which most intergovernmental relationships are created is by means of informal agreements among political leaders or managers to undertake a certain course of action. Research (Cooper et al., 1998) has found that regardless of how they are created, intergovernmental or cooperative agreements usually pertain to a single activity; concern services rather than facilities; are not permanent but contain provisions

for future renegotiations or termination; have stand-by provisions that come into effect when certain conditions arise; and are endorsed by higher levels of government.

The Intergovernmental Advisory Board (1998) suggests that intergovernmental collaboration is warranted when "...no single agency or organization has the authority, resources, or expertise to address a problem that cuts across geographic and political boundaries" (p. 7). However, Powell et al. (1996) point out that such collaboration should not be viewed simply as a means to compensate for a lack of internal resources. Rather IGR can be a means to further develop and strengthen the existing internal competencies of an organization as well as "...deepen [its] ability to collaborate, not just by managing relations dyadically, but by instantiating and refining routines for synergistic partnering" (p. 199).

Deil Wright notes that once agreements are reached IGRs bear several fundamental qualities. In his 1982 book titled *Understanding Intergovernmental Relations*, Wright outlined five distinctive features of IGR that still pervade the literature on the subject over twenty years later. First, governmental units of all types and levels participate in IRG activities and relationships. As such, IGR encompass not only the national-state exchanges at the heart of the federalist system but also the essential associations and affairs between national-local, state-local, and interlocal units (Luke & Caiden, 1999; Cooper et. al, 1998; Intergovernmental Advisory Board, 1998; Agranoff & McGuire, 1998). As explained by Wright (1983), "IGR suggests that the U.S. system (singular) is in fact a system of systems (plural)" (p. 423). The second aspect common to IGR is the human dimension. William Anderson (1960) pithily addressed this tenet over 40 years ago when he wrote; "It is human beings clothed with office who are the

real determiners of what the relations between units of government will be” (p. 4). The influential, yet highly amorphous human component includes the attitudes, perceptions, and general aptitude of the individuals occupying positions in the various governmental units (Denhardt, 1995, Gargan, 2000). The third distinctive feature of IGR is that officials regularly interact with officials from other jurisdictions. Whether these interactions are for the purpose of exchanging resources, information, or views, they are not one-time occasional occurrences; rather they underscore day-to-day patterns of contact (Agranoff & McGuire, 1999). Further, these interactions are not capriciously or arbitrarily undertaken but are instead targeted efforts to realize specific aims (Luke & Caiden, 1999; Agranoff & Lindsay, 1983). A fourth mark of IGR is that from Senators to community program directors all public servants are potential participants in intergovernmental processes; whether they simply phone another organization to ask a question or they design an interlocal service delivery system. The fifth and final aspect common to intergovernmental relations is policy. Many researchers (Denhardt, 1995; Ellison, 1998b; Bohte & Meier, 2000; Gargan, 2000) contend that public policy is formulated and achieved in an interactive and intergovernmental context. That is, behind the obvious macro workings of political gears, policy is in large part generated, implemented, and maintained by the micro interactions and activities of governmental officials (Schiavo-Campo & Sundaram, 2001). These actions also include inactions, intentions, discretion, and their combined consequences (Wright, 1983). The melding of these mercurial micro-elements into the backdrop of policy-making often produces an unpredictable environment for practitioners (Ellison 1998b; Denhardt, 1995; Oliver, 1990).

Wright provides a crisp summary of these five distinguishing attributes of IGR in a piece which appeared in the 1983 *Handbook of Organizational Management* (p. 425):

IGR encompasses linkages among all governmental entities in the U.S. political system, emphasizes the human dimension of the cross-boundary relationships, includes exchanges among officials (especially administrators), acknowledges that the exchanges are frequent and follow regular patterns, and incorporates policy or purposive behavior as a prominent element in the study and practice of the field.

While IGRs share these fundamental characteristics, understanding modern IGRs in this country requires understanding that relationships among governmental units are multi-dimensional. Schiavo-Campo and Sundaram (2001) note that each individual intergovernmental arrangement may vary on a number of unique structural traits, such as, whether the relationship coordinates horizontal (peer) or vertical (superordinate and subordinate) groups; is formally mandated or informally voluntary; structurally or procedurally driven; or institutionalized rather than ad hoc. IGRs can also vary in the number of participants (bilateral, multilateral, or regional); the types of participants (bureaucratic, political, private, or nonprofit); or the nature of the interaction (consultative or decision-making). Furthermore, a unit of government may have simultaneous and overlapping relationships with different jurisdictions, at various levels, to address a single issue (Agranoff & McGuire, 2001; Wright 1993).

Despite structural differences between IGRs, successful cooperation and administration can produce several advantages for participating governments, such as; the creation of a united front for building public support for regional programs; increased political power through multi-jurisdictional cooperation; shared liability; consistent laws,

regulations, policies, or practices across affiliated jurisdictions; and efficient management of pooled resources (Cooper et al., 1998). In addition, IGR can create interagency committees to study various issues; launch or coordinate proactive or reactive initiatives; coordinate local developments within the bounds of national or statewide plans; provide ways to lessen overhead through merged planning and administrative requirements; as well as call attention to fiscal, regulatory, and other impacts of pending legislation (Schiavo-Campo & Sundaram, 2001; Stenberg, 1984).

The interdependencies which underlie contemporary policies, programs, politics, and economics connect governmental units more closely than ever before (Gargan, 2000; Agranoff & McGuire, 1999; Wright, 1998). Through intergovernmental collaboration, information, resources, and ideas are exchanged, but for IGRs to be successful, participants must think beyond to needs of their immediate organization and develop a shared vision. Through concerted efforts or simply via frequent and repeated interaction, managers can not only establish rules and patterns necessary for intergovernmental collaboration, but can also develop this important sense of common purpose (Kickert & Klijn, 1997). Cooper et al. (1998) point out that understanding the extent and role of intergovernmental relations facilitates a better awareness of the scope of public administration in the American political system; the type of activities that public officials regularly perform; the major actors involved in the delivery of public goods and services; and the ever-changing administrative structure for addressing critical policy issues. This awareness brings into focus patterns of behavior fundamental to policy development and program administration that are otherwise obscured.

Initiatives that cross government boundaries not only introduce participating organizations to new patterns of cooperative behavior but also to new complexities (Nelson, 2000; Luke & Caiden, 1999). The interdependence born of these relations and initiatives can impede self-governance and complicate administration. Agranoff and Lindsay (1983) note that interdependent governments face challenges arising from overlapping legal and statutory authority; issues of agency autonomy or turf protection; the lack of high-level administrative support for or incentives to coordinate; the lack of perceived independence; and general difficulties in standardizing interjurisdictional procedures. Group Decision Support Systems (2002) points out that cross-agency initiatives often lack a comprehensible connection between vision, strategy, and management. This can be due to several causes such as; the lack of a detailed assessment of the current situation; a lack of clarity of the leader's intent; the lack of continuous involvement of the leaders; fragmentation at the top; a general lack of communication; and/or the initial rationale is no longer relevant.

Underlying these intergovernmental challenges is the need to achieve balance between the autonomy of subnational government units and the federal need to retain control of such units (Schiavo-Campo & Sundaram, 2001). Adding to this complexity, each partnering jurisdiction has its own governance, structure, procedures, and authority (Agranoff & Lindsay, 1983). It is often the case that collaborating governments have different budget cycles, application formats, monitoring procedures, decision-making processes, and reporting procedures. Taken together, these matters force program managers and administrators to contend with some difficult tasks such as, delineating accountability, determining funding obligations, and standardizing

interjurisdictional procedures (Stenberg, 1984; Macaluso, 1984). Addressing these matters and meeting the challenges inherent to intergovernmental programs and policy implementation are of central concern to government managers and administrators. Research (Bolman & Deal, 1999; Luke & Caiden, 1999; Cooper et. al, 1998; Wright, 1992; Agranoff & Lindsay, 1983) has shown that intergovernmental management can provide essential skills, techniques, and direction to minimize these challenges.

Intergovernmental Management

From overlapping authority, to issues of autonomy and turf protection, the intricate issues inherent to operating within and across intergovernmental associations create many challenging tasks for managers. Balancing goals against these complex challenges requires coordination and cooperation between government units. As such, intergovernmental concerns call for intergovernmental management (Gargan, 2000; Agranoff & McGuire, 1998; Kickert & Koppenjan, 1997). According to Wright (1998), the most distinguishing and apparent feature of IGM is its emphasis of the management process. For that reason, it is important to briefly discuss management in the classic sense before addressing the details of IGM.

In the purest form, management has been described as "...the organization and direction of resources to achieve a desired result" (Allison, 1999, p. 16). Yet managing is more complex than just determining a goal and enrolling actors towards achieving that end. Peter Drucker (1973) describes management as "...the organ of leadership,

direction, and decision..." in an organization (p. 17). He explains that management is equally a function, a discipline, and a task to be done. Existing within the dovetail of these roles, management is simultaneously concerned with knowing and predicting the future; being analytic and quantitative; as well as being rational and systematic (Wakeley, 1983). The breadth of these concerns compels, if not requires, managers to be functionally involved in near all aspects of the organization or department under their charge. It involves implementing multifarious strategies, often amid disagreement and under inconsistent conditions, to achieve cooperative solutions that affect both senior and staff elements of an organization (O'Toole, Hanf, & Hupe, 1997).

In a classic piece from 1937, Gulick and Urwick outlined seven general management functions: planning, organizing, staffing, directing, coordinating, reporting, and budgeting. These functions translate into activities such as structuring and designing an organization; setting goals for an organization; and ensuring that goals are met (Kickert, Klijn, & Koppenjan, 1997). Exactly which specific actions fall out of these key management functions depends on a matrix of variables not limited to the character of an organization, decision-making patterns, and the distribution of authority (Allison, 1999; Wright, 1983).

With increasing frequency, managerial activities often need to be carried out across formal legal jurisdictions and involve different public and/or non-profit organizations. The routine occurrence and observance of such interjurisdictional managerial activities is generally referred to as "intergovernmental management" (Intergovernmental Advisory Board, 2003, 1998; Advisory Commission on Intergovernmental, 1996; Mandell, 1979). Like intergovernmental relations,

intergovernmental management has been characterized many different ways causing scholars to acknowledge that there is no set or consensual definition (Wright, 1998; Agranoff & McGuire, 2001). Agranoff & McGuire (2001) posit that the reason for this variation is that, as a term, IGM is "...of recent vintage, specialized usage, limited visibility, and uncertain maturity because it includes so many disparate actions..." (p. 672). Indeed, a review of the literature reveals several descriptions whereby researchers fix upon different components of IGM. Some emphasize the role of managerial activities (Agranoff & McGuire, 2001, 1999, 1998; Bolman & Deal, 1999; Wright, 1998, 1992; Agranoff & Lindsay, 1983; Mandell, 1979); others focus on the importance of strategy and policy (Gargan, 2000; Radin, 2000; Ellison, 1998); while still others highlight structural integration and collaboration (Nelson, 2001; Perry & Kraemer, 1999; Intergovernmental Advisory Board, 1998).

Despite the various points of emphasis, interpreted collectively, IGM is the melding of interorganizational communication, strategic planning, and management actions to achieve collective goals and manage interdependencies that arise from intergovernmental relations. While IGR delineate connections and outline obligations between government units, IGM goes further by employing activities aimed at maximizing goal attainment and minimizing the challenges inherent to these associations. Whereas IGR identifies who the actors are and how they relate, IGM is an action-oriented process that allows administrators at all levels the wherewithal to act constructively (Mandell, 1979). Intergovernmental management provides the capabilities to take useful actions to enable intergovernmental relations to succeed. As such, intergovernmental management is an extension of intergovernmental relations.

Typical IGM actors are managers, such as information technology managers, program officers, and elected officials who are charged with maintaining intricate public programming (West & Berman, 2001; Cooper et al., 1998). However to one degree or another, most public managers and officials have engaged in some form of IGM whether or not they were consciously aware of it (Wright, 1999, 1983; Anderson, 1960). Agranoff & McGuire, (1998) assert that IGM techniques are enacted when three elements converge namely, strategic activity, interdependence, and multiple actors. That is, when conditions are uncertain and complex (requiring strategic activity); when problems and/or solutions have a direct effect on other governments (evidence of interdependence); and when collaborative efforts span multiple governments, sectors, or organizations (multiple actors). Striving to solve problems and meet goals in such an environment requires balancing and accommodating the mercurial political, legal, and technical idiosyncrasies of simultaneous and even conflicting formal relations and informal entanglements. Doing so commonly includes the complex execution of decisions and the mutual adherence to agreements as determined by participants.

In and of themselves, the outcomes of IGM activities generally do not change social structures or eliminate complex problems. The reason is that intergovernmental management is less concerned with macro changes that amend the larger political, economic, and social equilibrium (Radin, 2000; Bolman & Deal, 1999). Rather IGM regards policies, programs, systems, and structure principally as given and concentrates more on "...incremental adjustments in managerial activities that enhance service delivery" (Wright, 1998, p. 420). The foremost objective of IGM is achieving positive results through skillful public management. In practice the "nuts and bolts of

substantive issues” are of principal importance in intergovernmental management (Agranoff & Lindsay, 1983, p. 229). Because of this utilitarian nature, intergovernmental management can be employed ad hoc in response to conditions that arise across affiliated governmental units.

While the unstructured application of IGM techniques are seemingly common, as a developing theory several distinctive functions of IGM have been identified. In the manner of Gulick and Urwick’s 1937 assessment of the general functions of classic management, Wright (1983) identified three general, yet not wholly mutually-exclusive functions of IGM. He posits that the most prominent courses of action in intergovernmental management are 1) problem solving; 2) networking; and 3) providing coping mechanisms.

Problem Solving

Among the tasks common to all managers is to solve problems in a responsive and responsible way (McGowen, 1998; Kickert & Koppenjan, 1997). Yet Wright (1983) suggests that in an intergovernmental context problem solving is more than a task; it is the driving force of all activity. From this vantage, intergovernmental management is “an effort and a process where problem identification and strategies to problem resolution are the guiding notion” (Wright, 1983, p. 431). To be successful, participants must assume a joint-task orientation to problem solving because eventually, technical problems, authoritative issues, and political pressures must be overcome so that working solutions can be produced. Yet rising above these matters to arrive at viable

solutions can be challenging. Research by Ellison (1999) has found that cooperative rather than coercive mechanisms work better when intergovernmental associates share similar objectives. When intergovernmental linkages are grounded in reciprocity they are typically characterized by balance, equity, and mutual support, rather than by force and conflict (Oliver, 1990).

While technological and logistical issues are comparatively easy to resolve, the more thorny points to working intergovernmentally involve bridging different governmental cultures (Nelson, 2001). Among the leading concerns for problem solving within multi-jurisdictional settings are the legally established roles and relationships. Such jurisdictional demarcations regularly connote separate political, fiscal, and bureaucratic systems. To deal with these challenges, IGM actors must proceed slowly, incrementally, and on an issue-by-issue basis to devise jointly-owned solutions. This involves developing "...perceptions of similarities and common concern, relatively open exchange of information, and search and selection of alternatives that benefit more than one party" (Agranoff & Lindsay, 1983, p. 235).

Research by Agranoff & Lindsay (1983), which indirectly explored problem solving as an undertone of IGM, found that intergovernmental collaboration appears to be the most successful when the driving force behind cooperative efforts is developing solutions to specific matters at hand. Keeping the collaborative focus on a common issue(s) instead of on the morass of cooperation imbues efforts with a purposeful directive that appeared to be a particular component of success. Also essential was regular testing and renegotiating of resolutions, as well as the willingness of key actors to make adjustments and even submissions in the service of reaching solutions.

Intergovernmental problem solving often involves extensive 'nuts and bolts' work, such as, in-depth analyses of the current state of a problem, examining similar experiences in other communities if possible, investigating the current and potential role of various partners, and budget permitting, hiring consultants (Nelson, 2001; Radin, 2000; Oliver, 1990). Regardless of the various ways and potential means, for intergovernmental problem solving to be successful eventually decision makers must reach agreement, put it on paper, and implement the resolutions in the relevant jurisdictions. Jurisdictions and the actors representing them should remain focused on real issues while working toward reaching decisions that produce courses of action to ultimately solve problems (Stever, 1993; Stenberg, 1984). According to Agranoff & Lindsay (1983) two of the most important ingredients enabling distinct governments to effectively cooperate are maintaining a consistent focus on the problem at hand and making adjustments to resolve that particular problem.

Through intergovernmental problem solving, government bodies often make arrangements with other governments whereby the solutions require subsequent and regular interaction (Wright, 1990). As such, an essential element of IGM problem solving is coordination. The lack of measured coordination and cooperative interaction can damage, stall, or even halt seemingly well-designed solutions and/or policies during formation or implementation (Schiavo-Campo & Sundaram, 2001). In order for coordination to succeed, intergovernmental initiatives demand an understanding of the needs and wherewithal of all participating organizations (Governments Without Borders, 2002). These insights can be developed and harnessed via networking.

Networking

The swift evolution of communications, transportation, and information processing have connected governments such that the problems and programs of one government can have both immediate and delayed effects on another (Luke & Caiden, 1999). Notions of wholly-autonomous or isolated government operations have been displaced by intricate networks of interdependence. Whether joined through subtle or explicit interdependences, government units at all levels find themselves enmeshed in intentional and unintentional intergovernmental relationships (O'Toole, 1997). Consequently, working within and across multiple intergovernmental relations are now key public management undertakings (Posner, 2002; Frank, 2001; Osborne, 2001). As a result, intergovernmental networking and managing interdependencies have become undeniably more widespread and routine. Therefore, in addition to problem solving, a major function of intergovernmental management is to deal with these network-like circumstances, that is, to navigate interdependencies (McDonough, 2002; Davies, 2001).

Successful management in a world of complex intergovernmental problems, programs, and policies requires that jurisdictions locate actors who possess the additional resources that they need to achieve their goals. To this end, intergovernmental managers will find themselves regularly networking with numerous agencies, managers, and directors to stay abreast of the exploitable strengths and transmittable weakness of each but will only actually collaborate with the ones that can provide targeted or categorical resources (Agranoff & McGuire, 1998). As such, a

critical element in intergovernmental problem solving, and hence goal achievement, is employing networking techniques and strategies to strengthen intergovernmental relationships whereby a jurisdiction is well-positioned to quickly and successfully interact with critically positioned or endowed actors.

Minimizing barriers, such as local political opposition, misunderstandings, and lack of information is a critical component of successful IGM activity (Chi, 2000). Intergovernmental management makes use of networks and networking strategies as positive means with which to navigate intergovernmental relations and interdependencies (Mandell, 1979). Increasingly, public administrators recognize that quality intergovernmental management includes being attuned to the subtleties of partner governments. As such, intergovernmental initiatives should be preceded by a thorough understanding of the needs and capabilities of all participating governments (Nelson, 2001). While developing this insight requires a large investment of time and resources, understanding the challenges and functional realities of intergovernmental allies can clarify misperceptions, which in turn, can augment trust (Dearth, 2000; O'Toole, 1997). As such, whether formal or informal, dealings with intergovernmental partners are just as important as internal dealings from the vantage of intergovernmental management (Denhardt, 1995). Research by Agranoff and Lindsay (1983) found that awareness of partisan issues, differences, ideological stances, and political undercurrents contributed to successful intergovernmental cooperation and coordination.

Networks and networking, within the context of intergovernmental management, should not be confused with network management. Technically, network management

could be an intergovernmental activity if it occurs in a government setting where no single central authority or hierarchical ordering exists. However, in essence, network management is enlisted to maintain structural stability among formally recognized linkages and policy-driven connections (Kickert & Klijn, 1997; O'Toole, 1997). As Kickert & Koppenjan (1997) point out, network management assumes three general purposes, namely, intervening in existing patterns of relations, consensus building, and problem solving. It is important to note that these purposes are in the service of the network; that is to maintain the network. Intergovernmental management, however, enrolls networking strategies and fosters networking connections in situations where multiple stakeholders need to agree on goals and strategies (Luke & Caiden, 1999). As such networking activities, as used via intergovernmental management, are in service of solving an intergovernmental problem rather than in service of general coalition building and maintenance (Agranoff & McGuire, 2001; Wright, 1998; O'Toole, 1997).

Although similar, network management focuses on harmonizing strategies that exist within a set network; whereas intergovernmental management employs networking techniques to foster intergovernmental collaboration to craft joint strategy to address a specific problem or utilize others as resources. Network-oriented techniques which are regularly employed via intergovernmental management include mediation, arbitration, and mobilization (Kickert & Koppenjan, 1997; Oliver, 1990). In practice, these skills translate into such intergovernmental management activities as assessing one's connections to make a rough inventory of principle contingencies and alliances; looking for opportunities to coordinate resources and goals amongst allied governmental units; routinely striving to locate key allies at crucial nodes; and building trust among partner

governments to facilitate intergovernmental cooperation in the interest of solving or coping with problems (Intergovernmental Advisory Board, 1998; U.S. Advisory Commission on Intergovernmental Relations, 1993; Stenberg, 1984).

Coping Capabilities

Whether emanating from federal, state, or interlocal sources, not all intergovernmental policies and programs emerge with stable or clearly delineated procedures to delegate responsibility, allocate resources, or assign authority (Falcone & Lan, 1997). Nevertheless, subnational governments are regularly required to comply with vague policies and implement ill-fitted programs which filter down through the federal system (Agranoff, 2001). Yet local jurisdictions do not just acquiesce to the impulse and wish of state and national leadership and mindlessly adopt policies and programs as they appear (Stever, 1993; Turner, 1990). Rather they strive to adjust policies and programs to best serve their own local social, political, and economical needs (Bohte & Meier, 2000; Cooper et al., 1998; Stenberg, 1984). Sometimes local governments are successful; sometimes they are not.

Coping mechanisms, like such time-honored techniques as bargaining and negotiating, are often used to try to facilitate these adjustments. Yet administrators are not encouraged "...to exercise bureaucratic discretion since their role is believed to be executing policies crafted by legislators" (Chi, 2000, p. 301). At the same time, however, public managers are expected to behave like their private sector counterparts and "...maximize efficiency, engage in risk taking, and gain reputations as entrepreneurs"

(Gargan, 2000, p.649). In an effort to walk this fine line, local managers enroll problem solving techniques and call upon networked allies in other governments and/or offices to make intergovernmental initiatives as effective and productive as possible. However, there are instances and circumstances which can not be 'solved-away' or altered. In such situations, where a policy must be adhered to as is or a program produces unintended negative outcomes, a primary function of intergovernmental management is to provide coping strategies and mechanisms.

Localities often revert to coping strategies when rules, standards, or guidelines in and of themselves function as impediments to the general purposes for which higher level and local managers are working (Agranoff & McGuire, 1998). As such, coping strategies generally attempt to either change official policy/program specifics or seek regulatory/statutory relief, flexibility, or waivers (Radin, 2000; Wright, 1983). Yet as Falcone and Lan (1997) point out, intergovernmental actors from all levels of government routinely draw on an untold number and variation of coping techniques, depending on the assembly of subtle nuances unique to each situation. For example, in one situation an appropriate strategy might involve continuously assessing one's current strengths and weaknesses to avoid unforeseen outcomes; another set of circumstances might call for seeking media attention to invoke public protest concerning, for example, unfunded mandates; or a situation could simply require creating or modifying formal communication structures.

From the perspective of intergovernmental management, coping is fundamentally a management function, whether it entails the implementation of a minor technique or takes the form of a multilateral strategy. Equally, coping can be carried out in isolation

by a jurisdiction, such as to achieve its own ends within an intergovernmental partnership or to serve its unique needs within the bounds of a compulsory program and policy. Field studies conducted by Agranoff & McGuire (2001) found that considerable managerial time is spent engaged in intergovernmental transactions trying to fit local programs into national or state standards, rules, and regulations. In these instances, a jurisdiction might request a suspension or alteration of particular program requirement or regulation; it might attempt to redefine its program as a model or experiment; or it might seek to trade off strict compliance for increased flexibility.

Mounting interdependencies linking legally separate and distinct jurisdictions simultaneously generate problems and opportunities (Luke & Caiden, 1999). Whether used to stave off emerging and seemingly unavoidable problems or to seek a closer fit between policy/programs and localities, coping strategies, as a function of intergovernmental management, are vital to the success and maintenance of intergovernmental relationships and initiatives. Yet, employing coping techniques and mechanisms do more than just accommodate jurisdictional idiosyncrasies; they inadvertently test and refine the details, structure, and overall viability of the very relationships and initiatives they preserve.

By challenging policies, rules, procedures, and relationships, coping strategies enacted via intergovernmental management extend the principle of checks and balances and enliven experimentation and innovation. Radin (2000) expressed a similar sentiment when he wrote that regulatory discretion was not only “a way to meet the unique needs of individuals states, [but] it has also been closely tied to a research and development strategy, providing latitude to non-federal jurisdictions for experimenting

with new innovations and new ways for delivering services” (p. 154). By implementing reactive coping techniques, intergovernmental managers can more effectively and efficiently fulfill mutual goals without a prolonged period of laboring through legislative channels (Chi, 2000). However adaptation and innovation require an investment of time and resources which often works to discourage such endeavors. When these barriers can be overcome, the coping function of intergovernmental management has the ability to generate more mature initiatives and foster progress (Falcone and Lan, 1997).

While presented here separately, the primary intergovernmental management functions of problem solving, networking, and implementing coping strategies naturally overlap in practice. And in recent years, the scope and complexity of these functions have risen significantly due in large part to external circumstances that directly impact the shape of intergovernmental relationships (Governments Without Borders, 2002; Nelson, 2001; Gargan, 2000; Ellison, 1998). Among these influences are the increased prevalence of polices/programs that demand unconventional forms of organization and management; more willingness from federal /state governments to accommodate local conditions; the resurgent role of state governments in creating intergovernmental programs; and finally, increased local sophistication and capacity to work within the larger intergovernmental system. The theory of IGM suggests that navigating these conditions occurs within two distinct planes or environments, vertical and horizontal, with each often employing specific management activities (Schiavo-Campo & Sundaram, 2001; Agranoff and McGuire, 1999; Wright, 1983).

Vertical and Horizontal Environments

The vertical environment includes interactions between lower and higher levels of governments, such as local interacting with state, local interacting with federal, and state interacting with federal (McDonough, 2000; Intergovernmental Advisory Board, 1998). The nature of federalism, combined with a historical perception of inferior local government management, has made vertical the dominant environment in American intergovernmental relations and management (Stever, 1993). In addition, as the federal government oversees the intergovernmental system from the apex of this hierarchy, state and local governments are controlled more than they are controlling and dependent more than they are autonomous (Agranoff & McGuire, 1998).

Vertical interaction is often facilitated by the propagation of national norms, goals, and funding guidelines (Schiavo-Campo & Sundaram, 2001). This 'top-down model' is seemingly predicated on "...the growth of national programming and tipping the balance within the federal system toward executive control, with the federal government somehow "managing" its programs through state and local government managers" (Agranoff & McGuire, 2001, p. 672). Through such vertical intergovernmental management the different levels of government seek to assure top-down policy coherence from lower governments.

In a vertical environment, local governments primarily contact state political entities, such as the legislature; governor; or state agencies (i.e. the Office of Statewide Technology or State Department of Law Enforcement); and federal agencies (i.e. the Federal Communications Commission or Department of Defense) (U.S. Advisory

Commission on Intergovernmental Relations, 1993). Activities mainly include information and discretion seeking behaviors, such as seeking general program information or funding; interpretation of standards or rules; program or project guidance; regulatory relief, flexibility, or waiver; changes in official policy; or technical assistance (Agranoff and McGuire, 2001, 1999, 1998; Intergovernmental Advisory Board, 1998).

The horizontal environment includes interactions among units operating within the same level of government and the corresponding civic levels of nongovernmental organizations (Schiavo-Campo & Sundaram, 2001; Wright, 1998, 1983). Consequently, there are several horizontal planes where interaction occurs, such as between federal agencies; between the government bodies of different states; between agencies within the same state; as well as between local governments, such as counties, townships, special districts, cities. Local horizontal interaction can also occur between local governments and semi-private agencies, such as chambers of commerce, foundations, neighborhood associations; and with quasi-governmental organizations, such as utilities commissions, public-private partnerships, and private industry councils (Leach, 1998).

Horizontal or bottom-up jurisdiction-based IGM activities primarily involve policy/strategy making, resource exchange, and project based behaviors (Nelson, 2001; Agranoff & McGuire, 1999; Cooper et al., 1998; Oliver, 1990). Managing horizontally means working within an interdependent setting and can encompass a broad range of activities, such as building bases of support; agreeing on viable courses of action; developing bilateral or even multilateral coping strategies; engaging in both formal and informal partnerships; joint policy making; pooling resources and integrating differential contributions; consolidating problem solving efforts; employing joint financial incentives;

and acquiring technical assistance (Intergovernmental Advisory Board, 1998; Turner, 1990; Agranoff & Lindsay, 1983).

The initial view of intergovernmental management processes was largely vertical, focusing on how independent state and local governments worked to achieve nationally established objectives (Wright, 1999, 1983; Mandell, 1979; Sundquist, 1969). Historically, certain matters have been determined so significant to national interests that a commanding federal role is generally accepted, such as with issues of controlling contagious disease or defense of critical infrastructures. The vertical environment remains equally dominate in situations where a federal role is deemed necessary because a problem transcends state lines (U.S. Advisory Commission on Intergovernmental Relations, 1996), such as when polluted air from one state traverses another state or when governmental information nodes are poorly secured in one locale, directly affecting the security of all other nodes to which they are networked.

Yet, the last two decades have seen a considerable surge in devolution and the push for increased responsibility among local and state governments (Dilulio & Kettl, 1999; Downs & Murray, 1996; Turner, 1990). While senior political and administrative decision-makers are involved in the creation of formal and informal intergovernmental partnerships, more often, the operational details are left to the operatives (Intergovernmental Advisory Board, 1998). With less federal help, states and localities have been forced to strengthen their own capacities and resources to meet this transfer of responsibility in the face of increasingly complex intergovernmental problems (Radin, 2000; Rivlin, 1999). As a result, the view that vertical situations lead to predominately top-down, federally-dictated arrangements has evolved to recognize that

vertical environments and intergovernmental relations are actually more interactive as subnational governments increasingly make use of techniques and channels to negotiate for their own needs (Cooper et al., 1998; Falcone & Lan, 1997). The tug-of-war over program and policy leadership that has ensued has forced managers to find new ways to balance federal accountability and the discretion provided to state and local governments.

As policy responsibilities between the national and subnational governments have evolved, authority and influence amid the different levels of government crisscross to the point where vertical and horizontal actors often interact simultaneously (Agranoff & McGuire, 2001; Schiavo-Campo & Sundaram, 2001). Consequently, vertical and horizontal relationships often merge, overlap, or at the very least intermingle when issues are complex, such as protecting the critical digital infrastructure. Indeed, the President's Commission on Critical Infrastructure Protection (Allor & Lindley, 2000), U.S. General Accounting Office (20021c), and the Department of Homeland Security (2003) have declared that protecting America's critical infrastructure is the shared responsibility of federal, state, and local government in active partnership with the private sector. Frank McDonough (2002, online), Deputy Associate Administrator of the U.S. General Services Administration, asks government leaders "Can we afford not to collaborate"?

Application of Theoretical Ideas

As a concept, intergovernmental management conveys an enterprise that “...moves beyond federalism's traditional application to a sophisticated contemporary understanding of how the many units of government, at all levels, relate to one another” (Cooper et al, 1998, p. 101). As a model, it progresses beyond the vertical top-down interpretation of the federal system (Rivlin, 1999; Lane, 1999; Dilulio & Kettl, 1999) to capture a polycentric arrangement composed of overlapping and differentiated authorities (Imperial, 1998; Wright, 1988). However, this research does not focus on IGM as either a concept or a model. Nor does it attempt to explore the relative balance of power in the intergovernmental system or how jurisdictions act in response to a shift in absolute intergovernmental powers typical of IGM research. That is, unlike many inquiries into intergovernmental management (Pagano & Johnston, 2000; Radin, 2000; Guess, 1998; Ellison, 1998; Allen, 1994; Stever, 1993), this research does not focus on IGM as a response to the effects of devolution (the substitution of subnational decision making for national decision making), deregulation (reducing regulatory burden on subnational governments), or decrementalism (the gradual reduction of federal program funding) (Leach, 1998; Turner, 1990). Empirical studies that have approached IGM from these perspectives have generally concentrated on the diffusion and management of new responsibility through variable incentives, obligations, and controls; or focused on how IGM is employed with regard to specific programs which have local impact, such as community development block grants or general revenue sharing.

Instead this research investigates the prevalence of intergovernmental management activities, specifically, the prevalence with which county-level Information Technology Directors use such activities in securing critical digital infrastructure systems under their charge. This focus is grounded in several theoretical notions discussed in the previous chapter. First among these is that managers foster intergovernmental relations for reasons including necessity, to promote stability, or to increase efficiency (Oliver, 1990). Literature on information security (McDonough, 2002; Posner, 2002; Davies, 2001; Osborne, 2001; Tritak, 2001a; Willemsen, 2001) regularly highlights these very conditions to motivate managers and leaders to develop cooperative relationships, thereby removing interorganizational communication barriers enabling the sharing of best practices.

The second theoretical notion being applied to information security is that IGM is the application of such broad activities as problem solving, networking, and coping strategies to maximize goal attainment and minimize the challenges inherent to intergovernmental interdependencies (Agranoff & McGuire, 2001, 1998; Nelson, 2001; Bolman & Deal, 1999; Perry & Kraemer, 1999; Intergovernmental Advisory Board, 1998; Wright, 1998, 1992; Agranoff & Lindsay, 1983; Mandell, 1979). Successful intergovernmental management involves governments working with other governments through informal networks or formal partnerships. Success largely depends on participants sharing a common vision and working together under some sort of agreement (Intergovernmental Advisory Board, 1998). This is especially true of information security. Yet developing the coordination capabilities needed to effectively deal with threats to the critical digital infrastructure is complex and challenging (Brock,

2001a). It involves building trust so that information can be openly shared and difficulties can be candidly addressed (Dearth, 2000; O'Toole, 1997). It requires that IT managers not only know their interdependencies but also foster the relationships behind them (Critical Infrastructure Assurance Office, 2000).

This is essential for several reasons, for instance, the Center for Technology in Government (1997b) notes that traditional government services once provided by a single agency are giving way to complex service programs that require more intricate exchanges of information. These services increasingly necessitate networking and innovative management (Monroe, 2002; Nye, 2002). Additionally, as Osborne (2001) points out, emergency preparation, contingency planning, and risk management are most durable when grounded by a unified decentralized strategy. However, for such a strategy to work there must be a nurtured communication network between leaders and relevant managers (Posner, 2002; Collins, 2001; Tritak, 2001a). Finally, as pointed out by the Forum of Incident Response and Security Teams (2002), information security incidents do not respect geographical or administrative boundaries therefore; management must be prepared to instantly interact with other governments, agencies, and at the very least departments to contain a system breach. The lack of good communication breeds confusion, poor coordination, and frustration (Center for Technology and Government, 1997a). As such, this research is interested the extent county IT Directors and their staffs use intergovernmental networks.

Problem solving is an ever present activity in information security. As the Center for Technology and Government (1997a) points out, sometimes the best solution is found in the common sense and practical experience of the managers involved. In other

cases, as West and Berman (2001) note, information technologies present challenges that necessitate employees and managers from different departments, fields, or organizations to work together in an informal manner. Additionally, fiscal hardships have spurred many local governments to find ways to pool resources on technology initiatives and share data (Monroe, 2002). Whatever the case, the nature of information security provides many opportunities for managing relationships, work, and problems in novel ways. From the vantage of information security, intergovernmental management is “an effort and a process where problem identification and strategies to problem resolution are the guiding notion” (Wright, 1983, p. 431).

Throughout the literature on IT (Institute for Information Infrastructure Protection, 2003; National Institute of Standards and Technology, 2003; Miller & Gregory, 2002; Dacey, 2001; Information Assurance Advisory Council, 2001; Wulf, 2001; McCarthy, 1998; Everett, Dewindt, and McDade, 1997; Fraser, 1997), several management activities are regularly suggested as means to solve problems specific to information security. These include seeking technical and/or non-technical assistance; seeking legal/policy guidance; seeking funding/resources; seeking information related to information security programs; re-negotiate resource sharing/obligations related to an information security agreement; and re-negotiate roles, duties, or procedures related to an information security agreement. These activities are the focus of this research.

Like problem solving, coping activities are an ever present activity in information security. Often local governments must comply with one-size-fits-all directives and instructions from state and federal agencies (Center for Technology and Government, 1997a). Practices that are suitable in one county may be very unsuited to another.

Making intergovernmental endeavors even more difficult, IT managers often have to simultaneously straddle federal, state, and local electoral, budgetary, and legislative cycles. To better deal with these and other challenges inherent to information security in an intergovernmental setting, managers often seek out coping mechanisms from network peers (Institute for Information Infrastructure Protection, 2003; Collins, 2001; U.S. General Accounting Office, 2001b). In that no individual government manager is likely to change these systemic and environmental conditions, by pooling experiences and sharing best practices negative consequences can be ameliorated via well-targeted coping actions such as seeking regulatory or strategic flexibility; seeking legal/policy guidance; seeking funding/resources or information on information security programs (Frank, 2002; Hecker, 2002; Intergovernmental Advisory Board, 1998).

The third theoretical notion being applied to information security is that navigating intergovernmental relations occurs within two distinct planes or environments, vertical and horizontal, with each often employing specific management activities (Schiavo-Campo & Sundaram, 2001; Agranoff and McGuire, 1999; Wright, 1983). The breadth of concerned vertical and horizontal stakeholders quickly transform digital infrastructure protection into a slippery political quagmire. To begin with, there are information security managers and directors; security specialists and staff; systems analysts; network managers, administrators, and engineers; webmasters; and technical engineers. Beyond this technical realm are such state/local intergovernmental players as mayors, council members, county commissioners, city managers, elected officials, public-private partnerships, chambers of commerce, local utilities, private industry councils, regional initiatives, community networks, senior executives, appointed administrators, careers

service managers, and citizens. Even beyond these horizontal actors are state legislators, governor's office, congressional members, lobbyists, state agencies, federal agencies, the military, and the President.

As outlined in the previous chapter, there are several vertical levels of government actors. This research looks at how county IT Directors/staffs interact with federal and state agencies above them and sub-county jurisdictions (i.e. cities, townships, special districts) below them (McDonough, 2000; Intergovernmental Advisory Board, 1998). Also discussed in the previous chapter is that governments horizontally interface with external contemporaries (i.e. a county interacting with another county). Additionally, they horizontally interact 'intra-governmentally' with peer departments and offices within their own government. Further, the interaction between sub-state governments (i.e. county and local governments) are often treated horizontally. This research will explore how county IT Directors and staffs engage in each of these vertical and horizontal relationships with regard to several intergovernmental management activities.

Whether enacted vertically or horizontally, evidence suggests that intergovernmental management activities are not merely 'add-on' or 'special tasks' but rather routine administrative functions carried out by managers operating within the intergovernmental system (Cooper et al., 1998; Ellison, 1998; Allen, 1994; Wright, 1983). Such intergovernmental approaches are necessary when no single agency or organization has the authority, resources, or expertise to address a problem that cuts across geographic and political boundaries (Intergovernmental Advisory Board, 1998). The intergovernmental hurdles associated with information technology and security are

often cited as challenging and complex (Forman, 2003; Dalton, 2002; Collins, 2001; Cowings, 2001; Center for Technology in Government, 2000). Many long established rules and roles must be reassessed according to new and often confusing technologies and emerging laws. Questions quickly surface as to who has the power to determine and dictate procedure.

Consider for example, a sample of federal computer intrusion cases being tried during 2000 under computer crime statute 18 U.S.C. §1030 revealed that 94 percent of these crimes were interstate or International in scope (CCIPS, 2000). As such, each case has a unique array of variables that involve an assortment of stakeholders and public agencies representing different jurisdictions often with competing objectives and different levels of resources. The Institute for Information Infrastructure Protection (2003) asks the question "...who is responsible for security in this information infrastructure "commons" and who should pay for it" (p. 51). In a case of political equals, whose laws or procedures are ultimate, for example, Arizona or Vermont? Turkey or Austria? The broad array of issues facing leaders and managers include jurisdiction-specific problems, rules regulations, policies, agreements, mandates, funding, discretion seeking, legitimacy, consensus building, partnerships, task forces, conflicting priorities, and clashing authority, to list but a few.

Compared to addressing technological issues, many consider the details of working intergovernmentally to secure cyberspace more challenging (Collins, 2001; Willemsen, 2001; Center for Technology in Management, 2000). McDonough, (2000) points out, "The risks of failure are greater, and turf issues can be horrendous. The incentive system to encourage collaboration does not exist" (p. 5). The

Intergovernmental Advisory Board (1998) writes, “There are no structural elements in place that encourage different levels of government to work together. Project participants are often volunteers, coming from varying backgrounds, who work in organizations that have different pay scales and reward systems” (p. 7). And the Center for Technology in Government (1997b) notes,

There are very few incentives for staff to look outside their program boundaries to share responsibility or information or to integrate their operations with related programs. Even in the same agency, programs usually serve to divide rather than connect groups of people with similar responsibilities (p. 14).

Yet the U.S. General Accounting Office (2001c) avers for infrastructure protection to succeed, “It is critical that all participating federal, state, and local agencies interact in a seamless manner” (p. 31). Equally, Symantec (2000) urges governments to engage in partnerships and improve interorganizational communication and information sharing. Similarly, Tritak (2001a) notes that sharing information is necessary for technology managers “...to obtain a more accurate and complete picture of their operational risks, as well as acquire the techniques and tools for managing those risks” (p. 5). Each of these suggestions or activities is intergovernmental in scale and management in application. Each involves bridging different governmental cultures to solve problems, network, and develop coping skills; the activities at the heart of intergovernmental management.

Given the importance of critical digital infrastructure protection, this current research takes a close look at the use of intergovernmental management activities and interorganizational communication as they play such an important role in protecting

information systems (White House, 2003; Computer Science & Telecommunications Board, and National Research Council, 2002; Information Assurance Advisory Council, 2001; McCarthy, 1998). To that end, this research seeks to answer the questions: 1) which IGM activities do county IT Directors/staffs most often engage in on behalf of information security and critical digital infrastructure protection; 2) do county IT Directors/staffs make more use of vertical or horizontal IGM relationships on behalf of information security and critical digital infrastructure protection; 3) is there a relationship between office/county demographics and the IGM activities its IT Directors/staff most often engage in on behalf of information security and critical digital infrastructure protection? By discovering the intergovernmental management activities county managers use to secure the information systems comprising our critical infrastructure, we will be in a better position to understand our defenses and better protect ourselves from the largely invisible threats of cyberspace.

IV. METHODOLOGY AND DATA COLLECTION

As the of role intergovernmental activities in county level information security has yet to be studied, this investigation is exploratory. According to Stark and Roberts (1998), exploratory research is speculative whereby researchers "...make systematic observations of uncharted and little known phenomena in order to get an initial sense of what is going on" (p. 17). Babbie (1995) notes that while exploratory studies seldom provide complete answers to research questions; they are, however, instrumental for providing insight into relatively new and unstudied subjects and serve to direct future research. Therefore, the goal of this study was to take the first step, in what will hopefully be a series, toward building a body of knowledge aimed at understanding county level information security to better protect local elements of the critical digital infrastructure.

Observation Unit and Study Population

The observation unit for this research was county government. As discussed in the introduction and literature review, despite the noted efforts of many counties across the nation (Barrett, Greene, & Mariani, 2002; Monroe, 2002; Posner, 2002; Gonzales, 2001), poor information security remains rampant among these units of governments (Kous, 2003; Leazer, 2003; Perlman, 2002b; O'Connell, 2003; Brock, 2000; Dacey,

2000; PDD-63, 1998; Smith, 1998; Crescenzi, 1996). As such, the information security of these governments continues to be a concern among security experts yet it remains largely unexplored (Misra, 2003; American City & County Magazine, 2002; Barrett, Greene, & Mariani, 2002; Public Technology Inc., 2002; Gilmore Commission, 2001).

For this research, IT Directors functioned as county representatives. IT Directors, also known as Information Technology Managers, Chief Technology Officers, or Chief Information Security Officers are generally charged with technology planning; applications development; establishing strategic relationships with key IT suppliers and consultants; and IT staffing and training (CIO Magazine, 2002; Gartner Group, 2002; Perlman, 2002a). As such, they are often the most knowledgeable of all aspects of an organization's information technology and security efforts and therefore the most qualified to comment on the activities which their organization engages.

Specifically, the target population chosen for this research was IT Directors responsible for constitutional offices in Florida counties, namely; the Board of Commissioners Office, Clerk of Courts Office, Property Appraiser's Office, Sheriff's Office, Supervisor of Elections Office, and Tax Collector's Office. The population was expected to range between 66 Directors (where one IT Director is responsible for all county constitutional offices) to 396 Directors (where a separate Director is responsible for each constitutional office). However, a complete population list was not found to exist, so during October 2003 the researcher developed one from information provided by county Human Resource Departments, as 'key informants'. Key informants are individuals identified by a researcher as possessing unique knowledge on the subject under study or some other distinctive information (Babbie, 1995; Kumar, Stern, &

Anderson, 1993). Curtin (2003) describes a key informant a subject who is tapped to help gain access and guide data gathering.

Among the advantages associated with the use of key informants is that the information gathered comes directly from individuals who are deemed competent to speak on the topic of concern (Day, Blue, & Peake-Raymond, 1998). In addition, by employing a key informant approach it is possible to acquire rich information from relatively few individuals. Often used in qualitative research, a limitation with relying on key informants occurs when the role or experience of the informant is not closely associated with the phenomena under study (Kumar, Stern, & Anderson, 1993; Denzin, 1989; 1970). Thus, the quality of the data acquired is dependent upon how knowledgeable and objective the key informants are (Day, Blue, & Peake-Raymond, 1998). Given that county Human Resource Departments are specifically charged with maintaining an accurate record of current and past employees (Volusia County Government Online, 2003; Bay County Online, 2001; Hernando County Online, no date); they possess the unique knowledge sought after, thus minimizing the chief limitation of using key informants.

To develop a population list, the researcher visited all county websites to obtain contact information for the various IT Directors. When this information was not available on the website but an email address was listed, these offices were emailed weekly for four weeks and asked to provide contact information for their IT director. The researcher telephoned offices for which no email address was attained. In many instances, it was necessary to make several calls to the same office to clarify email responses or obtain missing information. Attempts to collect contact information stopped after a total of four

weeks. The final number of constitutional offices for which the researcher obtained contact information was 255 or 64.4 percent of the total 396 possible (see Table 1).

Table 1: Sampling Frame Development

Total Florida County Constitutional Offices	396
Offices that did not provide contact information for the IT Director	-63
Offices that outsource their IT needs	-72
Offices that declined to participate outright	-6
Sub-total	255
IT Directors responsible for more than one office	33
Final list of unique IT Directors included in this study	222

Variable Operationalization

To investigate the three broad research questions of this research (see the end of the previous chapter), several conceptual definitions were operationalized. It is important to point out that many ethical considerations inevitably arise when studying information security and critical infrastructure protection. In that these research findings will be available to the public, concerted attention was given to selecting which aspects of information security to explore. In an effort to avoid revealing vulnerabilities or jeopardizing confidentiality, this inquiry probed only for the frequency that select activities are conducted. For this research, frequency was defined as:

Frequency: the rate at which a condition occurs in a defined time period.

It was operationalized using an established five-point Likert scale adopted from the General Social Survey (1998). The ordinal scale is as follows- “weekly”, “monthly”, “several times a year”, “a few times a year”, and “never”.

The first question of this research endeavor was “which intergovernmental management activities do county IT Directors/staffs most often engage in on behalf of information security and critical digital infrastructure protection”. The concepts addressed by this question were intergovernmental management activity and information security which were defined as:

Intergovernmental Management Activity: a problem solving, networking, or coping activity that melds communication and management to achieve goals and manage interdependencies that arise from intergovernmental relations.

Information Security: actions taken to reduce the probability that a threat will exploit a system vulnerability. This includes measures to ensure confidentiality, integrity, and availability of system assets.

Intergovernmental management activity was operationalized into eight activities regularly cited in the literature as fundamental to information security management (see Chapters II and IV). These activities were: seek technical assistance; seek NON-technical assistance; seek information on an information security program or project; seek funding or resources to improve information security efforts; seek legal or policy guidance regarding information security; seek regulatory or policy flexibility regarding information security; attempt to modify duties or procedures of an established partnership/agreement relating to information security; and attempt to modify resource-sharing or funding obligations of an established partnership/agreement related to information security.

Although a defined concept in this research, information security was not explicitly operationalized for this study. This was because this research did not attempt

to directly measure the state of county information security but rather only the use of intergovernmental management activities for the purpose of information security. Therefore, as noted above, the concept of “intergovernmental management activities” was operationalized as “intergovernmental -information security- management activities”.

The second question of this research was “do county IT Directors/staffs make more use of vertical or horizontal intergovernmental relationships on behalf of information security and critical digital infrastructure protection”. The new concepts addressed by this question were vertical and horizontal intergovernmental relationships which were defined as:

Vertical intergovernmental relationships: interactions between lower and higher levels of governments.

Horizontal intergovernmental relationships: interactions between governments operating at a similar level.

In that the unit of analysis was county, vertical relationships were operationalized as occurring with: federal units (any office, agency, or department, such as Federal Bureau of Investigation, Federal Emergency Agency, Department of Homeland Security, Computer Emergency Response Team, et cetera) and with state units (any office, agency, or department, such as Florida Department of Law Enforcement, State Technology Office, Secure Florida, et cetera). Horizontal relationships were operationalized as occurring with: other Florida counties (any office or department located in county government different than the respondents, such as another county's Department of Information Technology, Clerk of Court office, Sheriffs Office, et cetera);

other governments located within the jurisdiction of the respondent's county (any part of a government unit located within the jurisdiction of the respondents county, such as a city or township et cetera); and with other departments within the respondent's own county government.

The third question of this research asked whether there is a relationship between county demographics and the intergovernmental management activities county IT Directors/staffs most often engage in on behalf of information security and critical digital infrastructure protection. The new and wide-ranging concept introduced by this question was demographics which was defined as:

Demographics are measured characteristics or attributes used to define a population.

For this research, demographics were operationalized in two ways. First, to provide for a more rich analysis, select county data publicly available from the U.S. Census Bureau (2003) was added into the dataset. The specific attributes were: County Population; Percent of Persons in the County with a Bachelor's Degree or Higher (age 25+); and the Level of Intergovernmental Revenue Received by the County. Second, to capture attributes specific to each county IT department, the survey probed for unique demographic information. Demographics specific to each county IT departments were operationalized as: the county units that fall under the IT Director's supervision for their information security needs for; the online services provided by the county itself, outsourced, or not provided at all; the perceived adequacy of funding the IT Director is able to apply core information security needs; the percentage of the IT Director's duties that focus on information technology or information security related issues; and finally,

the number of employees the IT Director supervises whose job deals only with information technology or information security.

This study also attempted to measure two different dimensions of the respondents' intergovernmental relationships. These dimensions were relationship 'importance' and 'degree developed' which were defined as:

Importance: Strongly affecting the course of events or the nature of things; significant.

Developed: Caused or influenced to acquire a more advanced or mature role, function, or form.

Relationship importance was operationalized as how important each type of intergovernmental relationship is to the success of the county's information security efforts. It was measured with the following five-point Likert scale adopted from the General Social Survey (1998), "Extremely Important", "Very Important", "Important", "Somewhat Important", and "Not Very Important". Degree of relationship development was operationalized as how developed the relationship between the county's IT department and each of the five types of governments/departments. It was measured with the following five-point Likert scale, also adopted from the General Social Survey (1998), "Extremely Developed", "Very Developed", "Developed", "Somewhat Developed", and "Not Very Developed".

Research Instrument

The tool of this research was a self-administered Internet survey which was emailed to respondents. As one of the most frequently used social scientific research technique, surveys are used to make descriptive assertions about particular populations (Leedy & Ormond, 2001; Stark & Roberts, 1998). They are particularly appropriate in situations where the phenomena under investigation are not accessible via direct observation (Frankfort-Nachmias & Nachmias, 1992). Self-administered surveys are best used in situation where respondents are perceived to possess accurate, ready-made answers that they can recall and would be willing to reveal (Dillman, 2000). All respondents were surveyed at essentially a 'point in time' giving this research a cross-sectional design (Singleton & Straits, 1998).

There are several benefits of conducting this research with the aid of the World Wide Web. First, because IT Directors are technology workers in addition to managers, administering the questionnaire to them in a format they are comfortable with, electronic, was an attempt to increase the response rate. Second, using email to distribute the URL of the survey and the Internet to host the survey was also intended to increase the response rate as individuals working out of town or from home were able to receive and complete the survey if they checked their email. Third, using the Internet helped to expedite the distribution and collection phases of data gathering. Fourth, like traditional mail surveys, email surveys are not beholden to geographic restrictions enabling access to dispersed populations. A fifth benefit was that by gathering data electronically, responses were automatically entered as raw data into an aggregate flat

data file which was imported into statistical software for analysis. By collecting and compiling data this way, human error which can occur during data entry (Babbie, 1995) was removed, thus producing a cleaner, more precise dataset.

The survey instrument was developed using the commercial survey service SurveyMonkey.com. Using established and proven survey-software increased the ease and accuracy with which the survey was circulated, completed, and the data was compiled. The software also tracked in real-time which respondents completed the survey and which had not. This allowed the researcher the ability to target only non-respondents for follow-up contact.

Data Collection and Response Rate

Data collection employed a multiple contact strategy (Dillman, 2000) involving four steps. First, a personalized introductory letter (see Appendix A) was mailed to the 222 unique IT Directors during the first week of November 2003. The letter introduced the purpose of the study, expressed the need for their participation, and provided contact information. It also alerted them that in one week they would receive a email from "infosec@mail.ucf.edu" which would include a hyperlink to the online survey.

Enclosed with the letter was an information sheet containing research details written with language accessible to participants (see Appendix A). According to the University of Central Florida Institutional Review Board (2003) providing participants with all the information they might reasonably need to know about a research endeavor

is one of the principal researcher's primary ethical responsibilities. Once participants have been advised of their role and rights with regard to a study, it is necessary to formally obtain their voluntary agreement to participate. Collectively these two steps are referred to as the informed consent process. Specifically, that is "...the process through which potential research participants are provided with all the information reasonably needed for them to decide whether to participate. The process additionally provides for obtaining voluntary agreement to participate in the research" (University of Central Florida Institutional Review Board, 2003, p. 7).

The second stage of contact occurred one week later, when a personalized email was sent to each IT Directors (see Appendix B). It briefly reintroduced the research, listed contact information, and provided a direct hyperlink to the online survey. Additionally, as part of the informed consent process, the email explained that the survey begins with a detailed disclosure of the research procedures and is directly followed by a question asking whether they have read the details and voluntarily agree to participate. They were informed that if they agree to participate, they must check a box before they begin the survey (see Appendix C). This was included in the email in an effort to lessen the likelihood that they would be confused by this section of the actual survey.

Third, one week later, IT Directors who had been identified as non-respondents were sent a follow-up email (see Appendix D) reminding them of the value of the research and again providing a direct hyperlink to the online survey. Fourth, and lastly, the following week, the remaining IT Directors who were identified as non-respondents

were sent a second follow-up email (see Appendix E) asking for their participation. The survey remained online until the second week of December 2003.

During data collection, several emails were returned undeliverable due to inaccurate addresses. While most were subsequently corrected and resent, the researcher was unable to obtain working emails for 13 IT Directors, resulting in a final sample size of 209. Of the 209 IT Directors contacted, 125 completed the survey for a response rate of 59.8 percent. The 125 respondents indicated that they were ultimately responsible for the IT needs of 149 different constitutional offices as 23 respondents, or 18.4 percent, supervise two or more offices. As such, this response rate represents 37.6 percent of the total 396 constitutional offices in Florida.

Further, the respondents represent 52 different counties or 78.8 percent of the 66 counties included in this study. The 14 counties for which there was no representation were: Bradford, Calhoun, Franklin, Gadsden, Glades, Gulf, Hamilton, Holmes, Jackson, Okeechobee, Taylor, Wakulla, Walton, and Washington (see Figure 1).

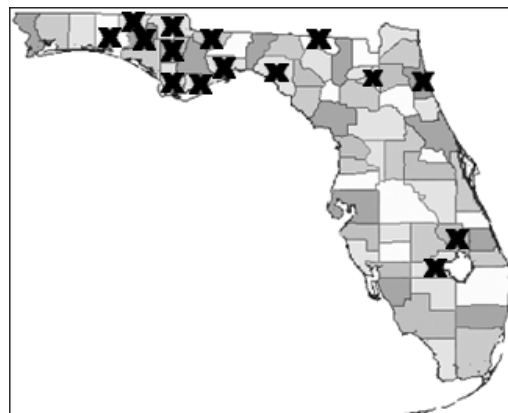


Figure 1: Florida Counties with No Representation in this Study

Independent Variable Coding

As the majority of the absentee counties cluster in the panhandle, a new independent variable “ZONE”, based on the US Army’s emergency and auxiliary communications program MARS (US Army, 2004), was introduced (see Figure 2). The goal of creating a variable that clustered counties by regions was to illuminate underlying qualities and influential factors not readily perceptible via the standard demographics already included in this study, such as population. For instance, does any particular zone exhibit unique patterns in intergovernmental contact? If so what similarities exist among the counties in that zone versus counties in other zones?

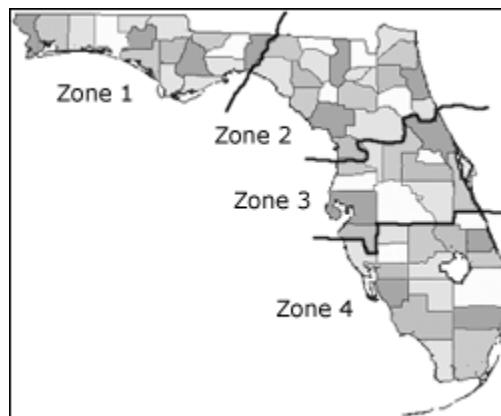


Figure 2: Florida Counties by U.S. MARS Zones

By including this variable, the researcher attempted to capture characteristics and behaviors potentially unique to counties in Zone 1 even though this area was under-represented (see Table 2).

**Table 2: Frequency for Independent Variable:
Which zone is the County in**

Zone	Cases	Percent
Zone 1	14	11.2
Zone 2	33	26.4
Zone 3	39	31.2
Zone 4	39	31.2
N = 125		

Additional inspection of the data revealed an overlap in supervisory status among several respondents. Specifically, as already noted 23 respondents indicated that they supervised two or more offices (see Table 3).

**Table 3: Frequency for Independent Variable:
“OFFICENU” (Number of Offices Supervised)**

Number of Offices	Cases	Percent
1 office	102	81.6%
2 offices	12	9.6%
3 offices	4	3.2%
4 offices	2	1.6%
5 offices	5	4.0%
All 6 offices	0	0%
N = 125		

Twenty-one of these 23 respondents were responsible for the Board of Commissioners Office plus another office(s), generally the Clerk of Court (14 cases) or the Supervisor of Elections (11 cases). In only four instances did a respondent indicate that s/he was responsible for a Sheriff’s Office in addition to another office. To control for effects from overlapping responsibility, two independent variables were created. The first variable “OFFICE” was created to include only the 102 respondents who supervise

a single constitutional office (see Table 4). This categorical independent variable was later used to detect difference between the six types of offices.

**Table 4: Frequency for Independent Variable:
“OFFICE” -Which Office do you Supervise**

Board of Commissioners	11
Clerk of Court	16
Property Appraiser	15
Sheriff	30
Supervisor of Elections	12
Tax Collectors	18
	N = 102

The second independent variable “Number of Offices” was created dichotomously to capture differences between respondents who supervised two or more offices (23 cases) versus those who supervise a single office (102 cases). The full dataset of respondents was then used to create six dichotomous independent variables to capture specific differences between each individual type of office supervised versus all others (see Table 5).

Table 5: Frequencies for Dichotomous Independent Variables for Type of Office Supervised (N’s = 125)

Variable	Yes/No
Board of Commissioners	32/93
Clerk of Court	30/95
Property Appraiser	24/101
Sheriff	23/102
Supervisor of Elections	34/91
Tax Collectors	28/97

As noted earlier, county data collected from U.S. Census Department and the state of Florida were incorporated into the final dataset to function as

independent/control variables. Again these independent variables were County Population; the Percent of Person's in the County (over 25) with a Bachelor's Degree or Higher; and the Level of Intergovernmental Revenue Received. Univariate analysis using Kolmogorov-Smirnov tests for normality in conjunction with normal probability plots (normal Q-Q plots) consistently revealed non-normal distributions due to severe positive skews in the data. Efforts to correct the variables via data transformations either failed or masked the true meaning of the data. For example, many county characteristics, such as population, are not normally distributed across Florida counties. Since transforming the variables or removing outliers only distorted the data, the researcher successfully opted to minimize the skew by recoding each continuous variable as ordinal. In an effort to maintain the true sense of the data, and thus the real difference between counties, each variable was recoded into groups following natural breaks in the data while trying to balance equal groups of cases (see Table 6).

Table 6: Independent Variables Recoded as Ordinal from the U.S. Census and State of Florida

Variable	Groups	Cases	Percent
Population (2000)	99,999 or less	30	24.0%
	100k – 199,999	34	27.2%
	200k – 499,999	41	32.8%
	More than 500k	20	16.0%
Percent of Persons w/ a Bachelor's degree or higher, age 25+ (2000)	14.9% or less	41	32.8%
	15 – 22.9%	42	33.6%
	More than 23%	42	33.6%
Total Intergovernmental Revenues: Federal, State, and Local (Fiscal Year 2000)	11.9 million or less	29	23.2%
	\$12 – 24.9 million	34	27.2%
	\$25 – 74.9 million	35	28.0%
	More than \$75 million	27	21.6%

Data gathered from survey responses were used to form three additional independent variables. The first measured the percent of the IT Director’s duties that focus on IT related issues (PERCENT; N=124). The original question provided six possible options (100%; 80%; 60%; 40%; 20%; and less than 20%), however, in effort to lessen the negative skew present in this response distribution, the final three categories (40%; 20%; and less than 20%) were collapsed in “40% or less” (see Table 7).

Table 7: Percent of Duties Focused on IT Related Tasks

Percent of Duties	Cases	Percent
40% or less	22	16.7%
60%	16	12.8%
80%	39	31.2%
100%	47	37.6%
N = 124		

The second variable measured the number of employees, whose job only supports IT, that the Director supervises (SUPERVIS; N=124). The original responses options were “0,” “1,” “2”, ...to “25”, and finally “more than 25”. Again to lessen the effects of a non-normal distribution of responses, the variable was recoded as ordinal (see Table 8).

Table 8: Number of Employees Supervised (N=124)

Employees	Cases	Percent
0	27	21.6%
1-4	41	32.8%
5-14	27	21.6%
15 or more	29	23.2%

The final independent variable derived from the survey was a composite, or index variable. Specifically, a composite variable is created by summing several indicators to produce a single scale of measurement (Rowe, 2002; SPSS, 1999; Hair et. al, 1998). Often indicators are selected because they are found to be statistically correlated via such data reduction tests as factor analysis with Cronbach's Alpha test for reliability. However, these tests assume normally distributed data. Univariate analysis of the pertinent factors using Kolmogorov-Smirnov tests for normality followed by visual inspections of probability plots consistently revealed non-normal distributions. Therefore, tests of reliability were inappropriate for creating this index variable.

While the use of statistical test to extract factors is desired, developing theoretical grounded composites variables is an acceptable alternative (Borsboom et. al, 2003; Wollman, 2002) hence this third variable was created to measure the adequacy of funding for several core IT needs (IBUDGET; N=79). This variable summed seven questions (see Table 9) that were all measured "Above Adequate" (=1), "Adequate" (=2), "Below Adequate" (=3), and "Far Below Adequate" (=4), with the additional option "Not Applicable" (=5). Respondents who did not answer all seven questions or who selected the option "Not Applicable" for any question were excluded from the index.

Table 9: Questions Used to Create the Independent Index Variable “Adequacy of Budget”

QUESTION:
How adequate is the funding you are able to apply to each of the following needs:

	Above Adequate		Adequate		Below Adequate		Not Adequate	
IT equipment/ software/ hardware	6	4.9%	87	71.3%	20	16.4%	8	6.6%
IT security equipment/ software/ hardware	8	6.4%	73	58.4%	26	20.8%	11	8.8%
Hiring outsource vendors	0	0%	68	54.4%	20	16%	10	8%
Hiring IT personnel and support staff	2	1.6%	65	52%	32	25.6%	12	9.6%
Training IT personnel	2	1.6%	68	54.4%	39	31.2%	7	5.6%
Computer security education for NON IT employees	0	0%	43	34.4%	40	32%	15	12%
Risk assessment/ management	1	0.8%	55	44%	43	34.4%	10	8%

However, in order to construct a more logically intuitive index, it was first necessary to recode the variables to reverse the scores. The resulting scale ranged from a summed score of 7, indicating the respondent perceived available funds to be far below adequate for all IT needs, to a summed score of 28, indicating that the respondent perceived their budget to be above adequate for all IT needs. To use this index variable to test for group difference, it was necessary to recode the summed scored as ordinal (see Table 10).

Table 10: Independent Index Variable for “Budget Adequacy” Recoded as Ordinal

Index Score	Groups	Cases	Percent
7-11	Far Below Adequate	6	4.8%
12-16	Below Adequate	22	17.6%
17-21	Adequate	46	36.8%
22-28	Above Adequate	5	4.0%

An additional index variable was to be created from a series of eight questions regarding which online services were provided by the office (see Table 11). Specifically,

response options were “provided by the county itself”, “outsourced”, or “not provided at all” with an additional option of “Do Not Know”.

Table 11: Question Regarding Online Services

QUESTION:

Thinking about the areas YOU SUPERVISE, please indicate whether each of the following ONLINE SERVICES are outsourced, provided by the county itself, or not provided at all:

- Permit or License Applications
 - Searchable Public Records
 - Voter Registration
 - Payment of Utility Bills
 - Payment of Tickets or Fines
 - Payment of Taxes
 - Filing electronic employment applications
 - Requests for services (streetlight repair, potholes, etc.)
-

However, review of the data showed that many respondents either skipped this set of questions outright or overwhelming selected “Do Not Know” which would suggest that they were unaware of whether/or how these services were being provided within the areas they supervised. As it does not seem typical for a supervisor to –not- know this information, the conclusion was reached that the question was not clear and therefore all responses were excluded from this analysis.

In the end, this analysis included nine independent variables (see Table 12). Based on the responses to these variables, the majority of IT Director in Florida constitutional offices focus 100 percent of his/her time to the IT related needs of one office, which has an adequate budget, and is staffed by one to four employees whose job only supports IT. The average county constitutional office services a population between 200k and half a million, of which between 15 and 23 percent of individuals over

the age of 25 have a bachelor's degree or higher. Further the average county intergovernmental revenue received is between \$25 million and \$74.9 million.

Table 12: Independent Variables

Variable	N
Type of Office Supervised	102
Number of Offices Supervised	125
Number of Employees Supervised	124
Percent of Duties Related to IT or information security	124
Adequacy of Budget	79
County Intergovernmental Revenue Totals	125
County Population	125
Percent of County Population with Bachelors Degrees or Higher	125
State Zones	125

Dependent Variable Coding

The survey was constructed in two parts, whereas the first half collected information for independent variables, the second half probed for the dependent variables. Collectively, the survey yielded 50 5-point ordinal dependent variables as respondents were asked about the frequency that they engage in eight activities with each of five types of governments (8 x 5 = 40 variables) plus two questions to gauge the overall importance and development of their relationships with each of five types of governments (2 x 5 = 10 variables).

Initial visual inspection of the dependent variables overwhelmingly revealed that IT Directors have an extremely low frequency of intergovernmental contact, regardless of activity or type of government contacted. Consequently, univariate analysis using Kolmogorov-Smirnov tests for normality in conjunction with probability plots consistently

revealed non-normal distributions due to these large skews in the data. Efforts to normalize the distributions through data transformation failed and attempts to collapse groups masked the true sense of the data. As a result, the decision was made not to alter the variables but instead to analyze all data with non-parametric tests which do not require data to be normally distributed. Specifically, the non-parametric tests Kruskal-Wallis One-way ANOVA and Mann-Whitney U for independent samples were selected and are discussed in the next section.

For the purposes of this analysis, each of these 10 groups of five questions was seen as a “set” and each set was used to create a separate composite variable to measure the common underlying dimension (see Table 13). Each index was created by summing cases where the respondent answered all five indicator questions.

Table 13: Dependent and Index Variables

Dependent Variable Label	Indicators for each Level of Government	Index Variable
1. Seek technical assistance	...with Federal: TECHF; ...with State: TECHS; ...with another County: TECHC; ...with another Government located within the County: TECHG; ...with another Department located within the County: TECHD	= ITECH N = 118
2. Seek NON-technical assistance	...with Federal: NONTECHF; ...with State: NONTECHS; ...with another County: NONTECHC; ...with another Government located within the County: NONTECHG; ...with another Department located within the County: NONTECHD	= INONTECH N = 117

3. Seek information on an IT security program or project	...with Federal: INFOF; ...with State: INFOS; ...with another County: INFOC; ...with another Government located within the County: INFOG; ...with another Department located within the County: INFOD	= IINFO N = 114
4. Seek funding or resources to improve IT security efforts	...with Federal: RESOURCF; ...with State: RESOURCS; ...with another County: RESOURCC; ...with another Government located within the County: RESOURCG; ...with another Department located within the County: RESOURCD	= IRESOURC N = 114
5. Seek legal or policy guidance regarding IT security	...with Federal: LEGALF; ...with State: LEGALS; ...with another County: LEGALC; ...with another Government located within the County: LEGALG; ...with another Department located within the County: LEGALD	= ILEGAL N = 115
6. Seek regulatory or policy flexibility regarding IT security	...with Federal: FLEXF; ...with State: FLEXS; ...with another County: FLEXC; ...with another Government located within the County: FLEXG; ...with another Department located within the County: FLEXD	= IFLEX N = 115
7. Attempt to modify duties or procedures of an established partnership/agreement relating to IT security	...with Federal: DUTIESF; ...with State: DUTIESS; ...with another County: DUTIESC; ...with another Government located within the County: DUTIESG; ...with another Department located within the County: DUTIESD	= IDUTIES N = 115
8. Attempt to modify resource-sharing or funding obligations of an established partnership/agreement related to IT security	...with Federal: OBLIGAF; ...with State: OBLIGAS; ...with another County: OBLIGAC; ...with another Government located within the County: OBLIGAG; ...with another Department located within the County: OBLIGAD	= IOBLIGA N = 115
9. Degree of relationship importance	...with Federal: IMPORTF; ...with State: IMPORTS; ...with another County: IMPORTC; ...with another Government located within the County: IMPORTG; ...with another Department located within the County: IMPORTD	= IIMPORT N = 114

10. Degree of relationship development	...with Federal: DEVELOPF; ...with State: DEVELOPS; ...with another County: DEVELOPC; ...with another Government located within the County: DEVELOPG; ...with another Department located within the County: DEVELOPD	= IDEVELOP N = 117
--	--	-----------------------

The original ordinal scale used for all eight dependent variables measuring an activity was “Weekly” (=1), “Monthly” (=2), “Several times a year” (=3), “A few times a year” (=4), and “Never” (=5). In order to construct more logically intuitive index variables, it was first necessary to recode these variables to reverse the scores. The resulting scale ranged from a summed score of 5, indicating the respondent never performed ‘said’ activity with any type of government, to a summed score of 25, indicating that the respondent performed ‘said’ activity weekly with each type of government.

The same procedures were undertaken for creating the index variables for the two questions which gauged the overall importance and development of different relationships but were measured on different 5-point ordinal scales. The resulting scales for these two variables ranged from a summed score of 5, indicating the respondent did not perceive any of his/her intergovernmental relationships as important/developed, to a summed score of 25, indicating that the respondent perceive all of his/her intergovernmental relationships as extremely important/developed.

Beyond these 10 indexes variables, five more composite variables were created by summing the eight activity questions by each type of government. For example, the composite variable “Frequency of Contact w/ Federal Offices” (IFED; N= 111) was created by summing responses to TECHF; NONTECHF; INFOF; RESOURCF;

LEGALF; FLEXF; DUTIESF; and OBLIGAF. In that eight variables were used to create the index, the resulting scale ranged from a summed score of 8, indicating the respondent never contacts federal offices for any of the eight activities, to a summed score of 40, indicating that the respondent contacts federal offices weekly for all eight activities. Constructed the same way, the final four index variables were “Frequency of Contact w/ State Offices” (ISTATE; N= 108); “Frequency of Contact w/ other Counties” (ICOUNTY; N= 107); “Frequency of Contact w/ another Government located within the County” (IGOV; N= 111); and “Frequency of Contact w/ another Department located within the County” (IDEPT; N= 110). To explore the relationships between these 15 dependent index variables and the nine independent variables previously discussed, the researcher turned to non-parametric testing.

Non-parametric Tests

In instances where parametric assumptions are violated non-parametric test are preferred because they use the ranks of the data rather than the raw values to calculate the test statistic (Olsen, 2003; Norusis, 1998; Lehmkuhl, 1996). However, since interval and ordinal information is lost in the conversion to ranks, these tests are not as powerful as their parametric counterparts. Further, for the same number of observations, parametric test are more conservative than non-parametric tests, meaning they produce fewer false positives or Type I Errors were one incorrectly rejects the null hypothesis (Chan, 2003; Wuensch, 2001). Using the conventional parametric alpha level of .05 for

non-parametric tests inadvertently increases the chance of making Type I Errors. To reduce this probability and make a test more conservative, a lower alpha level should be set (Hair et. al, 1998). Therefore, to decrease the likelihood of false positives, the level of required significance for all tests in this analysis was lowered from the standard parametric level of .05 to .01. Tests approaching significance was set at $p \leq .02$.

To test the null hypothesis that all samples come from identical populations, the Kruskal-Wallis test for independent groups was used. This test is the non-parametric alternative to ANOVA for independent groups to be used when data violate parametric assumptions (Norusis, 1998). The Kruskal-Wallis test statistic is calculated on the sums of ranks for combined groups after data from all groups are ordered (Garson, 2003). A significant p-value suggests that the differences observed are not coincidence. However, a significant test does not necessarily mean that every group differs from every other group; it only means that at least one group differs from the others (Hair et al. 1998). Therefore, a significant test is interpreted only as an overall difference between the groups. Unlike its parametric counterpart, ANOVA, there are no post-hoc tests available for Kruskal-Wallis (SPSS, 1998). Therefore, to determine what is driving significance, that is which group(s) differ from which other group(s), Mann-Whitney U for two independent samples was used to test group differences for significant independent variables.

The Mann-Whitney U test of difference is the nonparametric alternative to the two-sample t-test (Olsen, 2003). Valid for data which are either continuous or discrete, it works by comparing the medians of two groups rather than the means and is used to test the hypothesis that there is no difference between them (Chan, 2003). It computes

the test statistic 'U' by pooling the two samples and listing cases in order by their rank level and then test whether the ranks are randomly mixed between two samples. When the size of both groups exceed 20, as is the case for all dichotomous variables created for this analysis, the sampling distribution of U approaches a normal curve. For this study, Mann-Whitney tests were conducted only for two purposes:.. First, they were used to further explore significant Kruskal-Wallis tests (note: independent variables were prepared for Mann-Whitney testing by creating a new dichotomous indicator-coded (0/1) variable for each group of the independent variable). Second, they were used in situations where an independent variable was dichotomous and therefore Kruskal-Wallis testing was not possible (note: no variable recoding needed).

V. ANALYSIS AND FINDINGS

For this research, reporting test scores and significance levels was the primary manner used to represent findings. Measures of central tendency, such as means and standard deviations, were not reported as they generally do not provide a very useful description of data that is not normally distributed (Olsen 2003; Lehmkuhl, 1996). However, means were used in figures when they did help illustrate trends. Descriptive statistics better suited to explain nonparametric data include mode, median, and percentile rank (Bickel, 2002). After a thorough examination of the data, the researcher chose to report modes as they most effectively illuminated differences in this particular data. Specifically, a mode is the most frequently occurring response (Lehmkuhl, 1996). In non-normally distributed data, it is possible to have no mode however, this situation did not occur with any variable in this study.

General Analysis

To uncover patterns and norms with regard to this largely invisible population, frequencies and Crosstabs were initially used to examine the data. Several trends were observed and noted in this section. However, generalizations made herein presuppose that study respondents are representative of the true population. Further, these

generalizations only extend to IT Directors and their departments in Florida constitutional offices.

In the end, this analysis included 15 dependent index variables. Review of these variables revealed that the majority of intergovernmental or interorganizational contact preformed by IT departments in Florida constitutional offices for reasons related to IT or IT security happens only “A Few Times a Year” or “Never” regardless of the activity (see Table 14).

Table 14: Total Percent of Respondents who Contact Each Type of Government only “ A Few Times a Year” or “Never” Regardless of the Activity

	Government Contacted	Percent
	Federal	92.8%
	State	84.3%
	Another County	89.7%
Another Government Located within the Jurisdiction of their County		82.0%
Another Department Located within their County		65.5%

Specifically, 92.8 percent of respondents only contact federal offices a few times a year or never; 84.3 percent of respondents only contact state offices a few times a year or never; 89.7 percent of respondents only contact an office in an another county a few times a year or never; 82 percent of respondents only contact an office in an another government located within their county jurisdiction a few times a year or never; and 65.5 percent of respondents only contact departments located within their own county government a few times a year or never.

Largely consistent with their reported frequency of contact, the percent of respondents who perceived the overall relationship between their IT Department and

each the other types of governments as only ‘Somewhat Developed’ or ‘Not Developed’ was generally much higher than the percent who perceived the relationship as ‘Very Developed’ or ‘Extremely Developed’ (see Table 15). The exception was with departments located within their own county government

Table 15: Perceived Overall Relationship Development with Each Contact by Percents

	Extremely Developed	Very Developed	Developed	Somewhat Developed	Not Very Developed
Federal	0.0	2.6	2.6	15.4	79.5◀
	= 2.6%			= 94.9%	
State	5.1	11.1	25.6	34.2◀	23.9
	= 16.2%			= 58.1%	
County	2.6	7.7	27.4	31.6◀	30.8
	= 10.3%			= 62.4%	
Other Governments	5.1	12.8	19.7	30.8	31.6◀
	= 17.9%			= 62.4%	
Other Departments	24.6	26.3◀	17.8	21.2	10.2
	= 50.9%			= 31.4%	

“◀” : Mode

However, respondents’ perception of relationship development is in slight discord with perceived importance of several types of governments specifically with regard to federal and state (see Table 16).

Table 16: Perceived Importance of Each Contact to Overall IT Success

	Extremely Important	Very Important	Important	Somewhat Important	Not Very Important
Federal	2.4	8.0	8.0	25.6	51.8 ◀
	= 10.4%			= 77.4%	
State	7.9	19.3	24.6	30.7 ◀	17.5
	= 27.2%			= 48.2%	
County	0.9	8.8	19.3	34.2	36.8 ◀
	= 9.7%			= 71.0%	
Other Governments	7.0	13.2	17.5	21.9	40.4 ◀
	= 20.2%			= 62.3%	
Other Departments	24.3 ◀	18.3	17.4	21.7	18.3
	= 42.6%			= 40%	

“◀” : Mode

These figures would indicate that the relationships counties maintain with federal and state offices are not as developed as perhaps they should be considering the level of importance respondents place on these offices with regard to their information security efforts.

Examining the data according to overall frequency of each activity reveals that regardless of the type of government contacted, the eight intergovernmental or interorganizational activities addressed in this research also occur only a few times a year or less (see Table 17). Specifically, 60.2 percent of respondents seek technical assistance a few times a year or less; 71.8 percent of respondents seek non-technical assistance a few times a year or less; 76.3 percent of respondents seek information on a program or project a few times a year or less; 92.1 percent of respondents seek funding or resources to improve their information security efforts a few times a year or less; 87.8 percent of respondents seek legal or policy guidance a few times a year or

less; 93 percent of respondents seek regulatory or policy flexibility a few times a year or less; 96.3 percent of respondents attempt to modify duties or procedures of an established partnership/agreement relating to IT a few times a year or less; and 95.7 percent of respondents attempt to modify resource-sharing or funding obligations of an established partnership/agreement relating to IT a few times a year or less.

Table 17: Percent of Respondent who Engage in Each Activity “ A Few Times a Year or Less” Regardless of the Intergovernmental or Interorganizational Contact

Activity	Percent
Seek technical assistance	60.2%
Seek non-technical assistance	71.8%
Seek program or project information	76.3%
Seek resources or funding	92.1%
Seek legal or policy guidance	87.8%
Seek regulatory or policy flexibility	93.0%
Seek to modify duties or procedures w/ a partner or agreement	96.3%
Seek to modify resource or funding obligations w/ partner or agreement	95.7%

Of 124 respondents, the largest concentration (37.6 percent) indicated that 100% of their duties focus on IT or information security related issues (see Table 18). However, nearly one-third of respondents (“40% or Less” [22] + “60% or Less” [16] = 38/124 = 30.6%) indicated that less than 60% of their duties are dedicated to IT related issues. This means on average nearly one out of every three constitutional offices in the state does not have a full-time director supervising critical local information systems.

Table 18: Percent of Duties Focused on IT Related Tasks

Percent of Duties	Cases	Percent
40% or less	22	16.7%
60%	16	12.8%
80%	39	31.2%
100%	47	37.6%
N = 124		

The 38 respondents who indicated that less than 60% of their duties are dedicated to IT related issues disproportionately reside in Zones 1 and 2 which are the west and north respectively (see Table 19)⁵.

Table 19: Zone by Percent of Duties Focused on IT Related Tasks

	40% or less	60%	80%	100%
Zone 1 (west) N=14	5	1	5	3
	= 6 (42.8%)			
Zone 2 (north) N= 33	9	7	7	10
	= 16 (48.4%)			
Zone 3 (central) N= 38	3	5	16	14
	= 8 (21.0%)			
Zone 4 (south) N= 39	5	3	11	20
	= 8 (20.5%)			
Total N=124	Total= 38 (30.6%)			

Specifically, 42.8 percent of Zone 1 respondents and 48.4 percent of Zone 2 respondents are only able focus less than 60% of their duties to IT related issues. Meaning, the number of constitutional offices in the northern quarter of the state with

⁵ Once again it should be noted that Zone 1 was under-represented in relation to the other three zones which could in turn potentially impact findings.

less than full-time IT Directors is disproportionately higher than the rest of the state. However, more than half of all respondents (20 out of 39) working in the 17 counties of Zone 4 in the south of the state indicated that 100% of their duties are dedicated to IT related issues.

In addition, one-third of all respondents working in Zone 2 counties indicated that they supervise two or more offices (see Table 20). At the other end of the spectrum, less than one-sixth of Zone 4 directors (6 out of 39) and less than one-seventh of Zone 3 directors (5 out of 34) supervise two or more offices. However, of the 14 respondents from Zone 1 in the panhandle, only one (7.1 percent) indicated that s/he supervised two or more offices.

Table 20: Zone by Number of Offices Supervised

	Only One Office	Two or More Offices
Zone 1 (west) N=14	13	1 (7.1%)
Zone 2 (north) N= 33	22	11 (33.3%)
Zone 3 (central) N= 39	34	5 (12.8%)
Zone 4 (south) N= 39	33	6 (15.4)

Of 101 respondents, the largest concentration (34.6 percent) indicated that they supervise between one and four employees (see Table 21). However, one in four respondents (23 cases or 22.7 percent) indicated that they supervise no employees. Even more alarming, 47.8 percent of these respondents (11 of the 23 cases) also indicated that they are part-time Directors. This means that an average of 10.8 percent of constitutional offices in the state (11 out of 101 cases = 10.8) do not have a full-time

IT director or any supportive staff ensuring that crucial patches are installed and that vital data is backed-up.

Table 21: Number of Employees Supervised by Percent of Duties Focused on IT Related Tasks

	40% or less	60%	80%	100%	Totals
0	7	4	6	6	23 (22.7%)
	= 11 (47.8%)				
1-4	9	2	13	11	35 (34.6%)
	= 11 (31.3%)				
5-14	2	3	13	4	22 (21.7%)
	= 5 (22.7%)				
15 or more	1	3	5	12	21(20.7%)
	= 4 (19.0%)				
Total N=101	Total= 31 (30.6%)				

Of the respondent who indicated that they supervise no employees, 36.3 percent (12 cases) work for counties located in Zone 2 (see Table 22).

Table 22: Number of Employees Supervised by Zone

	[0]	[1 – 4]	[5 - 14]	[15 +]
Zone 1 (west) N=14	4 (28.5%)	7◀ (50%)	1 (7.1%)	2 (14.2%)
Zone 2 (north) N= 33	12 (36.3%)	14◀ (42.4%)	5 (15.1%)	2 (6%)
Zone 3 (central) N= 38	4 (10.5%)	7 (18.4%)	14◀ (36.8%)	13 (34.2%)
Zone 4 (south) N= 39	7 (17.9%)	13◀ (33.3%)	7 (17.9%)	12 (30.7%)
Total N=124	27	41◀	27	29

“◀” : Mode

Whereas IT departments in the 20 counties of Zone 2 seemed stretched thin for employees, offices located in the 14 counties of Zone 3, the central band across the state, appear to be the best staffed of the four zones. Of the respondents working in Zone 3 counties, only 10.5 percent (4 cases) indicated that they had no employees. Moreover, 34.2 percent (13 cases) have 15 or more employees and an additional 36.8 percent (14 cases) noted that they have between 5-14 employees.

As this analysis revealed, there appear to be trends in the data which coincide with zone membership. However, the question arose whether these similarities could more likely be attributed to underlying economic patterns occurring regionally rather than management decisions, for instance, regarding the appropriate number of employees. To explore this notion, the researcher ran Crosstabs between the variable “Zone” and the variable “Intergovernmental Revenue” and the index “Adequacy of Budget” and (see Tables 23 and 24).

Table 23: Zone by the Independent Variable “Intergovernmental Revenue

	Less than \$11.9 million	\$12 – 24.9 million	\$25 – 74.9 million	\$75 + million
Zone 1 (west) N=14	2 (14.2%)	8◀ (57.1%)	4 (28.5%)	0 (0%)
Zone 2 (north) N= 33	18◀ (54.5%)	12 (36.3%)	3 (9%)	0 (0%)
Zone 3 (central) N= 39	2 (5.1%)	9 (23.%)	15◀ (38.4%)	13 (33.3%)
Zone 4 (south) N= 39	7 (17.9%)	5 (12.8%)	13 (33.3%)	14◀ (35.8%)
Total N=124	29 (23.3%)	34 (27.4%)	35◀ (28.2%)	27 (21.7%)

“◀” : Mode

Based on the overall distribution of intergovernmental revenue, the majority of counties receive between \$12 and \$74.9 million. Whereas Zone 3 and specifically Zone 4 receive more monies on average; Zone 1 and particularly Zone 2 receive less. While intergovernmental revenue provides a glimpse into county funds, it provides an incomplete picture of overall county budget. Further, the real question here is how adequately county funds filter to IT departments.

A review of index variable “Adequacy of Budget” reveals that the majority of Directors in Zones 1, 3, and 4 perceived overall available funds for several core IT needs to be adequate.

Table 24: Zone by the Index variable “Adequacy of Budget”

	Far Below Adequate (7-11)	Below Adequate (12-16)	Adequate (17-22)	Above Adequate (23-28)
Zone 1 (west) N=8	1 (12.5%)	1 (12.5%)	5◀ (62.5%)	1 (12.5%)
Zone 2 (north) N= 25	3 (12%)	8 (32%)	12◀ (48%)	2 (8%)
Zone 3 (central) N= 24	0 (0%)	6 (25%)	16◀ (66.6%)	2 (8.3%)
Zone 4 (south) N= 22	2 (9%)	7 (31.8%)	13◀ (59%)	0 (0%)
Total N=79	6	22	46◀	5

“◀” : Mode

While the largest concentration of Zone 2 directors (48 percent) also indicated that their overall IT budget was adequate, a total of 44 percent (12% + 32%) noted that their budget was below adequate. Specifically, one-third indicated that funds were below adequate and 12 percent noted that their funding was far below adequate. As such, one might want to conclude that budgets were driving staffing decisions because

relative to the other zones, Zone 2 IT departments have smaller staffs; nearly one out of every two Directors (48.4 percent) are only able to dedicated 60% or less of their duties to IT related issues (refer to Table 19); and one-third of Directors simultaneously supervising two or more constitutional offices (refer to Table 20). However, a total of 40.8 percent of Zone 4 Directors (9% + 31.8%) also indicated that their overall budgets were inadequate. Yet 30.2 percent of offices in this zone have 15 or more employees (refer to Table 22); only one in five Directors (20.5 percent) are only able to dedicated 60% or less of their duties to IT related issues (refer to Table 19); and only 15.4 percent of Directors supervise two or more constitutional offices (refer to Table 20). As such, it seems that budget adequacy alone was not the driving force behind staffing differences and the researcher must conclude that there remains an underlying regional quality(s) or influential dynamic(s), or perhaps some other spurious factor not readily perceptible via the demographics explored in this research which is the reason of these regional differences.

Beyond regional differences, collectively the majority of respondents found funding for each core IT need to be adequate or better (refer to Table 24). However, at least one in five respondents indicated that it was below or far below adequate. Specifically, 56 percent, or one out of every two Directors indicated that funding for computer security education for non-IT employees was below adequate (see Table 25). Nearly half (48.6 percent) indicated that they did not have enough funding for risk assessment and risk management. And nearly 40 percent of respondents indicated that their funding for hiring IT employees was below adequate.

Table 25: Core IT Needs by Percent of Respondent who Indicated that Funding was Inadequate

Core IT Needs	Percent
IT equipment/ software/ hardware (N=121)	23.1%
IT security equipment/ software/ hardware (N=118)	31.3%
Hiring outsource vendors (N=98)	30.6%
Hiring IT personnel and support staff (N=111)	39.6%
Training IT personnel (N=116)	39.6%
Computer security education for NON IT employees (N=98)	56.1%
Risk assessment/ management (N=109)	48.6%

Further analysis revealed distinct difference according to office type. For instance, the majority of IT Directors in Board of Commissioners offices (53 percent) and the largest concentration of IT Directors in Sheriff's offices (32 percent) supervise 15 or more employees (see Table 26). However, the largest concentration of IT Directors in Property Appraiser's offices (33.3 percent) and Supervisor of Elections' offices (30.4 percent) supervise no employees. Whereas the largest concentration of IT Directors in Tax Collectors offices (46.4 percent) and Clerk of Court offices (33.3 percent) supervise between one and four employees.

Table 26: Number of Employees Supervised by Type of Office

Office	[0]	[1 – 4]	[5 - 14]	[15 +]
Board of Commissioners (N=32)	3 (9.3%)	6 (18.7%)	6 (18.7%)	17◀ (53.1%)
Clerk of Court (N=30)	5 (16.6%)	10◀ (33.3%)	9 (30.0%)	6 (20.0%)
Property Appraiser (N=23)	8◀ (33.3%)	6 (25.0%)	5 (20.8%)	4 (16.6%)
Sheriff (N=34)	7 (20.5%)	8 (23.5%)	8 (23.5%)	11◀ (32.3%)
Supervisor of Elections (N=23)	7 (30.4%)	10◀ (43.4%)	2 (8.6%)	4 (17.3%)
Tax Collectors (N=28)	7 (25.0%)	13◀ (46.4%)	4 (14.2%)	4 (14.2%)

“◀” : Mode

The different types of offices also have different rates for supervising two or more offices (see Table 27). For instance, 65.6 percent of IT Directors supervising Board of Commissioners offices also supervise another office. However, only 11.7 percent IT Directors supervising Sheriff’s offices also supervise another office.

Table 27: Percent of IT Directors who Supervise Two or more Office by Type of Office Supervised

Office	Percent
Board of Commissioners	65.5%
Clerk of Court	46.6%
Property Appraiser	37.5%
Sheriff	11.7%
Supervisor of Elections	47.8%
Tax Collectors	35.7%

Finally, the type of office a director supervises also impacts what percent of their duties will likely focus solely on IT related issues (see Table 28). For instance, 62.5 percent IT Directors supervising Board of Commissioners offices, 100% of their duties are IT related. However, for IT Directors in Property Appraisers offices, only one in four

(6 out of 24) report the same, whereas 43.4 percent (“40% of Duties” [12.5%] + “60% of Duties” [29.1%]) are only able to devote 60% or less of their duties to IT related issues. In contrast, 82.1 percent (“80% of Duties” [39.2%] + “100% of Duties” [42.8%]) of IT Directors in Tax Collectors’ offices focus 80% or more of their duties to IT related issues.

Table 28: Percent of IT Director’s Duties Focused on IT Related Issues by Type of Office Supervised

Office	[40% of Duties]	[60% of Duties]	[80% of Duties]	[100% of Duties]
Board of Commissioners (N=32)	4 (12.5%)	5 (15.6%)	3 (9.3%)	20 ◀ (62.5%)
Clerk of Court (N=30)	7 (23.0%)	4 (13.3%)	6 (20.0%)	13 ◀ (43.3%)
Property Appraiser (N=24)	3 (12.5%)	7 ◀ (29.1%)	7 ◀ (29.1%)	6 25.0%
Sheriff (N=34)	8 (23.5%)	5 (14.7%)	10 (29.4%)	11 ◀ (32.3%)
Supervisor of Elections (N=23)	4 (17.3%)	3 (13.0%)	4 (17.3%)	12 ◀ (52.1%)
Tax Collectors (N=28)	2 (7.1%)	3 (10.7%)	11 (39.2%)	12 ◀ (42.8%)

“◀” : Mode

Being exploratory, this study did not endeavor to establish causal relationships nor was it bound to hypotheses. Instead it sought to uncover patterns, like the ones just discussed, and to answer the following three questions: 1) is there a relationship between office/county demographics and the IGM activities its IT Directors most often engage in on behalf of information security and critical digital infrastructure protection; 2) which IGM activities do county IT Directors most often engage in on behalf of information security and critical digital infrastructure protection; 3) do county IT Directors

make more use of vertical or horizontal IGM relationships on behalf of information security and critical digital infrastructure protection? However, to help facilitate this analysis, these questions were tested as hypotheses. These findings and the conclusions are discussed next.

Question 1: Prevalence of IGM Activity

The first research question inquires into which IGM activities county IT Directors most often engage in as part of their information security efforts. As noted in the previous chapter, statistics such as mean and standard deviation do not provide useful descriptions of non-normally distributed data. Therefore, the researcher examined frequencies and modes as they most effectively describe the current data .

To recap, respondents were asked to indicate how often they engage in eight activities with each of five intergovernmental partners (federal, state, county, other governments, and other departments) using a scale of 1-5 [“Weekly” (=5), “Monthly” (=4), “Several times a year” (=3), “A few times a year” (=2), and “Never” (=1)]. Of the 40 resulting questions, 31 (77.5 percent) had a mode of “Never” while nine had a mode of “A few times a year” (see Table 29). None had modes of “Weekly”, “Monthly”, or “Several times a year”.

Table 29: The Nine Activities with Modes of ‘A Few Times a Year or Less’ rather than ‘Never’

Activity
Seek technical assistance from a STATE office
Seek technical assistance from another COUNTY
Seek technical assistance from a another DEPARTMENT
Seek program or project information from a STATE office
Seek program or project information from another COUNTY
Seek program or project information from a another DEPARTMENT
Seek legal or policy guidance from a STATE office
Seek legal or policy guidance from another COUNTY
Seek legal or policy guidance from a another DEPARTMENT

Of the nine questions for which “A few times a year” was the mode, they were equally divided among three activities; seek technical assistance; seek program or project information; and seek legal or policy guidance. Beyond the fact that only these three activities have modes other than ‘Never’, another dynamic clearly evident was that each of these more frequently performed activities occurs only with either a State office, another County, or another Department within the respondents own county. However, patterns of vertical or horizontal relationships are addressed in the next section.

Another way to determine which IGM activities county IT Directors most often perform was to look at frequencies. Doing so revealed that of the eight activities, seeking technical assistance was the most frequently preformed activity (see Table 30). Examining all 40 combinations of ‘activity by partner’ revealed that of the five most frequently performed activities ‘seeking technical assistance’ appears on the list three times, while ‘seeking non-technical assistance’ and ‘seeking program or project information’ each appeared once. It should also be pointed out that four of five activities

occur horizontally with other Departments within the respondents own county or with another Government within the jurisdiction of the respondents county.

Table 30: Five Most Frequent Activities by Percent of Respondents who Perform the Activity Several Times a Year or More

Activity	Percent
Seek technical assistance from another Department in own county	31.1%
Seek non-technical assistance from another Department in own county	17.6%
Seek technical assistance from another Government in the county	14.9%
Seek technical assistance from a State office	12.5%
Seek program or project information from another Department in own county	12.2%

While the earlier examination of modes revealed that the largest concentration of respondents ‘seek legal or policy guidance’ “A Few Times a Year” (whereas the majority of respondents “Never” perform five of the other activities), a review of frequencies revealed that this activity is rarely performed more than a few times a year regardless of the intergovernmental contact.

Another important facet of exploring the frequency of IGM activities was to look which activities occur the least. Again, examining all 40 combinations of ‘activity by partner’ revealed that seeking to modify either the duties/procedures or the resources/funding obligations of an established partnership/agreement relating to IT with either a Federal office or another county rarely occurs (see Table 31). Another infrequent activity is seeking resources or funding from another County.

Table 31: Five Least Frequent Activities by Percent of Respondents who Never Perform the Activity

	Activity	Percent
	Seek to modify duties/procedures of an agreement with a Federal office	94.8%
	Seek to modify resource/funding obligations of an agreement with a Federal office	94.8%
	Seek to modify duties/procedures of an agreement with another County	87.0%
	Seek resources or funding from another County	85.5%
	Seek to modify resource/funding obligations of an agreement with another County	81.9%

In reference to research Question One, which IGM activities county IT Directors most often engage in as part of their information security efforts, the data indicated that seeking technical assistance followed by seeking non-technical assistance and program/project information are the most frequently performed activities. The data also indicated that the least frequently performed activities are seeking to modify either the duties/procedures or the resources/funding obligations of an established partnership/agreement relating to information technology.

Question 2: Vertical vs. Horizontal Relationships

The second research question inquires whether county IT Directors make more use of vertical or horizontal IGM relationships as part of their information security efforts. As with research Question One, exploring frequencies helped to delineate which intergovernmental relationships county IT Directors most often call upon. Examining the frequency of each activity as performed with each type of contact revealed that ‘other Departments within the respondents own county’ were most frequently contacted for six of the eight activities (see Table 32). For the other two activities, seeking

regulatory/policy flexibility or legal/policy guidance, State offices were most frequently contacted.

Table 32: Most Frequent Partner for Each Activity

Activity	Partner
Seek to modify duties/procedures of a agreement with...	another Department in own county
Seek regulatory or policy flexibility from...	State
Seek program or project information from...	another Department in own county
Seek legal or policy guidance from...	State
Seek NON-technical assistance from...	another Department in own county
Seek to modify resource/funding obligations of a agreement with...	another Department in own county
Seek resources or funding from...	another Department in own county
Seek technical assistance from...	another Department in own county

Examining the frequency of each activity as performed with each type of contact revealed that Federal offices were contacted the least for six of the eight activities (see Table 33). Of the other two activities, seeking legal/policy guidance was performed the least often with other Governments with the respondents county and seeking resources/funding was performed the least often with other Counties.

Table 33: Least Frequent Partner for Each Activity

Activity	Partner
Seek to modify duties or procedures of a partner/agreement with...	Federal
Seek regulatory or policy flexibility from...	Federal
Seek program or project information from...	Federal
Seek legal or policy guidance from...	another Government in the county
Seek NON-technical assistance from...	Federal
Seek to modify resource/funding obligations with...	Federal
Seek resources or funding from...	another County
Seek technical assistance from...	Federal

In reference to Research Question Two, whether county IT Directors make more use of vertical or horizontal IGM relationships as part of their information security efforts, the data indicated -horizontal- as six of the eight activities were most often performed with other departments in the respondents county. Further, six of the eight activities were performed the least often vertically with Federal offices.

However of the eight activities, two were performed most often vertically with the State and two activities were performed least often horizontally with either other Counties or other Governments located within the respondents county. This led the researcher to conclude that while IT Directors make more use of horizontal relationship, vertical relationships are also important to county information security efforts.

Question 3: Demographics and IGM Activity

The third research question inquires whether there are relationships between office/county demographics and the IGM activity of IT Directors as part of their of information security efforts. To address this question Kruskal-Wallis tests were run to determine whether respondents answers in the 15 composite variables differed according to each of the independent variables. Tests are presented by the independent variables and the null hypotheses in each instance was that there is no overall difference between groups.

Office Supervised

The first point of exploration was to determine whether respondents answers in the 15 composite variables differed according to the type of office they supervised. Running Kruskal-Wallis tests for rank differences returned four of the 15 test significant at .01 (see Table 34).

Table 34: Kruskal-Wallis Tests Significant at $p \leq .01$ for the Independent Variable “Office Supervised” & the Composite Dependent Variables

Variable	H*	Sig.
Index of Frequency of Contact w/ FEDERAL Offices	32.92	.000
Index of Frequency of Contact w/ another GOVERNMENT in the County	22.49	.000
Index of Frequency to Seek Funding or Resources	20.12	.001
Index of Relationship Importance	19.22	.002

*NOTE: all DF = 5

Of the four significant variables, two pertain to overall interaction with a types government- “Frequency of Contact with Federal Offices” (H=32.92; $p=.000$) and “Frequency of Contact with Other Governments within the Jurisdiction of Your County” (H=22.49; $p=.000$); one pertains to an IGM activity- “Frequency to Seek Funding or Resources” (H=20.12; $p=.001$); and one pertains to the perceived importance of each type of government to the success of the office- “Relationship Importance” (H=19.22; $p=.002$). In each of these instances, the null hypothesis was rejected as there was evidence of an overall significant difference between groups.

Since a significant Kruskal-Wallis test does not denote that every group differs from every other group, Mann-Whitney tests were employed to determine specifically which group(s) differ from which other group(s).

Contact with Federal Offices

For the first significant index, “Frequency of Contact with Federal Offices”, the differences between groups of three dichotomous variables proved statistically significant at .01, specifically, “Board of Commissioners versus all other offices” (U=796.5 p=.003), “Sheriffs versus all other office: (U=671 p=.000), and “Tax Collectors (U=749 p=.008) versus all other offices” (see Table 35).

Table 35: Mann-Whitney Tests for Significant Dependent Index “Frequency of Contact with Federal Offices” by Independent Dichotomous Variables for Type of Office Supervised

Variable	U	Sig.
Board of Commissioners	796.5	.003 ◀
Clerk of Court	862.0	.029
Property Appraiser	733.0	.051
Supervisor of Elections	908.0	.987
Sheriff	671.0	.000 ◀
Tax Collector	749.0	.008 ◀

“◀” : Significant $p \leq .01$ | “✓” : Approaching Significance $p \leq .02$

Based on the scale of the dependent index variable (where a score of 8 indicates no contact across all eight activities and a score of 40 indicates weekly contact across all eight activities), Figure 3 reveals that on average, Board of Commissioners offices and Sheriffs offices contact federal offices at a higher frequency than the other types of offices, while Tax Collectors offices contact federal offices less frequently.

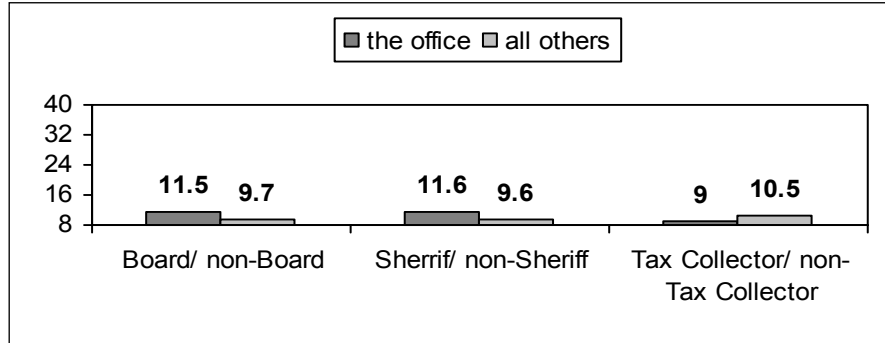


Figure 3: Frequencies of Index “Contact with Federal Offices” by Dichotomous “Board of Commissioners”, “Sheriff”, and “Tax Collector” Variables

To further explore which actions are driving the significance of these relationships, and thus the frequency of contact with federal offices, Mann-Whitey tests were run between each of the three significant dichotomous variables and the eight indicator variables that comprise the index variable “Frequency of Contact with Federal Offices”.

“Board of Commissioners Offices”

Starting with Board of Commissioners offices (see Table 36), the frequency with which this type of office contacts federal offices statistically differs from other types of offices for two activities; “seeking program information” (U=947; p=.002) and “seeking legal or policy guidance” (U=973.5; p=.005), while “seeking regulatory or policy flexibility” (U=1089.5; p=.017) is approaching significance.

Table 36: Mann-Whitney Tests for Dichotomous “Board of Commissioners” by Index Factors of “Frequency of Contact w/ Federal Offices”

	Variable	U	Sig.
	Seek technical assistance	1128.5	.037
	Seek non-technical assistance	1225.5	.165
	Seek program or project information	947.0	.002 ◀
	Seek resources or funding	1152.0	.176
	Seek legal or policy guidance	973.5	.005 ◀
	Seek regulatory or policy flexibility	1089.5	.017 ✓
	Seek to modify duties or procedures w/ a partner or agreement	1224.0	.202
	Seek to modify resource or funding obligations w/ partner or agreement	1294.5	.708

“◀” : Significant $p \leq .01$ | “✓” : Approaching Significance $p \leq .02$

Examining clustered bar charts between the means of frequency for these significant activities and whether the respondent supervised a Board of Commissioners office or not, revealed that on average this type of office more frequently engages in each of these three activities than other types of offices (see Figure 4).

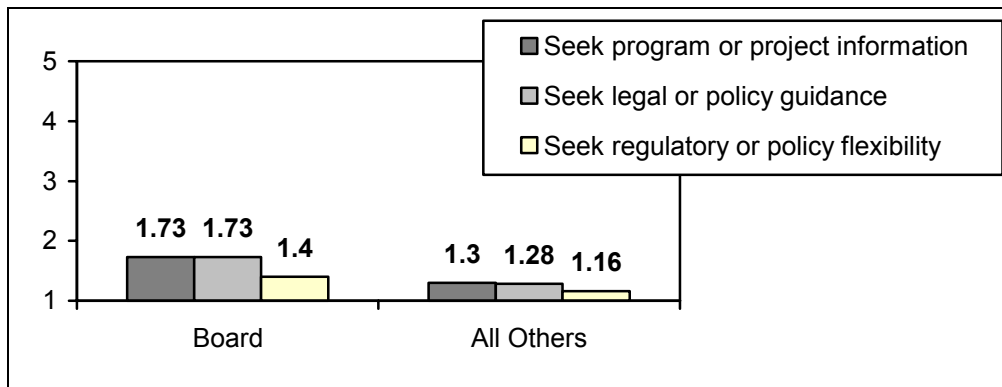


Figure 4: Frequencies of Significant Indicator Variables for “Frequency of Contact with Federal Offices” by “Board of Commissioners Versus All Others”

“Sheriff’s Office”

The frequency with which Sheriff’s Offices contact federal offices (see Table 37) statistically differs from other types of offices for two activities included in the index; “seeking non-technical assistance” (U=1045.5; p=.003) and “seeking resources or funding” (U=714.5; p=.000). While the frequency with which they “seek legal or policy guidance” from federal offices (U=1033.5; p=.017) approaches significance.

Table 37: Mann-Whitney Tests for Dichotomous “Sheriff’s Office” by Index Factors of “Frequency of Contact w/ Federal Offices”

	Variable	U	Sig.
	Seek technical assistance	1171.0	.077
	Seek non-technical assistance	1054.5	.003◀
	Seek program or project information	1165.5	.141
	Seek resources or funding	714.5	.000◀
	Seek legal or policy guidance	1033.5	.017✓
	Seek regulatory or policy flexibility	1345.5	.898
	Seek to modify duties or procedures w/ a partner or agreement	1281.0	.731
	Seek to modify resource or funding obligations w/ partner or agreement	1236.5	.188

“◀” : Significant $p \leq .01$ | “✓” : Approaching Significance $p \leq .02$

Examining clustered bar charts between the means of frequency for each these significant activities and whether the respondent supervised a Sheriffs Office or not, revealed that on average this type of office more frequently engages in each of these three activities then other types of offices (see Figure 5).

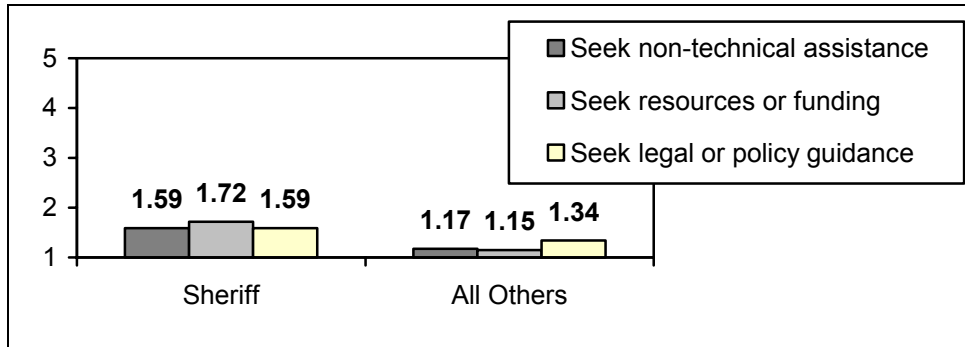


Figure 5: Frequencies of Significant Indicator Variables for “Frequency of Contact with Federal Offices” by “Sheriff’s Office Versus All Others”

“Tax Collector’s Office”

The frequency with which Tax Collectors Offices contact federal offices (see Table 38) does not statistically differ from other types of offices for any specific activity in the index. However, the frequency with which they seek legal or policy guidance from federal offices (U=913.0; p=.019) is approaching significance.

Table 38: Mann-Whitney Tests for Dichotomous “Tax Collector” by Index Factors of “Frequency of Contact w/ FEDERAL Offices”

Variable	U	Sig.
Seek technical assistance	1022.5	.066
Seek non-technical assistance	1017.5	.048
Seek program or project information	965.5	.046
Seek resources or funding	964.5	.042
Seek legal or policy guidance	913.0	.019✓
Seek regulatory or policy flexibility	1075.5	.191
Seek to modify duties or procedures w/ a partner or agreement	1136.0	.716
Seek to modify resource or funding obligations w/ partner or agreement	1120.5	.168

“◀” : Significant p ≤ .01 | “✓” : Approaching Significance p ≤ .02

Contact with Another Government in the County

Referring back to the Kruskal-Wallis tests run to determine if there were groups differences between type of office supervised and the 15 index variables, a second significant index was “Frequency of Contact with another Government located within the Jurisdiction of Your County”. Running Mann-Whitney tests between this variable and the six dichotomous office variables revealed that the difference between “Board of Commissioners office versus all other offices” (U=659 p=.000) was statistically significant (see Table 39).

Table 39: Mann-Whitney Tests for Significant Dependent Index “Frequency of Contact with another Government located within the Jurisdiction of Your County” by Independent Dichotomous Variables for Type of Office Supervised

Variable	U	Sig.
Board of Commissioners	659.0	.000 ◀
Clerk of Court	954.0	.111
Property Appraiser	730.5	.102
Supervisor of Elections	828.5	.526
Sheriff	1144.0	.633
Tax Collector	780.0	.035

“◀” : Significant $p \leq .01$ | “✓” : Approaching Significance $p \leq .02$

Based on the scale of the dependent index, where a score of 8 indicates no contact across all eight activities and a score of 40 indicates weekly contact across all eight activities, Figure 6 illustrates that on average, Board of Commissioners offices contact other governments located within the jurisdiction of their county at a higher frequency than the other types of offices.

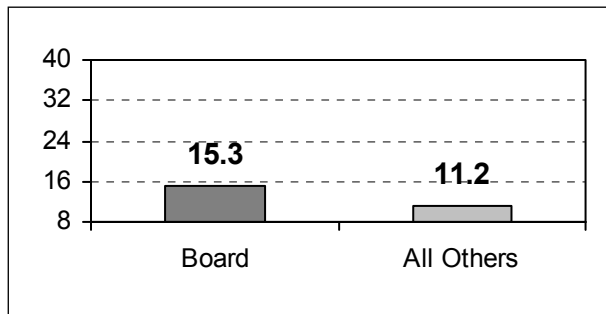


Figure 6: Frequency of Index of “Frequency of Contact w/ another Government in Your County Jurisdiction” by Dichotomous “Board of Commissioners”

To further explore which activities are driving the significance of this relationship, Mann-Whitey tests were run between the dichotomous variable Board of Commissioners and the eight indicator variables that comprise this index. As evident in Table 40, the frequency with which a Board of Commissioners office contacts other government offices located within the jurisdiction of its own county statistically differs from other types of offices for all but one activity- seeking to modify resource or funding obligations with a partner or agreement (U=1118.5; p=.053).

Table 40: Mann-Whitney Tests for Dichotomous “Board of Commissioners” by Index Factors of “Frequency of Contact w/ another Government in Your County Jurisdiction”

Variable	U	Sig.
Seek technical assistance	930.0	.002 ◀
Seek non-technical assistance	868.5	.001 ◀
Seek program or project information	914.0	.002 ◀
Seek resources or funding	944.5	.000 ◀
Seek legal or policy guidance	1004.0	.007 ◀
Seek regulatory or policy flexibility	976.5	.003 ◀
Seek to modify duties or procedures w/ a partner or agreement	893.0	.000 ◀
Seek to modify resource or funding obligations w/ partner or agreement	1118.5	.053

“◀” : Significant $p \leq .01$ | “✓” : Approaching Significance $p \leq .02$

Examining clustered bar charts between the means of frequency for the seven statistically significant activities and whether the respondent supervises a Board of Commissioners office or not illustrates that on average this type of office more frequently engages in each of these activity with other government offices located within the jurisdiction of its own county then do other types of offices (see Figure 7).

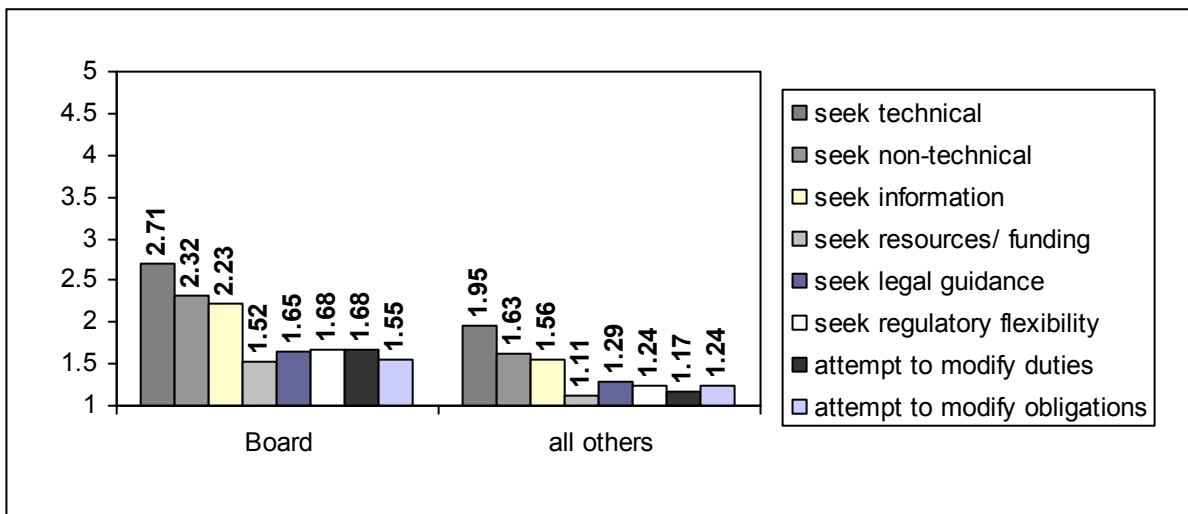


Figure 7: Indicator Variables for “Frequency of Contact w/ another Government Located within the Jurisdiction of Your County” by “Board of Commissioners ” versus All Others

Seeking Funding or Resources

The third index denoted significant by Kruskal-Wallis testing was “Frequency of Seeking Funding or Resources”. Again, Mann-Whitney testing revealed the only statistically significant difference between groups occurs between the dichotomous variable “Board of Commissioners office versus all other offices” (U=889.5 p=.008) (see Table 41).

Table 41: Mann-Whitney Tests for Significant Dependent Index “Frequency of Seeking Funding or Resources” by Independent Dichotomous Variables for Type of Office Supervised

Variable	U	Sig.
Board of Commissioners	899.5	.008 ◀
Clerk of Court	988.5	.098
Property Appraiser	736.0	.067
Supervisor of Elections	949.5	.837
Sheriff	1078.5	.124
Tax Collector	964.5	.206

“◀” : Significant $p \leq .01$ | “✓” : Approaching Significance $p \leq .02$

To further explore which activities are driving the significance of this test, Mann-Whitney tests were run between this dichotomous variable and the five indicator variables that comprise this activity index (see Table 42). Two tests were significant for groups differences; “seeking resources/funding from another government within the jurisdiction of your county” (U=944.5; $p=.000$) and “seeking resources/funding from other department within your own county” (U=996.0; $p=.009$).

Table 42: Mann-Whitney Tests for Dichotomous “Board of Commissioners” by Index Factors of “Frequency of Seeking Funding or Resources”

Variable	U	Sig.
from Federal	1152.0	.176
from State	1297.5	.737
from Another County	1158.5	.044
from Another Government Located within the Jurisdiction of their County	944.5	.000 ◀
from Another Department Located within their County	996.0	.009 ◀

“◀” : Significant $p \leq .01$ | “✓” : Approaching Significance $p \leq .02$

Examining clustered bar charts between the means of frequency for these two significant activities and whether the respondent supervises a Board of Commissioners

office or not, illustrates that on average this type of office more frequently engages in these activity then other types of offices (see Figure 8).

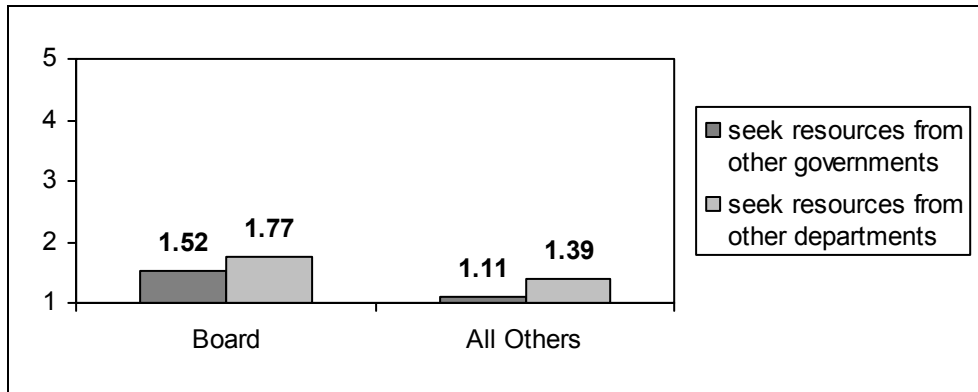


Figure 8: Significant Indicator Variables for “Frequency of Seeking Resources or Funding” by “Board of Commissioners Versus All Others”

Overall Relationship Importance

The fourth and final index denoted significant in Kruskal-Wallis testing was “Overall Relationship Importance”. While Mann-Whitney testing between this index and the six dichotomous office variables revealed no statistically significant differences between groups, “Board of Commissioners office versus all other groups” approached significance at $p=.019$ ($U=918.0$) (see Table 43). However, because no test was significant at .01, the researcher failed to reject the null hypotheses that there was no differences between groups.

Table 43: Mann-Whitney Tests for Significant Dependent Index “Overall Relationship Importance” by Independent Dichotomous Variables for Type of Office Supervised

	Variable	U	Sig.
	Board of Commissioners	918.0	.019 ◀
	Clerk of Court	1078.5	.407
	Property Appraiser	976.0	.795
	Supervisor of Elections	950.5	.849
	Sheriff	1207.0	.732
	Tax Collector	898.0	.095

“◀” : Significant $p \leq .01$ | “✓” : Approaching Significance $p \leq .02$

Because Board of Commissioners was approaching significance, the researcher opted to further explore which activities were driving the test. As such, Mann-Whitney tests were run between this dichotomous variable and the five indicator variables that comprise this activity index (see Table 44). Two tests were significant for groups differences; “overall relationship importance of other governments within the jurisdiction of your county” (U=782.0; $p=.001$) and “overall relationship importance of other departments within your own county” (U=890.5; $p=.008$).

Table 44: Mann-Whitney Tests for Dichotomous “Board of Commissioners” by Index Factors of “Overall Relationship Importance”

	Variable	U	Sig.
	from Federal	1234.0	.715
	from State	1178.5	.479
	from Another County	1114.0	.247
	from Another Government Located within the Jurisdiction of their County	782.0	.001 ◀
	from Another Department Located within their County	890.5	.008 ◀

“◀” : Significant $p \leq .01$ | “✓” : Approaching Significance $p \leq .02$

Examining clustered bar charts between the means of frequency for these two significant activities and whether the respondent supervises a Board of Commissioners

office or not, illustrates that on average this type of office more frequently engages in these activity then other types of offices (see Figure 9).

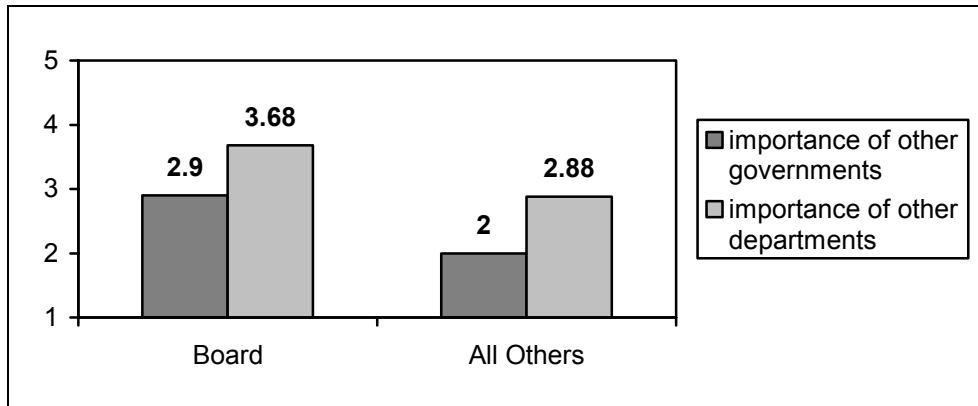


Figure 9: Significant Indicator Variables for Dependent Index “Overall Relationship Importance” by “Board of Commissioners Versus All Others”

Percent Duties Focuses on IT Related Issues

The second point of exploration probed to determine whether respondents’ answers in the 15 composite variables differed according the percent of their time dedicated to IT and IT security related issues. This independent variable was included as the researcher suspected an inverse relationship between the percent of respondents time dedicated to IT related issues and the need for the office to seek outside assistance. Specifically, the less time a respondent had to tend to IT related issues, the more likely s/he would might need to seek assistance.

Running Kruskal-Wallis tests for rank differences produced one test approaching significance at less than .02. The near significant index was “Frequency of Contact with

Other Governments Located within the Jurisdiction of Your County” ($H=10.275$; $DF=3$; $p=.016$). However, because the test was not significant at .01, the researcher did not explore this variable any further and failed to reject the null hypothesis as there was no evidence of an overall difference between groups.

Population with Bachelors Degree or Higher

The third point of exploration probed to determine whether respondents’ answers in the 15 composite variables differed according to the percent of county population with Bachelors degrees or higher. This independent variable was included as the literature on IT Security (as discussed throughout Chapter II) points to the importance of having qualified IT employees on staff and the role post-secondary education plays in developing this workforce. The researcher reasoned that a county with a larger pool of educated applicants would more easily be able to staff its offices with qualified employees versus counties with a smaller of pool applicants with post-secondary degrees. Moreover, the better educated employees are, the more likely that they would be able to solve problems on their own and thus less likely to need to seek outside assistance. As such, the researcher suspected an inverse relationship between the percent of county population with Bachelors degrees or higher and the need for the office to seek outside assistance.

Running Kruskal-Wallis tests for rank differences produced one test significant at .01. Specifically, this test pertains to overall interaction with the state, “Frequency of Contact with State Offices” ($H=11.72$; $DF=2$; $p=.003$). Therefore, the null hypothesis

was rejected as there was evidence of an overall significant difference between groups. To determine specifically which group(s) differ from which other group(s), Mann-Whitney tests were employed between the index and dichotomous variables for each of the groups (see Table 45).

Table 45: Mann-Whitney Tests for Index “Frequency of Contact w/ State Offices” by Dichotomous Variables of “Percent of County Population, age 25+, which Hold Bachelor’s Degrees or Higher”

Dichotomous Variable	U	Sig.
14.9% or less w/ bachelors degree or higher	1070.0	.064
15 – 22.9% w/ bachelors degree or higher	1008.5	.125
23% or more w/ bachelors degree or higher	758.5	.001 ◀

“◀” : Significant $p \leq .01$ | “✓” : Approaching Significance $p \leq .02$

These tests revealed significant differences in frequency of contact with State offices between counties where 23 percent or more of the population have bachelors degrees or higher versus all other counties ($U=758.5$; $p=.001$). Based on the scale of this index variable, where a score of 8 indicates no contact across all eight activities and a score of 40 indicates weekly contact across all eight activities, Figure 10 reveals that on average, counties where 23 percent or more of the population have at least a bachelors degree contact state offices at a lower frequency than counties with a smaller population of residents with a similar education.

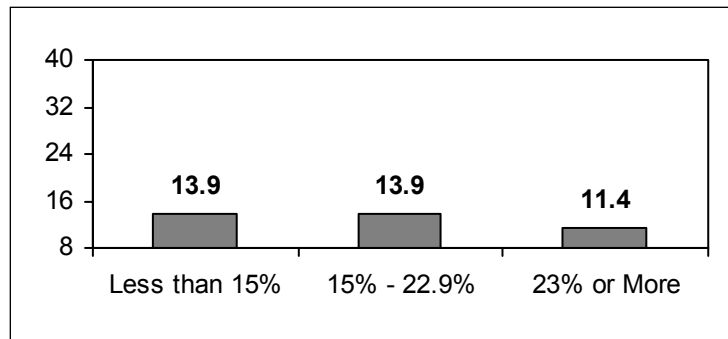


Figure 10: Frequencies of Index “Frequency of Contact w/ State Offices” by Percent of County Population, age 25+, which Hold Bachelor’s Degrees or Higher”

To further explore which actions are driving the significance of this test, hence the frequency of contact with state offices, Mann-Whitey tests were run between the eight indicator variables that comprise the index variable and the dichotomous variable created to capture differences between this population versus the others. As evident in Table 46, the frequency with which offices serving counties where “23 percent or more of the population (age 25+) have at least bachelor’s degrees” “seek technical assistant from the state” statistically differs (U=1133.5; p=.006) from counties with a lower percentage of post-secondary graduates. Differences between groups approach significance with regard to two other state-related activities, namely, “seeking non-technical assistance” (U=1128.0; p=.014) and “seeking program or project information” (U=111.5; p=.011).

Table 46: Mann-Whitney Tests for Dichotomous Variable “23% or More of Population Hold Bachelor’s Degrees or Higher” by Index Factors of “Frequency of Contact w/ State Offices”

	Variable	U	Sig.
	Seek technical assistance	1133.5	.006 ◀
	Seek non-technical assistance	1128.0	.014 ✓
	Seek program or project information	1111.5	.011 ✓
	Seek resources or funding	1149.0	.022
	Seek legal or policy guidance	1164.0	.024
	Seek regulatory or policy flexibility	1289.5	.211
	Seek to modify duties or procedures w/ a partner or agreement	1267.5	.187
	Seek to modify resource or funding obligations w/ partner or agreement	1279.0	.164

“◀” : Significant $p \leq .01$ | “✓” : Approaching Significance $p \leq .02$

Examining clustered bar charts between the means of frequency for these three activities and whether the respondent does or does not supervise an office in a county where 23 percent or more of the population have at least bachelor’s degrees revealed that, on average, offices in counties with a higher percent of post-secondary graduates less frequently contact state offices for these activities than other offices in counties with a lower percent of post-secondary graduates (see Figure 11).

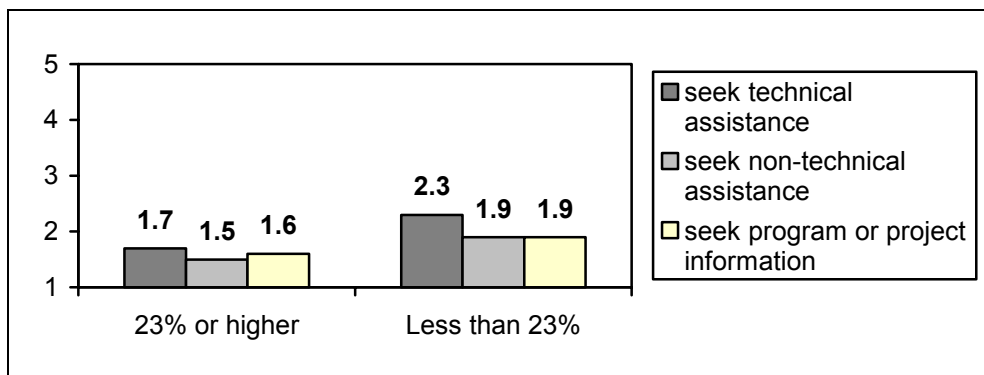


Figure 11: Significant Factors from “Frequency of Contact w/ STATE Offices”

Adequacy of Funding

The forth point of exploration probed to determine whether respondents' answers in the 15 composite variables differed according to the overall perceived adequacy of funds s/he is able to apply to the core IT needs as measured in the composite variable "Adequacy of Budget". This independent variable was included as the researcher reasoned that an office with insufficient funds to meet its needs would more likely need to seek outside assistance.

Running Kruskal-Wallis tests for rank differences produced two test approaching significance at less than .02. The near significant indexes were "Frequency of Contact with Other Governments Located within the Jurisdiction of Your County" (H=10.49; DF=3; p=.019) and "Overall Relationship Importance" (H=9.83; DF=3; p=.020). However, because neither test was significant at .01, the researcher failed to reject the null hypotheses that there is no overall difference between groups.

Non-significant Demographic Variables

This research also probed to determine whether respondents' answers in the 15 composite variables differed according five other independent variables, however none of these proved statistically significant. The first non-significant variable was the "number of offices supervised", specifically if an IT Director supervised two or more offices versus supervising just one (see Table 47). This dichotomous independent variable was included as the researcher suspected an inverse relationship between the number of office supervised and the need for the office to seek outside assistance.

Table 47: Mann-Whitney Test for the Independent Variable “Supervise Only One Office”

	Variable	U	Sig.
	Index of Frequency of Contact w/ FEDERAL offices	857.0	.333
	Index of Frequency of Contact w/ STATE offices	867.5	.720
	Index of Frequency of Contact w/ Other COUNTIES	736.5	.188
	Index of Frequency of Contact w/ Other GOVERNMENTS in the County	739.0	.072
	Index of Frequency of Contact w/ Other DEPARTMENTS in the County	701.5	.123
	Index of Frequency to Seek technical assistance	957.5	.357
	Index of Frequency to Seek non-technical assistance	881.5	.250
	Index of Frequency to Seek program or project information	733.5	.073
	Index of Frequency to Seek resources or funding	1046.0	.997
	Index of Frequency to Seek legal or policy guidance	887.0	.227
	Index of Frequency to Seek regulatory or policy flexibility	938.5	.390
	Index of Frequency to Modify duties/procedures of a partnership	791.5	.076
	Index of Frequency to Modify resource/ funding obligations of a partnership	936.0	.503
	Index of Relationship Importance	997.0	.914
	Index of Relationship Development	846.0	.163

The second non-significant variable looked at “the number of employees supervised” by each IT Director (see Table 48). This variable was included as the researcher suspected an inverse relationship between the number of IT employees on staff and the need for the office to seek outside assistance. That is, the more employees in an office, the less likely the need would arise to seek outside assistance.

Table 48: Kruskal-Wallis Tests for “Number of Employees Supervised”

	Variable	H*	Sig.
	Index of Frequency of Contact w/ FEDERAL offices	8.752	.033
	Index of Frequency of Contact w/ STATE offices	2.844	.416
	Index of Frequency of Contact w/ Other COUNTIES	1.199	.753
	Index of Frequency of Contact w/ Other GOVERNMENTS in the County	6.248	.100
	Index of Frequency of Contact w/ Other DEPARTMENTS in the County	1.412	.703
	Index of Frequency to Seek technical assistance	2.449	.485
	Index of Frequency to Seek non-technical assistance	.342	.952
	Index of Frequency to Seek program or project information	1.053	.788
	Index of Frequency to Seek resources or funding	4.043	.257
	Index of Frequency to Seek legal or policy guidance	2.284	.516
	Index of Frequency to Seek regulatory or policy flexibility	.088	.993
	Index of Frequency to Modify duties/procedures of a partnership	1.588	.662
	Index of Frequency to Modify resource/ funding obligations of a partnership	.198	.978
	Index of Relationship Importance	2.339	.505
	Index of Relationship Development	2.394	.495

*NOTE: all DF = 3

The third non-significant variable was the size of the county population the respondent serviced (see Table 49). This was explored as the researcher suspected that offices in counties with larger populations might have more sophisticated IT systems which might in turn lead to and/or require more intergovernmental and interorganizational contact.

Table 49: Kruskal-Wallis Tests for “Number of Office Supervised”

	Variable	H*	Sig.
	Index of Frequency of Contact w/ FEDERAL offices	.875	.831
	Index of Frequency of Contact w/ STATE offices	6.500	.090
	Index of Frequency of Contact w/ Other COUNTIES	5.827	.120
	Index of Frequency of Contact w/ Other GOVERNMENTS in the County	1.299	.729
	Index of Frequency of Contact w/ Other DEPARTMENTS in the County	.654	.884
	Index of Frequency to Seek technical assistance	3.736	.291
	Index of Frequency to Seek non-technical assistance	4.308	.230
	Index of Frequency to Seek program or project information	.375	.945
	Index of Frequency to Seek resources or funding	1.119	.773
	Index of Frequency to Seek legal or policy guidance	1.682	.641
	Index of Frequency to Seek regulatory or policy flexibility	3.480	.323
	Index of Frequency to Modify duties/procedures of a partnership	.074	.995
	Index of Frequency to Modify resource/ funding obligations of a partnership	.943	.815
	Index of Relationship Importance	2.685	.443
	Index of Relationship Development	4.437	.218

*NOTE: all DF = 3

The fourth non-significant variable was the level of intergovernmental revenue received by the county the respondent serviced (see Table 50). This variable was included as the researcher suspected that there might be a positive relationship between the amount of intergovernmental funding received and the rate of intergovernmental and interorganizational contact.

Table 50: Kruskal-Wallis Tests for “County Intergovernmental Revenue”

	Variable	H*	Sig.
	Index of Frequency of Contact w/ FEDERAL offices	1.431	.698
	Index of Frequency of Contact w/ STATE offices	8.394	.039
	Index of Frequency of Contact w/ Other COUNTIES	6.669	.083
	Index of Frequency of Contact w/ Other GOVERNMENTS in the County	.810	.847
	Index of Frequency of Contact w/ Other DEPARTMENTS in the County	.582	.901
	Index of Frequency to Seek technical assistance	3.018	.389
	Index of Frequency to Seek non-technical assistance	3.756	.289
	Index of Frequency to Seek program or project information	.520	.914
	Index of Frequency to Seek resources or funding	1.476	.688
	Index of Frequency to Seek legal or policy guidance	2.934	.397
	Index of Frequency to Seek regulatory or policy flexibility	4.088	.252
	Index of Frequency to Modify duties/procedures of a partnership	1.247	.742
	Index of Frequency to Modify resource/ funding obligations of a partnership	1.192	.755
	Index of Relationship Importance	3.801	.284
	Index of Relationship Development	3.580	.311

*NOTE: all DF = 3

The fifth and final non-significant variable was the zone of the state which the county, hence office, is located (see Table 51). This variable was included as the researcher attempted to capture any regional characteristics and behaviors thus illuminate underlying qualities and influential factors not readily perceptible via other demographics. Specifically, does any particular zone exhibit unique patterns of intergovernmental contact. It should be noted that Zone 1 (see Figure 2) was underrepresented in this study which could have contributed to test outcomes.

Table 51: Kruskal-Wallis Tests for “ Zone”

	Variable	H*	Sig.
	Index of Frequency of Contact w/ FEDERAL offices	2.341	.505
	Index of Frequency of Contact w/ STATE offices	4.958	.175
	Index of Frequency of Contact w/ Other COUNTIES	5.226	.156
	Index of Frequency of Contact w/ Other GOVERNMENTS in the County	.755	.860
	Index of Frequency of Contact w/ Other DEPARTMENTS in the County	3.335	.343
	Index of Frequency to Seek technical assistance	1.084	.781
	Index of Frequency to Seek non-technical assistance	3.809	.283
	Index of Frequency to Seek program or project information	1.780	.619
	Index of Frequency to Seek resources or funding	1.376	.711
	Index of Frequency to Seek legal or policy guidance	3.50	.320
	Index of Frequency to Seek regulatory or policy flexibility	4.773	.189
	Index of Frequency to Modify duties/procedures of a partnership	.318	.957
	Index of Frequency to Modify resource/ funding obligations of a partnership	.859	.835
	Index of Relationship Importance	.796	.850
	Index of Relationship Development	3.598	.308

*NOTE: all DF = 3

In reference to Research Question Three, which under-lays the various points of exploration just discussed, the data indicated that there is a relationships between certain office/county demographics and the IGM activity of IT Directors. Specifically, a relationship exists between the IGM activities of an IT Director and: the type of office supervised; the percent of duties which the Director focuses on IT related issues; the percent of county population with post-secondary education; and the overall adequacy of IT budget.

Conversely, there appears to be no statistically significant relationship between the IGM activity of an IT Director and: the regional zone in which an office/county is located; the number of employees which the IT Director supervises; the number of

offices which the IT Director supervises; the population size of the county; or the level of intergovernmental revenue received by the county in which the office is located.

Summary

An analysis of the data obtained from this electronic survey of 125 IT Directors of constitutional offices of Florida counties has been presented in this chapter. Grounded in the literature on information technology and security, as well as the theory of intergovernmental management, this analysis explored the relationships between nine independent variables and 15 dependent index variables. Through univariate analysis, it was determined that most variables violated the assumptions of parametric tests due to heavily skewed data or non-normal distributions. While the skews of most independent variables were lessened via ordinal recoding, none of the dependent variables could be corrected without losing valuable information. This proved to severely limit the intended analysis as parametric tests were no longer appropriate. In light of the violated assumptions, non-parametric tests were used, specifically, Kruskal-Wallis and Mann-Whitney.

Since non-parametric tests are not as conservative as parametric tests in preventing Type I errors, the significance level was lowered from .05 to .01. However, as Hair et al (1998) note, by attempting to lessen the chance of committing Type I Errors one concurrently reduces the power of the statistical test which dictates the probability of successfully finding differences when they actually exist. Therefore, the

statistical results presented here most likely underestimate true difference as the researcher increased the probability of committing Type II errors, that is, failing to reject a null hypothesis when it is actually false.

To explore research questions one and two descriptive statistics, specifically modes and frequencies were examined. Analysis revealed that county IT Directors most often seek intergovernmental assistance horizontally, from other Departments within their own governments. Further, they seek intergovernmental assistance the least often vertically, from Federal offices. The most frequently performed intergovernmental activity was seeking technical assistance, however seeking program/project information was also performed more frequently than the six other activities explored in this research. The two least frequently performed activities were seeking to modify either the duties/procedures or the resources/funding obligations of an established partnership/agreement relating to IT.

To explore research question three, whether there were relationships between select office/county demographics and the IGM activity of IT Directors, non-parametric Kruskal-Wallis test for independent groups were used when the independent variable had three or more groups. Eight of the nine independent variables satisfied this condition (the ninth independent variable was dichotomous, “supervise one office versus supervise more than one office” therefore Mann-Whitney U was used, however, no statistical relationships were found). Testing these eight variables with each of the 15 indexes resulted in 126 tests of which five were statistically significant at .01. These significant tests were followed up with Mann-Whitney U tests to determine specifically which group(s) differ from which other group(s). Of these tests, seven were statistically

significant. Finally, in an effort to determine what was driving the significance, Mann-Whitney U tests were re-run between the seven groups which proved statistically different and the underlying factors of the relevant index variable. Of these tests, 14 were statistically significant.

Four of the five significant Kruskal-Wallis tests indicated that differences between respondents intergovernmental and interorganizational behaviors were due to difference in the type of office supervised. Specifically, the frequency with which a respondent: contacts federal offices; contacts offices in other governments located within county jurisdiction; seeks funding or resources; and the overall perceived importance of their relationships with different governments were not the same for all six types of offices.

Further exploration revealed that most of the differences occur between IT departments in Board of Commissioner's offices versus the IT departments of other types of constitutional offices. While perhaps it could be expected that Board of Commissioners offices would have a higher level of INTRA-county horizontal contact as this office is often the anchor for county-wide programs; however data revealed that this higher contact extended beyond the county. In particular, when compared to other constitutional offices, IT departments in Board of Commissioners offices more frequently contact other governments located within the jurisdiction of their county for seven of the eight activities included in this research (the exception being "seeking to modify resource/funding obligations with a partner/agreement" for which differences were not significant).

IT departments in Board of Commissioners offices also more frequently contact federal offices to seek program/project information and regulatory/policy flexibility than

other offices. Additionally, they contact federal offices to seek legal/policy guidance more frequently than the other offices with the exception of Sheriff's offices which contact federal offices to seek legal/policy guidance the most frequently. The IT departments in Sheriff's offices also contact federal offices seeking non-technical assistance and resources/funding more frequently than the other types of offices, even Boards of Commissioners. At the other end of this spectrum, IT departments in Tax Collectors offices are the least likely to contact a federal office, particularly for legal or policy guidance.

Board of Commissioners offices also more frequently seek resources/funding from other departments within its county than do the other types of offices. Further the data suggests that compared to other types of constitutional offices, Boards of Commissioners place a higher level of relationship importance on both other departments within its own county as well other government within the jurisdiction of its county.

Exploring the fifth significant Kruskal-Wallis test revealed that on average, offices in counties with a higher percent of post-secondary graduates (23 percent or more) less frequently contact state offices seeking technical assistance, non-technical assistance, or program/project information than do offices in counties with a lower percent of post-secondary graduates. However, it is not know if that is because the employees are truly more competent.

The analysis presented in this chapter examined the prevalence of intergovernmental and interorganizational contact and activities as preformed by IT Directors in Florida county constitutional office as part of their information security

efforts. Findings are limited to this populations and are no generalizations should be beyond this population. However, the patterns and trends uncovered here serve as the first step toward understanding this unseen population and for developing a baseline for future comparison studies. The implications of these findings, the limitations, as well as suggested future research are discussed next in the final chapter.

VI. IMPLICATIONS

The purpose of this research was to explore the roles of intergovernmental management, activity, and communication in protecting the information systems of our critical infrastructure. Specifically, the aim was to investigate how county-level Information Technology Directors use intergovernmental relations and activities in securing critical information systems under their charge. To that end, this research sought to answer the questions: 1) which IGM activities do county IT Directors/staff most often perform; 2) do county IT Directors make more use of vertical or horizontal IGM relationships; 3) is there a relationship between office/county demographics and the IGM activities its IT Director/staff most often performs? The significance of the findings are twofold as there are theoretical implications as well as practical implications. Each of which are presented in this final chapter.

Theoretical Implications

The impetus for this research was not to test suppositions of the theory of Intergovernmental Management. Rather, the theory was used to guide research questions in an effort to discover and explain patterns of activity. Despite this fact, the research findings do have theoretical connotations which add to the body of research on intergovernmental management.

First, these findings challenge the theoretical notion that IGM involves the regular application coping strategies, in addition to problem solving and networking (Agranoff & McGuire, 2001, 1998; Nelson, 2001; Bolman & Deal, 1999; Perry & Kraemer, 1999; Intergovernmental Advisory Board, 1998; Wright, 1998, 1992; Agranoff & Lindsay, 1983; Mandell, 1979). While these three activities are presented in the literature as unique functions, they naturally overlap in practice. For instance, a manager might employ coping strategies to best solve a certain problem however, not all problems can be solved using these solutions.

Of the eight activities explored in this research, three activities fall more closely inline with the application of coping strategies rather mere problem solving activities (see Chapter III for distinctions). Specifically, seeking regulatory/policy flexibility; seeking to modify the duties/procedures of an established partnership/agreement; and seeking to modify the resources/funding obligations of an established partnership/agreement are all fundamentally coping strategies. Likewise, two activities fall more closely inline with problem solving activities rather than coping strategies, specifically, seeking technical assistance and seeking non-technical assistance. However, of all eight activities in this study, the respondents performed the three coping activities the least often and performed the two problem solving activities the most frequently. Therefore, findings from this research would suggest that employing coping strategies is not a regular a part of intergovernmental management as the literature would imply.

Indeed local governments are regularly required to comply with vague policies and implement ill-fitted programs from state and federal agencies. In such situations,

where a policy must be adhered or a program produces unintended negative outcomes, the literature states that a primary function of intergovernmental management is to provide coping mechanisms (Agranoff, 2000; Bohte & Meier, 2000; Cooper et al., 1998; Center for Technology and Government, 1997a; Stever, 1993; Turner, 1990; Stenberg, 1984). Specifically, localities often revert to coping strategies to attempt to either change official policy/program specifics or they seek regulatory/statutory relief, flexibility, or waivers (Radin, 2000; Wright, 1983).

Yet, employing coping techniques and mechanisms do more than just accommodate jurisdictional idiosyncrasies; they inadvertently test and refine the details, structure, and overall viability of the very relationships and initiatives they preserve. By challenging policies, rules, procedures, and relationships, coping strategies, enacted via intergovernmental management, extend the principle of checks and balances and enliven experimentation and innovation. By implementing reactive coping techniques, intergovernmental managers can more effectively and efficiently fulfill mutual goals without a prolonged period of laboring through legislative channels (Chi, 2000, Radin, 2000). However adaptation and innovation require an investment of time and resources which often works to discourage such endeavors. When these barriers can be overcome, the coping function of intergovernmental management has the ability to generate more mature initiatives and foster progress (Falcone and Lan, 1997).

However, based on the discrepancy between the literature and these study findings, either the bulk of policies governing county IT Departments in Florida constitutional offices are adequate and on target or IT Directors lack the time and resources to develop innovative solutions. Thus the theoretical implication of this finding

is that either coping strategies are not a regular function of IGM or that only particular types of government offices are prone to use of coping strategies regularly. Only additional research could determine which is truly the case.

These research findings have another implication for the theory of intergovernmental management. Specifically, these findings support the notion that IGM occurs within two distinct environments, vertical and horizontal, with each often employing specific and distinct management activities (see Chapter II for discussion). As outlined in Chapter III, this research looked at how county IT directors interact vertically, with federal and state agencies above them, as well as horizontally, with external contemporaries including other counties, other governments located within the jurisdiction of the respondents own county, and other departments within the respondents own county. Analysis of the data found that while county IT Directors make more use of horizontal IGM relationships- they also make vertical contacts as part of their information security efforts.

Specifically, the data indicated that six of the eight activities were most often performed horizontally with other departments in the respondents county and two activities were most often performed vertically with the State. The two activities most often performed vertically are seeking regulatory/policy flexibility and seeking program/project information. It should be noted that it was anticipated to find that seeking regulatory/policy flexibility would be performed most often vertically as it is primarily a coping strategy which are regularly employed within subordinate/ordinate relationships. Thus the only way these problems can be addressed is vertically. Yet as mentioned in the prior discussion, this activity is rarely performed by the study

population (93 percent perform this activity only a few times a year or less). Other problems, however, can be addressed through horizontal efforts. Included among the six activities that are regularly performed horizontally are the predominantly problem solving activities; seeking technical and non-technical assistance. This would suggest that county IT Directors most often attempt to solve problems horizontally rather than vertically.

Taken together, findings from this research do not support the theoretical supposition that coping strategies are a regularly performed intergovernmental management activity. However, this research does support the assumption that IGM does indeed occur in both vertical and horizontal environments, whereby certain activities are more likely to be performed in one environment versus the other.

Practical Implications

Beyond the two theoretical implications of this research just discussed, there are also four distinct practical implications. The first practical implication of this research begins with the newly acquired knowledge that overwhelmingly, county IT Directors in Florida constitutional offices rarely -if ever- contact federal offices regarding IT related issues- be it to seek technical assistance or legal guidance, et cetera. This knowledge has practical significance because the federal response to critical infrastructure protection is driven in part by policies which state that federal agencies should be

providing outreach to state and local governments to aid their infrastructure protection efforts (see Chapter II for discussion).

This federal strategy, supported in large part by Presidential Decision Directive 63 of 1998, the 2003 National Strategy to Secure Cyberspace, and the newly created Department of Homeland Security, promotes a strong policy preference for consensus-building and voluntary cooperation rather than regulatory actions. Indeed, the U.S. General Accounting Office avers for infrastructure protection to succeed, “It is critical that all participating federal, state, and local agencies interact in a seamless manner” (2001c, p. 31). To this end, several federal offices have been tasked to work with state and local governments “...to ensure that systems are created and well managed to share threat warning, analysis, and recovery information among government network operation centers...” (Executive Order 13231, 2001, section 5a). Toward this end, collaborative public-private endeavors have been designed for sharing best practices; evaluating new technologies; raising cybersecurity awareness; increasing criminal justice activities; and developing national security programs to deter future cyber threats.

Yet, as discussed in Chapter V, the literature on information security suggests that local, state, and national agencies have yet to truly function in the spirit of cooperation, do not share enough information, and generally lack a coordinated working plan to deal with cyber attacks. This current research supports this assertion as study respondents overwhelmingly indicated that they never contact federal agencies for six of eight intergovernmental activities. Therefore, it appears that a main path of the national strategy, federal-to-local, is not an effective channel for disseminating elements

critical to information security including best practices, risk management, alerts/advisories, incident handling, and legislation.

This leads directly into the second practical implication of this research, namely the knowledge that local IT Directors, specifically those responsible for county constitutional offices, are more like to turn to a State office than a federal office for IT related assistance. Knowing that state offices, rather federal offices, are more preferred by local governments as a point of contact for IT related issues provides program and policy makers with a prudent direction from which to set about improving the national strategy.

Yet this research also found that the county IT Directors/staffs in this study population rarely initiate contact other government offices or departments for IT related assistance. Recall that all of the activity-related questions asked in the survey were presented in an active voice, for example, ...how often do you or your office seek to or attempt to 'xyz'. This research did not probe to find out how the directors/offices responded to being contacted. As such, the third practical implication of this research is by knowing that county IT Directors/staffs in the study population are not likely to initiate contact with other government offices on their own -program and policy makers could consider revising the national strategy whereby federal or state offices initiate regular interaction and thereby actively disseminate information rather than function as passive resources.

The fourth practical implication of this study goes beyond constitutional offices to the larger arena of public affairs. That is, knowing that IT Directors/staffs in the study population do not wholly operate in accordance with the national infrastructure

protection strategy by contacting federal offices, should serve to alert program and policy makers to the possibility that IT Directors in other types of offices in other types of local government may also slip through the national strategy. The implication of this to the various public affairs sectors, such as criminal justice, public administration, and social work, rest in the reality that beyond the 66 counties in Florida, there are over 87,000 units of local government providing vital services to the American public ranging from public safety, to health and social welfare, to public works (refer to Chapter II for full discussion). The operation of these local offices depends on the critical digital infrastructure, whether it is to supply them with power, to correctly route their financial transactions, or to enable them to communicate with the public. Therefore, the provision of such vital services depend on the unfettered operation of CDI.

These vital services are at the core of public affairs. For example, if a computer network supporting the criminal justice system were breached or cut off from other CDI elements, Fire Rescue, EMS, police, and others might be unable communicate to one another during emergencies. Dangerous fugitives or potential terrorists could unknowingly be admitted into the country or released from custody because police are unable access databases containing criminal histories. If a computer network supporting the public administration sector were compromised, programs supporting social security, unemployment, official records, passport applications, and drivers licenses, to name but a few, could be brought to a standstill. If a computer network supporting the social work and social services sector were penetrated or exploited, vital services from food stamps to Medicaid could not be provided because client files would inaccessible, corrupt, or even erased. Overall, numerous essential daily services could grind to a halt

if key elements of the CDI or any element therein were maliciously breached. In conjunction with our reliance on secure information networks, the findings of this current study point to the need for all public affairs sectors to determine the effectiveness of interorganizational and intergovernmental management and communication in the information security efforts of their local offices. It is critical that each sector, from criminal justice, to public administration, to social work be certain that its computer networks are supported by effective policies and procedures which are in accordance with the national infrastructure protection strategy.

As the literature reviewed for this research consistently avers, threats to the critical digital infrastructure do not just pertain to the information technology industry but rather to all sectors of the critical infrastructure and all parts of government. From regional correctional facilities to branch offices of the Department of Children and Family Services, local government offices increasingly rely on information and communication technologies to provide and improve the services they provide. As such, more and more units of local government, much like Florida county constitutional offices, are likely to retain their own IT Director or employ one between two or more offices. Literature on information management highlights three responsibilities unique to IT managers, (1) anticipating and understanding technological change, (2) anticipating and understanding information security, and (3) maintaining effective communication between IT and non-IT divisions. Merging these ideas, managers must approach information security as a mosaic, whereby each piece, or element, is understood in terms of the effect on the sum total. This also requires a mindfulness of elements which exist outside of a manager's immediate area of responsibility or authority, such as other

organizations with which relations take place. This is perhaps most especially true with regard to government information systems, for as the Center for Technology and Government (1997a) points out, "No government information system stands completely on its own. Each system is implemented in a work environment that includes people, processes, organizational relationships, and other systems" (p. 36). Therefore, if other units of local government follow patterns of behavior similar to Florida county constitutional offices, then best practice are not being shared, risk assessment is partitioned, and incident handling is fragmented, thus leaving the security of the critical digital infrastructure, and hence public affairs, in jeopardy.

Limitations

By and large there are five limitations to this research. First, an operational limitation stems from the ethical considerations inherent in studying security issues. The need to obscure specific details intrinsic to the configuration of each county's information security naturally curtails the potential depth of analysis. However, despite this limitation, this research was able ascertain the current breadth and interplay between intergovernmental activities and information security in Florida counties.

There are three limitations with the design of the research. Specifically, when conducting email or Internet surveys, there can be considerable variation among respondents systems, such as different screen sizes, set preferences, and email clients, such as Microsoft Outlook, GroupWise, or Hotmail. The various system permutations

can result in disparities between the visual design of the questionnaire, such as misalignment (Dillman, 2000). However, in a personal correspondence to the researcher (dated 03/27/03), a technician at Surveymonkey.com reassured that the company was aware of this issue and they continually test and modify their programming to compensate for such variations. Thus, lessening this limitation. The third limitation of this research was the narrow study population. While this drawback limits generalizability, the findings can be used as a baseline for future comparison studies with counties in other states and as well as city governments. As such, this research serves as a first step to illuminate the prevalence of intergovernmental management activities in information security efforts.

The fourth limitation is due to the fact that IT Directors were asked to quantify the intergovernmental activities of the staffs they supervise. Although IT Directors were asked to provide this second-hand observation, in this instance, they are functioning as Key Informants reporting the activities that regularly occur in the offices under their purview.

The fifth limitation is due to the non-normal distributions of the data. While every effort was made to produce a sound and rigorous examination of the issues under study, unavoidable limitations in the data restricted the statistical depth of this analysis. Because the alpha level was lowered to increase to power of the non-parametric tests, the statistical findings of this analysis should be viewed as conservative as true significant differences may have existed where none were reported.

Future Research

This research sought to investigate how county-level Information Technology Directors use intergovernmental relations and management activities as part of their information security efforts. However, to determine if intergovernmental assistance does indeed improve information security as claimed by the federal government and others, a future study should simultaneously assess the success each office has had in securing the information systems under their charge (i.e. noting rates of intrusion and denial of service) along with patterns and rates of intergovernmental activity.

It would be equally valuable for a future study to employ personal interviews to qualitatively explore why Florida county IT Directors rarely engage in intergovernmental contact. In particular, is it because they are able to solve most problems on their own? Perhaps because they turn to private or non-governmental sources for help? Or do they limit outside input, hence interaction, in an effort to protect their turf?

A third direction for future research would be to explore the information security of the 18 percent of Florida constitutional office that outsource their IT needs. As noted in Chapter V, when developing the population list for this current research, 72 offices indicated that they hire a private company to take care of their information technology and security. In actuality, this number is most likely much higher as the researcher was unable to determine the IT Director for 63 other offices, even after multiple attempts, leading the researcher to believe that many of these offices do not have one on staff. Nonetheless, offices without a public IT Director were not included in this research as a private vendor could not function intergovernmentally in the truest sense. This creates

many questions, such as where do these vendors turn for IT assistance or legislative/policy guidance? How do these contracted vendors interact with the myriad of government offices involved in critical infrastructure protection, such as Florida Department of Law Enforcement, State Technology Office of Florida, the FBI, and Department of Homeland Security, to name but a few? And perhaps the most pertinent question which could be answered from the convergence of the studies proposed here, which offices are the most secure- the ones supervised by a county IT Director who rarely engages in intergovernmental contact; the ones supervised by a county IT Director who regularly engages in intergovernmental contact; the ones supervised by a private vendor who rarely contacts government offices; or finally, the ones supervised by a private vendor who regularly contacts government offices?

A fourth area for future research would address differences between the structure of IT departments in the various zone of the state which were identified here. Specifically, a qualitatively study using focus groups could help to determine what is driving the differences. The insight gained could then be utilized to attempt to gauge the effectiveness of the variously configurations and develop state-wide standards and best practices.

A final direction for future research would address the issue of generalizability. As noted in the previous section, the knowledge gained from this study can only be transferred to the larger public affairs arena to alert program and policy makers to the possibility that IT Directors may be slipping through the national strategy. However, these study findings, in and of themselves, can not be generalized to different populations. Therefore, future research should expand beyond constitutional offices,

counties, and the state of Florida to explore information security in different settings and local government environments. Only then would there be a clear picture as to the role and effectiveness of intergovernmental management and communication in securing local elements of the national critical infrastructure.

Concluding Remarks

From military operations to hospital nursing stations, networked computers have come to play a role in most every sphere of modern public affairs. The literature reviewed for this research indicates that a well-coordinated large-scale cyber attack has the potential to disrupt daily life in America and across the global. As cyber attacks become more sophisticated, the risk to ALL networked systems increases. Whether public or private, whether federal, state, or local, the threat is equally real.

Consequently, county leaders must respond accordingly to understand the threats, take measures to protect themselves, and determine how they will respond in the event that they are attacked, or if parts of the critical digital infrastructure were rendered inoperable. Along side their national and subnational peers, county Information Technology Directors work on the frontlines trying to balance public demands and entrepreneurial growth with the realities of cyber security and national defense. By working intergovernmentally, they make use of innate networks, seek to solve problems, and to a lesser extent employ coping strategies.

The rise of the Information Age challenges us to update antiquated modes and ideas of security, government, privacy, and borders. Information security incidents do not respect geographic or administrative boundaries therefore, management must be prepared to instantly interact with other governments, agencies, and at the very least departments, to contain a system breach. The lack of good communication can breed confusion, poor coordination, and loss of services. The U.S. General Services Administration firmly states that intergovernmental management will be *the* challenge for information security the next 20 years (McDonough, 2002). Several converging conditions support this position including a demonstrated need to integrate distinct databases to meet homeland security needs and the presence of program overlap between numerous agencies in a time of budget deficits. Collectively, these and other conditions point toward the growing importance of integrated systems and collaboration which are at the heart of intergovernmental management.

In testimony before the U.S. House of Representatives Select Committee on Homeland Security, the U.S. Comptroller General stated the indisputable need to "...clarify the appropriate roles and responsibilities of federal, states, and local entities and build a framework for partnerships for coordination, communication, and collaboration" (Walker, 2002, p. 4). Discerning the roles of interorganizational and intergovernmental management, activities, and communication in the information security efforts of local government is a necessary step toward these ends.

Critical digital infrastructure protection is a complex social, economic, and administrative issue that affects the health, welfare, and security of citizens in all communities. Without assessing the effectiveness of intergovernmental collaboration

and communication, which lay at the heart of the federal protection strategy, our national security remains vulnerable. Only by examining actual information security efforts, as this current research has done, will we be able to effectively protect our critical digital infrastructure from the largely invisible threats discussed in here. As illustrated in this chapter, the findings of this current research have both theoretical and practical implications. It is the express hope of this researcher that they be used to generate dialogue as well as a deeper inquiry into the intergovernmental and local dimensions involved in protecting the U.S. critical digital infrastructure and ensuring our modern way of life.

APPENDIX A: INTRODUCTORY LETTER

«first» «last»
«Title»
«street»
«city», «state» «zip»

November 4, 2003

Dear «salutation» «last»,

My name is Joah Devenny, I am a Ph.D. Candidate at the University of Central Florida. Next week I will conduct a survey that explores how Florida county Information Technology Directors interact with their peers to stay on top of changing technology and threats. I am writing you to ask you to take part in this valuable research.

You have been chosen to participate because of the critical role you play in protecting local aspects of the critical digital infrastructure. By learning how you interact with your peers, officials will be able to develop policies better suited to your *actual* day-to-day activities, rather than what they *think* you do.

On Monday, November 10th, you will receive an email from infosec@mail.ucf.edu. This email will include a hyperlink to a web survey hosted by surveymonkey.com.

**The survey is ONLY 16 questions and will take just 7 minutes to complete.

** You will NOT be asked ANY sensitive questions about your information security configurations. You will ONLY be asked how often you interact with certain peers and basic questions about your county.

Your participation is voluntary and responses will be strictly CONFIDENTIAL. Only summary data will be discussed in the final report. For more details of this research, please review the enclosed information sheet.

To verify the authenticity of this research request feel free to call the UCF Public Affairs Doctoral Program at (407)-823-0170. Should you have any question please contact Joah Devenny at (352) 795-5064.

Thank you for your consideration,

Joah Devenny, M.A.
Doctoral Candidate/Principle Researcher

Advisory Committee
Eileen Abel, Ph.D.
Stephen Holmes, Ph.D.
Ronnie Korosec, Ph.D.
Mary Van Hook, Ph.D.

Research Information Sheet

Please read the following information to decide if you would like to participate in this study. This information will be represented to you in the survey. It will be followed by a question asking whether you have read the study procedure and voluntarily agree to participate. If you agree, please check the box that will be provided in the survey.

Research title:	Critical Digital Infrastructure Protection and the Intergovernmental Activities of Information Technology Directors in Florida Counties
Research purpose:	To investigate how county-level Information Technology Directors use intergovernmental relations and management activities in securing critical information systems and assets under their charge.
What you will be asked to do:	You will be asked 1) to click on a hyperlink you will receive in a email which will take you to an Internet survey; 2) you will then be asked to answer 16 non-sensitive multiple-choice questions.
Time required:	Seven (7) minutes
Risks:	There are no known risks for participation.
Benefits and Compensation:	There is no compensation or other direct benefit to you for participation.
Confidentiality:	All answers will be kept in an encrypted data file in the researcher's secure office. Your identity and the county you work for will be kept confidential and not used in any report.
Voluntary participation:	Your participation is voluntary. There is no penalty for not participating. You do not have to answer any question you do not wish to answer.
Right to withdraw from the study:	You have the right to withdraw from the study at any time without consequence
Whom to contact if you have questions:	Joah Devenny, M.A., Doctoral Candidate, Public Affairs Doctoral Program, Orlando, FL 32816; (352)795-5064 -or- Eileen Abel, Ph.D., Research Supervisor, (407)823-0170.
Whom to contact about your rights:	UCF-IRB Office of Research, 12443 Research Parkway, Suite 207, Orlando, FL 32826; (407) 823-2901.

APPENDIX B: EMAIL

Dear {recipient},

A few days ago, you should have received a letter asking you to take part in an important survey on information security approved by the University of Central Florida.

Specifically, this research explores how county Information Technology Directors interact with other governments. Please volunteer a moment of your time to represent {xx county} and share your experiences.

** The survey is ONLY 16 questions and takes just 7 minutes to complete.

** You will NOT be asked ANY sensitive questions about your information security configurations.

** You will ONLY be asked how often you interact with certain peers for 10 activities plus 6 basic questions about your county.

To complete the survey please click the link below or type the link into a browser window.

[Survey Link]

The survey begins with some general information about the research. It is followed by a question asking whether you have read the details and voluntarily agree to participate. If you agree, you will be asked to check the box provided before you begin the survey.

Should you have *any* question please feel free to contact Joah Devenny at (352) 795-5064.

Thank you for your valuable time,

Joah Devenny, M.A.
Principle Researcher

Advisory Committee

Eileen Abel, Ph.D.
Stephen Holms, Ph.D.
Ronnie Korosec, Ph.D.
Mary Van Hook, Ph.D.

APPENDIX C: SURVEY INSTRUMENT

Intergovernmental Information Security Activities
of Florida Counties

Thank you for agreeing to participate in this important research.
Please take a moment to read the following study details.

Research Purpose: To investigate how county-level Information Technology Directors use intergovernmental relations and management activities in securing critical information systems and assets under their charge.

What you will be asked to do: You were already asked to click on a hyperlink to take you to this survey; now you will be asked to answer 16 multiple-choice questions.

Risks: There are no known risks for participation.

Benefits and Compensation: There is no compensation or other direct benefit to you for participation.

Voluntary participation: Your participation is voluntary. There is no penalty for not participating. You do not have to answer any question you do not wish to answer.

Right to withdraw from the study: You have the right to withdraw from the study at any time without consequence

Confidentiality: All answers will be kept in an encrypted data file in the researcher's secure office. Your identity and the county you work for will be kept confidential and not used in any report.

Whom to contact about participants' rights: UCF-IRB Office of Research, 12443 Research Parkway, Suite 207, Orlando, FL 32826; (407) 823-2901.

Please select one of following statement:

I have read the study description just provided and I voluntarily AGREE to participate in the study.

I have read the study description just provided and I DO NOT AGREE to participate in the study.

Next -- >>

Thank you for agreeing to participate. For all questions, the following definition is implied:

Information Security: actions taken to reduce the probability that a threat will exploit a system vulnerability. This includes measures to ensure confidentiality, integrity, and availability of system assets.

1. Which Florida county do you work for?

[drop box with all counties listed]

2. Please select ALL of the following county units that fall under your supervision for their information security needs:

- ALL county departments and offices fall under my supervision
- Board of County Commissioners
- Clerk of Court
- Property Appraiser's Office
- Supervisor of Elections' Office
- Sheriffs Office
- Tax Collector's Office
- County Administration/Management
- Emergency Management
- Fire and Rescue Services
- Health and Human Services
- Public Works
- Utilities
- Other (please specify)

3. Thinking about the areas YOU SUPERVISE, please indicate whether each of the following ONLINE SERVICES are outsourced, provided by the county itself, or not provided at all:

	Currently outsourced	Currently provided by the county itself	Not currently provided
Permit or license application			
Searchable Public Records			
Filing electronic employment applications			
Requests for services (streetlight repair, potholes, etc.)			
Payment of Utility Bills			
Voter Registration			
Payment of Tickets or Fines			
Payment of Taxes			

4. How adequate is the funding you are able to apply to each of the following needs?

	Above Adequate	Adequate	Below Adequate	Far Below Adequate	Not Applicable
IT equipment/ software/ hardware					
IT security equipment, software, and hardware					
Hiring outsource vendors					
Hiring IT personnel and support staff					
Training IT personnel					
Computer security education for NON IT employees					
Risk assessment/ management					

5. Faced with shrinking budgets, counties often require managers to perform more than one job. For example, a county might combine the job of "Administrative Services Director" with that of "Facilities Management Director".

Thinking about your own job, what percent of your duties focus on information technology or information security related issues?

- 100%
- 80%
- 60%
- 40%
- 20%
- less than 20%

6. How many employees do you supervise whose job deals ONLY with information technology or information security?

[drop box with 0-"25 or more" listed]

<< -- Previous Next -- >>

The final 10 questions ask how often YOU OR YOUR STAFF engage in certain activities with the each following TYPES of governments.

FEDERAL: any office, agency, or department, such as FBI, FEMA, Department of Homeland Security, CERT, etc...

STATE: any office, agency, or department, such as FDLE, State Technology Office, Secure Florida, etc...

OTHER FLORIDA COUNTIES: any office or department located in ANOTHER county government, such as another county's Department of Information Technology; Clerk of Court office; Sheriffs Office; etc...

OTHER GOVERNMENTS LOCATED WITHIN THE JURISDICTION OF YOUR COUNTY: any part of a government unit located within the jurisdiction of your county, such as a city or township; etc...

OTHER DEPARTMENTS WITHIN YOUR COUNTY

<< -- Previous Next -- >>

How often do YOU OR YOUR STAFF engage in the following activities with each of the following types of governments:

7. Seek technical assistance related to information security...

	Weekly	Monthly	Several times a year	A few times a Year	Never
Federal					
State					
Other Florida Counties					
Other governments located WITHIN the jurisdiction of your county					
<i>Other departments in YOUR county governments</i>					

8. Seek NON-technical assistance related to information security...

	Weekly	Monthly	Several times a year	A few times a Year	Never
Federal					
State					
Other Florida Counties					
Other governments located WITHIN the jurisdiction of your county					
<i>Other departments in YOUR county governments</i>					

9. Seek information on an information security program or project...

	Weekly	Monthly	Several times a year	A few times a Year	Never
Federal					
State					
Other Florida Counties					
Other governments located WITHIN the jurisdiction of your county					
<i>Other departments in YOUR county governments</i>					

10. Seek funding or resources to improve information security efforts...

	Weekly	Monthly	Several times a year	A few times a Year	Never
Federal					
State					
Other Florida Counties					
Other governments located WITHIN the jurisdiction of your county					
<i>Other departments in YOUR county governments</i>					

11. Seek legal or policy guidance regarding information security...

	Weekly	Monthly	Several times a year	A few times a Year	Never
Federal					
State					
Other Florida Counties					
Other governments located WITHIN the jurisdiction of your county					
<i>Other departments in YOUR county governments</i>					

12. Seek regulatory or policy flexibility regarding information security...

	Weekly	Monthly	Several times a year	A few times a Year	Never
Federal					
State					
Other Florida Counties					
Other governments located WITHIN the jurisdiction of your county					
<i>Other departments in YOUR county governments</i>					

13. Attempt to modify duties or procedures of an established partnership/agreement relating to information security...

	Weekly	Monthly	Several times a year	A few times a Year	Never
Federal					
State					
Other Florida Counties					
Other governments located WITHIN the jurisdiction of your county					
<i>Other departments in YOUR county governments</i>					

14. Attempt to modify resource-sharing or funding obligations of an established partnership/agreement related to information security...

	Weekly	Monthly	Several times a year	A few times a Year	<i>Never</i>
Federal					
State					
Other Florida Counties					
Other governments located WITHIN the jurisdiction of your county					
<i>Other departments in YOUR county governments</i>					

15. Overall, how IMPORTANT is each of the following TYPE of government to the success of your information security efforts...

	Extremely Important	Very Important	Important	Somewhat Important	<i>Not very Important</i>
Federal					
State					
Other Florida Counties					
Other governments located WITHIN the jurisdiction of your county					
<i>Other departments in YOUR county governments</i>					

16. Overall, how DEVELOPED is the relationship between your IT department and each of the following TYPES of government...

	Extremely Developed	Very Developed	Developed	Somewhat Developed	<i>Not very Developed</i>
Federal					
State					
Other Florida Counties					
Other governments located WITHIN the jurisdiction of your county					
<i>Other departments in YOUR county governments</i>					

<< -- Previous Next -- >>

Thank you for your valuable time.

Should you have any questions or would like to receive an electronic summary of the research findings, please contact:

Joah Devenny, M.A.
Principle Research

Public Affairs Doctoral Program
University of Central Florida
Orlando, FL 32816
infosec@mail.ucf.edu
352-795-5064

<<-- Previous [Click here to close window.](#)

APPENDIX D: FIRST FOLLOW-UP EMAIL

Dear {recipient},

Last week you should have received an email asking you to take part in an important survey, approved by the University of Central Florida, which explores how county-level Information Technology Managers interact with other governments.

If you have not yet completed the survey, please know that your participation is ***VERY IMPORTANT***. Only YOU can shed light on this important aspect of information security.

By learning how you and your peers interact, policy makers will be able to develop legislation better suited to YOUR day-to-day activities rather than what they THINK you do. Please take a moment of your time to represent {xx county} and share your experiences.

** The survey is ONLY 16 questions and takes just 7 minutes to complete.

** You will NOT be asked ANY sensitive questions about your information security configurations.

** You will ONLY be asked how often you interact with certain peers for 10 activities plus 6 basic questions about your county.

To complete the survey please click the link below or type the link into a browser window.

[Survey Link]

Should you have any question please contact Joah Devenny at (352) 795-5064 or Dr. Eileen Abel at (407) 823-3967.

Thank you for your cooperation,

Joah Devenny, M.A.
Principle Researcher

Advisory Committee

Eileen Abel, Ph.D.
Stephen Holms, Ph.D.
Ronnie Korosec, Ph.D.
Mary Van Hook, Ph.D.

APPENDIX E: SECOND FOLLOW-UP EMAIL

Dear {recipient},

It was a pleasure speaking with you on the phone today regarding the important role you play in protecting local information security systems. Also, thank you for allowing me to explain my current research into how county-level Information Technology Managers interact with other governments.

I'd like to take a quick moment to remind you how vital this research is to understanding how you and your government peers interact. The findings of this research will help policy makers develop legislation better suited to YOUR day-to-day activities.

Your participation is ***VERY IMPORTANT***. Only YOU can shed light on this important aspect of information security. Please take a moment of your time to represent {xx county} and share your experiences.

** The survey is ONLY 16 questions and takes just 7 minutes to complete.

** You will NOT be asked ANY sensitive questions about your information security configurations.

** You will ONLY be asked how often you interact with certain peers for 10 activities plus 6 basic questions about your county.

To complete the survey please click the link below or type the link into a browser window.

[Survey Link]

Should you have any question please contact Joah Devenny at (352) 795-5064 or Dr. Eileen Abel at (407) 823-3967.

Thank you for your cooperation,

Joah Devenny, M.A.
Principle Researcher

Advisory Committee

Eileen Abel, Ph.D.
Stephen Holms, Ph.D.
Ronnie Korosec, Ph.D.
Mary Van Hook, Ph.D.

APPENDIX F: UCF INSTITUTIONAL REVIEW BOARD APPROVAL



Office of Research

November 7, 2003

Joah Devenny
[REDACTED]
[REDACTED]

Dear Ms. Devenny:

With reference to your protocol entitled, "Critical Digital Infrastructure Protection and the Intergovernmental Activities of Information Technology Directors in Florida Counties," I am enclosing for your records the approved, executed document of the UCFIRB Form you had submitted to our office.

Please be advised that this approval is given for one year. Should there be any addendums or administrative changes to the already approved protocol, they must also be submitted to the Board. Changes should not be initiated until written IRB approval is received. Adverse events should be reported to the IRB as they occur. Further, should there be a need to extend this protocol, a renewal form must be submitted for approval at least one month prior to the anniversary date of the most recent approval and is the responsibility of the investigator (UCF).

Should you have any questions, please do not hesitate to call me at 823-2901.

Please accept our best wishes for the success of your endeavors.

Cordially,

A handwritten signature in black ink, appearing to read "Chris Grayson".

Chris Grayson
Institutional Review Board (IRB)

Copies: Eileen Abel, Ph.D.
IRB File

**IRB COMMITTEE APPROVAL FORM
FOR UCF/OOR/IRB USE ONLY**

PI(s) Name: Joah Devenny

Title: Critical Digital Infrastructure Protection and the Intergovernmental Activities of Information Technology Directors in Florida Counties.

Check as applicable (optional):

- Yes No Have sufficient assurances been given to the committee to establish that the potential value of this research exceeds the risks involved?
- Yes No Written and oral presentations must be given to participating subjects (parents or guardians, if minors) informing them of the protocol, possible risks involved, the value of the research, and the right to withdraw at any time.
- Yes No A signed written consent must be obtained for each human subject participant.
- Yes No Are cooperating institutions involved? If yes, was there a sheet attached providing the name of the institutions, the number and status of participants, name of the involved official of the institution, telephone, and other pertinent information?

Committee Members:


Dr. Theodore Angelopoulos: _____
Ms. Sandra Browdy: _____
Dr. Jacqui Byers: _____
Dr. Ratna Chakrabarti: _____
Dr. Karen Dennis: _____
Dr. Barbara Fritzsche: _____
Dr. Robert Kennedy: _____
Dr. Gene Lee: _____
Ms. Gail McKinney: _____
Dr. Debra Reinhart: _____
Dr. Valerie Sims: _____

Contingent Approval
Dated: _____

Final Approval
Dated: _____

Expedited
Dated: 5 Nov 2003

Exempt
Dated: _____

Chair, IRB
Signed: 
Dr. Sophia Dziegielewska

LIST OF REFERENCES

- ABC Action News (2003). *Virus triple-punch Slows Down Bay Area Computer Users*. Retrieved 09/12/03 from <http://www.abcactionnews.com/stories/2003/08/030822virus.shtml>
- Agranoff, R. (1986). *Intergovernmental Management: Human Services Problem Solving in Six Metropolitan Areas*. Albany, NY: State University of New York Press.
- Agranoff, R., and Lindsay, V. A. (1983). Intergovernmental Management: Perspectives from Human Services Problem Solving at the Local Level. *Public Administration Review*, May/June, 227-237.
- Agranoff, R., & McGuire, M. (2001). American Federalism and the Search for Models of Management. *Public Administration Review*, 61(6), 671-681.
- Agranoff, R., & McGuire, M. (1999). Expanding Intergovernmental Management's Hidden Dimensions. *American Review of Public Administration*, 29(4), 352-369.
- Agranoff, R., & McGuire, M. (1998). A Jurisdictional-based Model of Intergovernmental Management in U.S. Cities. *Publius*, 28(4), 1-20.
- Allen, M. B. (1994). Intergovernmental Recordkeeping in the Information Age. *Intergovernmental Perspective*, Spring, 24-27.
- Allor, P. G. & Lindley, J. R. (2000). IT-ISAC - ISAC Defined. Retrieved 05/14/03 from <https://www.it-isac.org/isacinfowhtppr.php>
- Altshuler, A., Morrill, W., Wolman, H., & Mitchell, F. (1999). *Governance and Opportunity in Metropolitan America*. Committee on Improving the Future of U.S. Cities Through Improved Metropolitan Area Governance, National Research Council.
- Amarelo, M. (2003). *DHS Looks at Vulnerabilities, Priorities S&T Undersecretary McQueary Says at AAAS Colloquium*. Retrieved 05/15/03 from <http://www.aaas.org/news/releases/2003/0416colloq2.shtml>
- American City & County (2002). International Threats Hit Home for Local Leaders. *American City & County*, November 1.
- Ammons, D. N. (1999). Performance Measurement in Local Governments. In F. S. Lane (Ed.) *Current Issues in Public Administration* (6th ed.) (293-305). Boston: Bedford/St. Martin's.
- Anderson, K. (1999). *Intelligence-Based Threat Assessments for Information Networks and Infrastructures*. Retrieved 05/14/03 from http://www.aracnet.com/~kea/Papers/threat_white_paper.shtml
- Arrison, S. (2002). *An E-government Revolution*. Retrieved 04/18/03 from http://www.pacificresearch.org/pub/act/2002/act_02-01-15.html
- Associated Press. (2003, January 28). Weekend Internet Attack Exceeded Experts' Fears. *The St. Petersburg Times*, pp. E6.

- Associated Press. (2002, October 23). Key Internet Servers Hit by Attack. *CNN.com Technology*. Retrieved 10/23/02 from <http://www.cnn.com/2002/TECH/10/23/internet.attack.ap/index.html>
- August, R. H. (1994). Strategic Planning in Computer Services: Is the Tail Wagging the Dog? *ACM: Meet the Shadowy Future: Proceedings of the 22nd Annual ACM SIGUCCS Conference on User Services*, 49-52.
- Babbie, E. (1995). *The Practice of Social Research* (7th Ed.) Belmont, CA: Wadsworth Publishing Company.
- Barrett, K., Greens, R., & Mariani, M. (2002). Grading the Counties: A Management Report Card. *Governing*, 15(5), 21-89.
- Bay County Online. (2003). *Human Resources Division*. Retrieved 09/17/03 from <http://www.co.bay.fl.us/bchr/index.html>
- Berkowiz, B. (2001). Information Warfare: Time to Prepare. *Issues in Science and Technology*, 17(2), 37-44.
- Bettelheim, A, & Adams, R. (2001). America's Infrastructure at Risk: What is the Federal Role?. *Congressional Quarterly*, 59(37), 2259-2261.
- Bickel, D. R. (2002). Robust Estimators of the Mode and Skewness of Continuous Data, *Computational Statistics and Data Analysis*, 39, p. 153-163.
- Bissett, A. & Shipton, G. (2000). Some Human Dimensions of Computer Virus Creation and Infection. *International Journal of Human-Computer Studies*, 52, 899-913.
- Bohte, J. & Meie, K. J. (2000). The Marble Cake: Introducing Federalism to the Government Growth Equation. *Publius*, 30(3), 35-46.
- Bolman, L. G. & Deal, T. E. (1999). Reframing Organizational Leadership. In F. S. Lane (Ed.) *Current Issues in Public Administration* (6th ed.) (171-182). Boston: Bedford/St. Martin's.
- Borsboom, D., Mellenbergh, G. J., & van Heerden, J. (2003). The Theoretical Status of Latent Variables. *Psychological Review*, 110(2) p. 203-219.
- Bowser, B. (1998). www.localgovernment.com: Opening the window to on-line democracy. *American City & County*, Jan 1.
- Brock, J. L. (2000a). *Critical Infrastructure Protection: Challenges of Building a Comprehensive Strategy for Information Sharing* (GAO/T-AIMD-00-268). Statement before the Subcommittee on Government Management, Information, and Technology, Committee on Government Reform, U.S. House of Representatives, July 26, 2000. Washington, DC: U.S. General Accounting Office.
- Brock, J. L. (2000b). *Critical Infrastructure Protection: Comments on the National Plan for Information Systems Protection* (GAO/T-AIMD-00-72). Statement before the Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary, U.S. Senate, February 1, 2000. Washington, DC: U.S. General Accounting Office.
- Brune, T. (2000). Aim: Securing the Cyberfuture. *Newsday*. February 13 Issue, A3.
- Careless, J. (2003). *Security Conference Offers Weird, Woeful Predictions*. Retrieved 05/22/03 from <http://www.computerworld.com/securitytopics/security/story/0,10801,81402,00.html>

- Carlson, D. (1987). *Intergovernmental Relations*. Retrieved 02/02/10 from <http://www.nmu.edu/politicalscience/profpages/Carlson/federalism.pdf>
- Center for Strategic and International Studies. (1998). *Global Organized Crime Project*. Washington DC: Author.
- Center for Technology in Government. (2000). *Designing the Digital Government of the 21st Century: A Multidisciplinary Workshop*. Albany, NY: Author.
- Center for Technology in Government. (1997a). *Tying a Sensible Knot: A Practical Guide to State-Local Information Systems*. New York: University of Albany/ SUNY.
- Center for Technology in Government. (1997b). *Partners in State-Local Information Systems: Lessons from the Field*. Albany, NY: Author.
- CERT. (2003). *CERT/CC Statistics 1988-2003*. Retrieved 06/02/03 from <http://www.cert.org/stats/>
- Chafetz, J. S. (1978). *A Primer on the Construction and Testing of Theories in Sociology*. Itasca, Il., F. E. Peacock Publishers.
- Chan, Y. H. (2003). Biostatistics 102: Quantitative Data – Parametric & Non-parametric Tests. *Singapore Medical Journal* 44(8), 391-396.
- Charney, S. (1994). Computer Crime: Law Enforcement's Shift from a Corporeal Environment to the Intangible, Electronic World of Cyberspace. *Federal Bar News*, 41(7), 489 - 494.
- Cheney, G. (1999). Cyberfraud and Computer Crime. *Strategic Finance*, 81(5), 38-42.
- Chi, K. (2000). Administration of Innovations in State Government. In J. J. Gargan (Ed.) *Handbook of State Government Administration* (289-306). New York: Marcel Dekker, Inc.
- CIO. (2002). The State of the CIO. *CIO Magazine*. March 1.
- Clark, Richard E. (1998). *Terrorism, Cyber Security, and the Bill of Rights. Remarks to the American Bar Association Committee on Law and National Security*. Retrieved 09/18/01 from http://www.ciao.gov/CIAO_Document_Library/archives/RC_Speech_11-12-98_ABA.htm
- Cohen, F. (2000). *Statement before the Joint Economic Committee February 23, 2000*. Retrieved 02/5/01 from <http://www.cdt.org/security/dos/000223senate/cohen.html>
- Collins, J. S. (2001). *Pockets of Chaos: Management Theory for the Process of Computer Security*. Retrieved 05/03/03 from <http://www.sans.org/rr/start/chaos.php>
- Computer Science & Telecommunications Board and National Research Council. (2002). *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*. Washington, DC: National Academy Press.
- Committee on the Internet in the Evolving Information Infrastructure. (2001). *The Internet's Coming of Age*. Sponsored by Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, and National Research Council. Washington, D.C.: National Academy Press.
- Computer Security Institute. (2002). *CSI/FBI Computer Crime Survey*. San Francisco, CA: Author.

- Cooper, P.; Brady, L. P., Hidalgo-Hardeman, O., Hyde, A., Naff, K. C., Ott, J. S., & White, H. (1998). *Public Administration for the Twenty-First Century*. Fort Worth: Harcourt Brace College Publishers.
- Costello, S. (2001). Study: Nearly 4,000 DoS Attacks Occur per Week. Retrieved 05/25/01 from <http://www.cnn.com/2001/TECH/internet/05/24/dos.study.idg/index.html>
- Council for Excellence in Government. (2003). *The New E-government Equation: Ease, Engagement, Privacy & Protection*. Washington DC: Author.
- Cowings, J. (2001). *Strategic Leadership and Decision Making*. Retrieved 09/19/01 from <http://www.ndu.edu/ndu/inss/books/strategic/cont.html>
- Crescenzi, A. C. (1996). *Protecting American Assets- Who is Responsible?* Retrieved 01/22/03 from <http://security.isu.edu/pdf/AmerAssetsWhoRespons.pdf>
- Critical Infrastructure Assurance Office. (2002). *State and Local Government*. Retrieved 11/13/02 from <http://www.ciao.gov/state/index.html>
- Critical Infrastructure Assurance Office. (2000). *Practices for Securing Critical Information Assets*. Washington D.C.: author.
- CyberAtlas. (2003). Population Explosion! Retrieved 05/29/03 from http://cyberatlas.internet.com/big_picture/geographics/article/0,1323,5911_151151,00.html
- Dacey, R. F. (2003a). *Information Security: Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures* (GAO-03-564T). Testimony Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform, House of Representatives 04/08/2003. Washington DC: U.S. General Accounting Office.
- Dacey, R. F. (2003b). *Further Efforts Needed to Fully Implement Statutory Requirements in DOD* (GAO-03-1037T). Testimony Before the Subcommittee on Terrorism, Unconventional Threats and Capabilities, Committee on Armed Services, House of Representatives United States General Accounting Office GAO. 07/24/03. Washington DC: US General Accounting Office.
- Dacey, R. F. (2002). *Progress Made, But Critical Federal Operations and Assets Remain at Risk* (GAO-03-303T). Testimony Before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives 11/19/2002. Washington DC: U.S. General Accounting Office.
- Dacey, R. F. (2001). *Protecting America's Critical Infrastructures: How Secure are Government Computer Systems?* Testimony Before the Subcommittee on Oversight and Investigations Hearing, House Committee on Energy and Commerce 04/05/2001. Washington DC: U.S. House of Representatives.
- Dalrymple, P. W. (1998). Networks Part 1: Protecting Against Attacks on Open Systems. *Instrumentation and Control Systems*. 71, 51-55.
- Dalton, P. A. (2002). *National Preparedness: Integration of Federal, State, Local, and Private Sector Efforts is Critical to an Effective National Strategy for Homeland Security* (GAO-02-621T). Testimony Before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives 04/02/2002. Washington DC: U.S. General Accounting Office.

- Davies, T. R. (2001). *States Slow to Prepare to IT Infrastructure for Future Attacks*. Retrieved 02/05/03 from <http://www.washingtontechnology.com/cgi-bin/udt/im.display.printable>
- Day, P.A., Blue, E.T. & Peake-Raymond, M. (1998). Conducting research with An Urban American Indian Community: A Collaborative Approach. *Journal of American Indian Education*. 37(2), 21-33.
- Dearth, D. H. (2000). Critical Infrastructures and the Human Target in Information Operations. In A. D. Campen and D. H. Dearth (Eds.) *Cyberwar 3.0 Human Factors in Information Operations and Future Conflict* (203-209). Fairfax VA, AFCEA International Press.
- Deibert, R. J. (2003). *What Happened to Cyberwar?* Retrieved 05/20/03 from http://www.ssrc.org/programs/itic/publications/ITST_materials/deibertbrief3.pdf
- Deloitte Research. (2000). *At the Dawn of E-government: The Citizen as Customer*. New York: Author.
- Denby, D. (2000, November 27). The Speed of Light. *The New Yorker*, 132-141.
- Denhardt, R. B. (1995). *Public Administration: An Action Orientation* (2nd ed.). Belmont: Wadsworth Publishing Company.
- Denhardt, R. B. (1998). Five Great Issues in Organization Theory. In J Rabin, W. B. Hildreth, & G. J. Miller (Eds.) *Handbook of Public Administration* (2nd ed.) (117-144). New York: Marcel Dekker, Inc.
- Denning, D., & Baugh, W.E. (2000). Hiding Crimes in Cyberspace. In D. Thomas & B. D. Loader (Eds.), *Cybercrime: Law Enforcement, Security, and Surveillance in the Information Age* (105-131). New York: Routledge.
- Denzin, N. K. (1989). *The Research Act: A Theoretical Introduction to Sociological Methods*. Englewood Cliffs, New Jersey: Prentice Hall.
- Denzin, N. K. (1970). *Sociological Methods: A Sourcebook*. Chicago: Aldine Publishing Company.
- Department of Homeland Security. (2003). Information Analysis & Infrastructure Protection. Retrieved 05/15/03 from http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0094.xml
- Department of Justice. (1998). *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, Retrieved 11/20/2000 from http://www.usdoj.gov/criminal/cybercrime/white_pr.htm
- Dick, R. (2001). *Protecting America's Critical Infrastructures: How Secure are Government Computer Systems?* Testimony Before the Subcommittee on Oversight and Investigations Hearing, House Committee on Energy and Commerce 04/05/2001. Washington DC: U.S. House of Representatives.
- Digital Divide Network. (2003). *Digital Divide Basics Fact Sheet*. Retrieved 05/29/03 from <http://www.digitaldividenetwork.org/content/stories/index.cfm?key=168>
- Dilulio, J. J. Jr. & Kettl, D. F. (1999). Fine Print: The Contract with America, Devolution, and the Administrative Realities of American Federalism. In F. S. Lane (Ed.) *Current Issues in Public Administration* (6th ed.) (93-102). Boston: Bedford/St. Martin's.
- Dillman, D. A. (2000). *Mail and Internet Surveys: The Tailored Design Method*, (2nd Ed). New York: John Wiley & Sons, Inc.

- Doddrell, G. R. (1996). Information Security and the Internet. *Internet Research: Electronic Networking Applications and Policy*, 6 (1), (5-9).
- Dornan, A. (2002). *Hackers and Terrorists, or Presidents and CEOs?*. Retrieved 09/03/03 from <http://www.networkmagazine.com/article/NMG20020930S0016>
- Downs, A. & Murray, S. (1996). National Civic Review Roundtable: The Future of Regional Governance. *National Civic Review*, 85(2), 8-15.
- Drogin, B. (2000, January 8). Clinton Offers Plan to Fight Digital Terror. *Los Angeles Times*. A1.
- Drucker, P. F. (1973). *Management: Tasks, Responsibilities, and Practices*. New York: Harper & Row, Publishers.
- Dunn, D. (1999). *Virtual government puts locals online*. Retrieved 05/07/03 from http://www.americacityandcounty.com/ar/government_government_technologyvirtual_government
- Ellison, (1998). Intergovernmental Relations and the Advocacy Coalition Framework: the operation of federalism in Denver water politics. *Publius*, 28 (4), 35-5).
- Elazar, D. (1987). *Exploring Federalism*. Tuscaloosa, AL: The University of Alabama Press.
- European Committee on Crime Problems. (2000). *Draft Convention on Cyber-Crime*. Retrieved 11/11/00 from <http://www.cybercrime.gov/coedraft.htm>
- Everett, C. B., Dewindt, M. & McDade, S. (1997). The Silicon Spear: An Assessment Of Information Based Warfare (IBW) And U.S. National Security. In R. E. Neilson (Ed.) *Sun Tzu Art of War in Information Warfare*. Washington, D.C: National Defense University.
- Falcone, S. & Lan, Z. (1997). Intergovernmental Relations and Productivity. *Public Administration Review*, 57(4), 319-322.
- FedStats.gov. (2002). *Florida*. Retrieved 11/8/02 from <http://www.fedstats.gov/qf/states/12000.html>
- Fisher, D. (2003a). *South Korean Group Sues Microsoft Over Slammer*. Retrieved 05/06/03 from <http://www.eweek.com/article2/0,3959,1054790,00.asp>
- Fisher, D. (2003b). *Clarke Takes Gov't to Task Over Security*. Retrieved 07/16/03 from http://www.eweek.com/print_article/0,3668,a=44781,00.asp
- Florida Association of Counties. (2001). *Governmental Relations: Guiding Principles*. Tallahassee, FL: Author.
- Forman, M. A. (2003). *Statement of Mark A. Forman Associate Director for Information Technology and Electronic Government Office of Management and Budget Before the Committee on Government Reform Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations*. U.S. House of Representatives. April 8, 2003.
- Forman, M. A. (2001). *Statement of Mark A. Forman Associate Director for Information Technology and Electronic Government Office of Management and Budget Before the Committee on Government Reform Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations*. U.S. House of Representatives. November 9, 2001.

- Forum of Incident Response and Security Teams. (2002). *A Description*. Retrieved 05-14-03 from <http://www.first.org/about/first-description.html>
- Frank, D. (2002). *Sharing called Key to Cyber Plan*. Retrieved 12-02-02 from <http://www.fcw.com/fcw/articles/2002/0923/web-cato-09-25-02.asp>
- Frank, D. (2001). *Constructing E-government Leaders*. Retrieved 09-25-02 from <http://www.fcw.com/fcw/articles/2001/0813/cov-s1-08-13-01.asp>
- Frankfort-Nachmias, C. & Nachmias, D. (1992). *Research Methods in the Social Sciences*, (4th ed.) New York: St. Martin's Press.
- Fraser, B. (1997). *Site Security Handbook*. Request for Comments 2196. Internet Engineering Task Force. Network Working Group.
- Frederickson, G. H. (1997). *The Spirit of Public Administration*. San Francisco, CA: Jossey-Bass.
- Freund, G. (2003). *Beware of the New Breed of Hacker*. Retrieved 05/15/03 from http://zdnet.com.com/2100-1107_2-1001204.html
- FTAA Joint Government-Private Sector Committee of Experts on Electronic Commerce (2002). *The U.S. Approach to Electronic Government: A Path to Improved Service Delivery and Increased Citizen Participation and Interaction*. Retrieved 07/23/03 from <http://www.ftaa.ecom/inf/139>
- Gargan, J. J. (2000). State Governing Challenges for the New Century. In J. J. Gargan (Ed.) *Handbook of State Government Administration* (641-654). New York: Marcel Dekker, Inc.
- Garson, G. D. (2003). *Tests for Two Independent Samples: Mann-Whitney U, Wald-Wolfowitz Runs, Kolmogorov-Smirnov Z, & Moses Extreme Reactions Tests*. Retrieved 01/12/04 from http://davidmlane.com/hyperstat/dist_free.html
- Gartner Group. (2002). *Mission of the CIO*. Retrieved 11/11/02 from http://www.cio.com/research/executive/edit/gartner_description.html
- Gartner Consulting. (2002). *Member Technology Services: A report prepared on behalf of the Florida Leagues of Cities June, 30, 2000*. Maitland, FL: Author.
- General Social Survey. (1998). *Codebook Indexes*. Retrieved 02/02/03 from <http://www.icpsr.umich.edu:8080/GSS/homepage.htm>
- Gilmore Commission. (2001). *Cyber Terrorism: A View from the Gilmore Commission*. Hearing before the Committee on Science House of Representatives October 17, 2001: Author
- Global Reach. (2001). *Forrester Projects \$6.8 Trillion for 2004*. Retrieved 05/25/03 from <http://glreach.com/eng/ed/art/2004.e-commerce.php3>
- Goldberg, I. (2003). *Institute for the Advanced Study in Information Warfare*. Retrieved 05/14/03 from <http://www.psycom.net/iwar.1.html>
- Goodman, M. D. (1997). Why the Police Don't Care about Computer Crime. *Harvard Journal of Law & Technology*, 10(3), 466 - 494.
- Gonzales, J. (2001). *Statement of the Honorable Javier Gonzales, Commissioner, Santa Fe County, New Mexico, and President, National Association of Counties, on The Local Role in Homeland*

- Security. Before the United States Senate Committee on Governmental Affairs. December 11, 2001.* Retrieved 06/27/03 from http://www.senate.gov/~gov_affairs/121101gonzales.htm
- Governing.com (2002a) *Information Technology: 40-County Average Grade C+*. Retrieved 11/10/02 from <http://www.governing.com/gpp/gp2it.htm>
- Governing.com (2002b) *Managing Technology Conference Report*. Retrieved 11/9/02 from <http://www.governing.com/mtech2cr.htm>
- Government Electronics and Information Technology Association. (2001). *Information Assurance and Critical Infrastructure Protection: A Federal Perspective*. Washington DC: Author.
- Governments Without Boundaries. (2002). *A Management Approach to Intergovernmental Programs*. Retrieved 02/03/03 from <http://www.gwob.gov/report/executivesummary.html>
- Graham-Rowe, D. (2003). *Red Alert on the e-war Front*. Retrieved 07/16/03 from <http://www.newscientist.com/hottopics/tech/article.jsp?id=24024800>
- Group Decision Support Systems (GDSS). (2002). *Best Practices for Managing Cross-Agency e-government Initiatives*. Retrieved 10-20-02 from <http://www.gdss.com/wp/CAP.html>
- Guel, M. D. (2001). A Short Primer For Developing Security Policies. Retrieved 05/03/03 from http://www.sans.org/resources/policies/Policy_Primer.pdf
- Guess, G. M. (1998). Comparative and International Administration. In J Rabin, W. B. Hildreth, & G. J. Miller (Eds.) *Handbook of Public Administration* (2nd ed.) (535-569). New York: Marcel Dekker, Inc.
- Gulick, L. & Urwick, L. (1937). *Papers on the Science of Administration*. New York: Institute of Public Administration.
- Hair, J.F., Jr., Anderson, R.E., Tatham, R.L., & Black, W. C. (1998). *Multivariate Data Analysis, (5th Ed.)* Upper Saddle River, NJ: Prentice Hall.
- Hansell, S. (2003). *Hackers Hijack Computers Remotely in New Surge of Spam*. Retrieved 05/21/03 from <http://www.thestate.com/mld/thestate/business/technology/5902697.htm>
- Hecker, J. (2002). *Intergovernmental Coordination and Partnership will be Critical to Success*. Testimony before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives 07/03/2002. Washington DC: U.S. General Accounting Office.
- Held, D.A & McGrew, D.G. & Perraton, J. (1999). *Global Transformations: Politics, Economics, and Culture*. Stanford: California. Stanford University Press.
- Hennessy, J.L., Patterson, D.A., & Lin, H. S. (2003). *Information Technology for Counterterrorism: Immediate Actions and Future Possibilities*. Unknown: Computer Science and Telecommunications Board.
- Hernando County Florida. (no date). *Human Resources*. Retrieved 09/17/03 from <http://www.co.hernando.fl.us/hr/>
- Hobbs, S. (2000). *Cyber Threats: Viruses, Worms, Trojans, and DoS Attacks*. Retrieved 05/10/03 from <http://www.sans.org/rr/malicious/threats.php>

- Hoene, C., Baldassare, M. & Brennan, B. (2002). *Homeland Security and America's Cities*. Washington DC: National League of Cities
- Hurewitz, B. J., & Lo, A. M. (1993). Computer - Related Crimes. *American Criminal Law Review*, 30, 495 - 521.
- Intergovernmental Advisory Board. (2003). *High Payoff in Electronic Government: Measuring the Return on E-government Investments*. Washington, DC: Intergovernmental Advisory Board and the Federation of Government Information Processing Councils.
- Intergovernmental Advisory Board. (1998). *Foundations for Successful Intergovernmental Management: Federal, State and Local Government Experiences*. Federation of Government Information Processing Councils in cooperation with the Office of Intergovernmental Solutions Office of Governmentwide Policy U.S. General Services Administration.
- International City/County Management Association. (2002). *Forms of Local Government*. Retrieved 11/09/02 from <http://icma.org/documents/index.cfm>
- Imperial, M. T. (1988). *Intergovernmental Policy Implementation: Examining Interorganizational Networks and Measuring Network Performance*. Retrieved 02/09/03, from http://people.uncw.edu/imperialm/Instructor/papers/Imperial_AOM_98.pdf
- Information Assurance Advisory Council. (2001). *Threat Assessment and Early Warning Work Group: Policy Paper Summary*. Retrieved 05/14/03 from <http://www.iaac.org.uk/Wgs/Threats%0Policy%20Paper%20Summary.pdf>
- Institute for Information Infrastructure Protection. (2003). *Cyber Security Research and Development Agenda*. Washington, DC: author.
- Iowa State Association of Counties. (2003). *County Officials 2003*. Retrieved 08/19/03 from <http://www.sos.state.ia.us/publications/countydirectory/>
- Isenberg, D. (2002). *Securing U.S. Water Supplies*. Center for Defense Information Terrorism Project. Retrieved 07/17/03 from <http://www.cdi.org/terrorism/water-pr.cfm>
- IT-ISAC. (2003). *IT-ISAC Says "Slammer" Worm Affects Over 200,000 Machines in North America*. Retrieved 05/15/03 from https://www.it-isac.org/documents/pressreleases/01_27_2003_slammer.pdf
- Iversen, G. R. & Norpoth, H. (1987). *Analysis of Variance* 2nd Ed. London: Sage Publications.
- Juhnke, D. H. (2002). *Cyber Terrorism or Cyber Crime?* In Computer Forensics Inc. Retrieved 09/09/03 from <http://www.forensics.com/pdf/Cyber.pdf>
- Jordan, J. (1997). *Extranet Security: A Technical Overview from a Business Perspective*. Presented at the 20th NISSC Proceedings, October 1997, Baltimore, Maryland.
- Katz, A. J., & Carter, D. L. (1998). An Assessment of Computer Crime Victimization in the United States. In L. J. Moriarty. and D. L. Carter (Ed.), *Criminal Justice Technology in the 21st Century* (219-244). Springfield, Illinois: Charles C. Thomas Publisher, Ltd.
- Kayyem, J. N. & Howitt, A. M. (2002). *Beyond the Beltway: Focusing on Hometown Security*. A Report of the Executive Session on Domestic Preparedness John F. Kennedy School of Government: Harvard University.

- Kickert, W. J. M., Klijn, E.-H., & Koppenjan, J. F. M. (1997). Introduction: A Management Perspective on Policy Networks. In W. J. M. Kickert, E. H. Klijn, and J. F. M. Koppenjan (Eds.), *Managing Complex Networks* (1-13). London: Sage Publications.
- Kickert, W. J. M. and Koppenjan, J. F. M. (1997). Public Management and Network Management: An Overview. In W. J. M. Kickert, E. H. Klijn, and J. F. M. Koppenjan (Eds.), *Managing Complex Networks* (35-61). London: Sage Publications.
- Kouns, G. (2003). Automating infrastructure maintenance. *American City & County*. January, 1.
- Koerner, B. I. (2003). *Bush's Cyberstrategy: The administration's war against a bogus threat*. Retrieved 05/07/03 from <http://slate.msn.com/id/2079549/>
- Korzyk, A. D. Sr. & Wynne, A. J. (1997). *Who Should Really Manage Information Security In the Federal Government?* Retrieved 01/22/03 from <http://secutrity.is.edu/pdf/whomanage.pdf>
- Krebs, B. (2003). *Cyber War Game Tests Future Troops*. Retrieved 05/19/03 from <http://www.washingtonpost.com/wp-dyn/articles/A21871-2003Apr23.html>
- Krebs, B. (2002). *U.S. Government Flunks Computer Security Tests*. Retrieved 07/20/03 from <http://www.securityfocusonline.com/news/1693>
- Kremmen, J. (2002). *Cyber attack threat is real and constant*. Retrieved 07/10/02, from http://www.msnbc.com/news/kns_1169305.asp
- Kumar, N., L. W. Stern, and J. C. Anderson (1993), Conducting Interorganizational Research Using Key Informants. *Academy of Management Journal*, 36 (December), 1633-51.
- Lane, F. S. (1999). *Current Issues in Public Administration* (6th ed.). Boston: Bedford/St. Martin's.
- Leach, R. H. (1998). Federalism and Intergovernmental Relations. In J Rabin, W. B. Hildreth, & G. J. Miller (Eds.) *Handbook of Public Administration* (2nd ed.) (449-465). New York: Marcel Dekker, Inc.
- Leazer, M. (2003). *Internet worm shuts down county clerk's computers*. Retrieved 09-09-03 from http://www.kentuckynewera.com/cgi-bin/view.cgi?/200308/20+Internet-worm-08-20-03_news.html+20030820+news
- Lee, M. (2001). *The Missing Link: State Profiles of the Chief Information Officer*. Learning Paper Series. A Report of the Government Performance Project, Syracuse University.
- Leedy, P. D. & Ormrod, J. E. (2001). *Practical Research: Planning and Design* (7th ed.). Upper Saddle River, New Jersey: Merrill Prentice Hall.
- Lehmkuhl, L. D. (1996). Nonparametric Statistics: Methods for Analyzing Data Not Meeting Assumptions Required for the Application of Parametric Tests. *Journal of Prosthetics and Orthotics*, 8(3), 105-113.
- Lemos, R. (2003). *Security group: ICQ is flawed*. Retrieved 05/15/03 from http://zdnet.com.com/2100-1105_2-999870.html
- Libicki, M. C. (1995). *What is Information Warfare?*. Washington, DC: National Defense University.
- Liebetrau, A. M. (1983). *Measures of Association*. London: Sage Publications.

- Lipson, H. F. (2002). *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*. Pittsburgh, PA: CERT Coordination Center Special Report.
- Litt, R. S. (1997). *Internet Crimes Affecting Consumers*: Statement of Robert S. Litt, Deputy Assistant Attorney General, Criminal Division, United States Department of Justice, Before the Subcommittee on Technology, Terrorism and Government Information, Senate Judiciary Committee, United States Senate, Washington, D.C., (March 19, 1997) Washington DC: U. S. Department of Justice.
- Long, D. (2000). Protecting Critical Infrastructures: The Global Private-Sector Perspective. In A. D. Campen and D. H. Dearth (Eds.) *Cyberwar 3.0 Human Factors in Information Operations and Future Conflict* (223-232). Fairfax VA, AFCEA International Press.
- Luke, J. S., & Caiden, G. A. (1999). Coping with Global Interdependence. In F.S. Lane (Ed.), *Current Issues in Public Administration* (376-385). Boston: Bedford/St. Martin.
- Macaluso, A. C. (1984). Background and History on the Study Committee on Policy Management Assistance. In D. S. Wright and H. L. White (Eds.) *Federalism and Intergovernmental Relations* (58-67). Washington D. C.: American Society for Public Administration.
- Mandell, M. (1979). Letters to the Editor: Intergovernmental Management. *Public Administration Times*, 2(December), 2 & 6.
- Mayr, D. (1995). See. *Think. The History of the Net*. Retrieved 05/25/03 from <http://members.magnet.at/dmayr/history.htm#22>
- McCarthy, L. 1998. *Intranet Security: Stories from the Trenches*. Mountain View, CA: Sun Microsystems/ A Prentice Hall Title.
- McDonald, S. (2001). *Protecting America's Critical Infrastructure: How Secure Are Government Computer Systems?* Testimony before the Subcommittee on Oversight and Investigations Hearing, House Subcommittee on Energy and Commerce. April 5, 2001.
- McDonough, F. A. (2002). *The Perfect Storm is Accelerating Electronic Government*. U.S. General Services Administration.
- McDonough, F. A. (2000). *Tomorrow's Reinvented Government: 10 Changes Ahead*. U.S. General Services Administration.
- McWilliams, B. (2001). *CERT: Cyber Attacks Set to Double in 2001*. Retrieved 10/20/01 from <http://securityfocus.com/news/266>
- Miller, L. & Gregory, P. (2002). *CISSP for Dummies*. New York: Wiley Publishing, Inc.
- Mills, A. (1995). *Inadequate Security Encourages the Thief*. *Industrial Management and Data Systems*, 95(2), 3-5.
- Mintzberg, H. & Lampel, J. (1999) Reflections on a Strategy Safari. *Sloan Management Review*, 40(3), 21-30.
- Misra, S. (2003). High-tech Terror. *American City & County*, June 1.
- Moore, B. J. (1997). Case for Requiring Information Technologies Strategic Plans. *IEEE*, 430-437.

- Monroe, J. (2002). *Saving by Sharing*. Retried 12/02/02 from <http://www.fcw.com/print.asp>
- Moteff, J. D. (2002). *Critical Infrastructure: Background, Policy, and Implementation*. Congressional Research Service Report to Congress.
- Nash, E. (2003). *Hackers Bigger Threat Than Rogue Staff*. Retrieved 05/17/03 from <http://www.vnunet.com/News/1140907>
- National Association of Counties (NACO). (2001a). *Counties and Homeland Security. Policy Agenda to Secure the People of America's Counties*. Retrieved 1/22/02 from <http://www.naco.org/programs/homesecurity/policyplan.cfm>
- National Association of Counties (NACO). (2001b). *Strengthening Homeland Security*. Retrieved 7/22/02 from <http://www.naco.org/programs/homesecurity/whfact.cfm>
- National Association of Counties (NACO). (2001c). *About Counties*. Retrieved 7/22/02 from <http://www.naco.org/counties/index.cfm>
- National Infrastructure Protection Center. (2002). *Swarming Attacks: Infrastructure Attacks for Destruction and Disruption*. Washington D.C.: author.
- National Institute of Standards and Technology. (2003). *Common Criteria for IT Security Evaluation Common Language to Express Common Needs*. Retrieved 05/07/03 from <http://csrc.nist.gov/cc/index.html>
- National League of Cities. (2002). *Cities See Biological, Cyber-Terrorism as Top Threats, One Year After 9-11*. Retrieved 09/12/03 from http://www.nlc.org/nlc_org/site/newsroom/nations_cities_weekly/display.cfm?id=214B536A-DE8D-4607-B826F223354AC523
- National Research Council. (1999). *Summary of a Workshop on Information Technology Research for Crisis Management*. Sponsored by the Committee on Computing and Communications Research to Enable Better Use of Information Technology in Government, National Research Council.
- Naughton, K. (1999). CyberSlacking. *Newsweek*, U.S. Edition, (62).
- Nelson, L. (2001). *Building Blocks for Successful Intergovernmental Programs*. Retrieved 11/12/02, from http://www.gsa.gov/Portal/content/pubs_content.jsp
- NetScreen Technologies. (2003a). *Defense in Depth: A Strategy to Secure Federal Networks*. Retrieved 05/07/03 from <http://www.netscreen.com/resources/whitepapers/government/>
- NetScreen Technologies. (2003b). *Securing Tactical Wireless LANs: NetScreen Security Solutions for Wireless LANs*. A White Paper by NetScreen Technologies, Inc. Retrieved 05/07/03 from <http://www.netscreen.com/resources/whitepapers/government/>
- New Atlantis, The, (2003). *Is Cyberspace Secure? An Interview with Howard A. Schmidt*. Retrieved 05/05/03 from <http://www.thenewatlantis.com/archive/1/interview.htm>
- Nielsen NetRatings. (2003). *Global Internet Index*. Retrieved 05/29/03 from http://www.nielsen-netratings.com/news.jsp?section=dat_gi
- NIST Bulletin. (1995). *Preparing for Contingencies and Disasters*. Retrieved 09/17/01 from <http://csrc.nist.gov/publications/nistbul/csl95-09.txt>

- Noonan, T. (2001). Protecting America's Critical Infrastructures: How Secure are Government Computer Systems? Testimony Before the Subcommittee on Oversight and Investigations Hearing, House Committee on Energy and Commerce 04/05/2001. Washington DC: U.S. House of Representatives
- Norusis, M. J. (1998). *SPSS 8.0: Guide to Data Analysis*. Upper Saddle River, NJ: Prentice Hall.
- Nye, J. S., JR. (2002). Information Technology and Democratic Governance. In E. Ciulla Kamarck and J. S. Nye, Jr. (Eds.) *Governance.com: Democracy in the Information Age* (1-16). Harrisonburg: R. R. Donnelley and Sons.
- O'Connell, K. A. (2003). Computerizing Government. *American City & County*. July, 7.
- OECD. (2003). *OECD Member Countries*. Retrieved 06/01/03 from <http://www.oecd.org/EN/countrylist/0,,EN-countrylist-0-nodirectorate-no-no-159-0,00.html#country>
- OECD. (2002a). *OECD Information Technology Outlook 2002*. Retrieved 06/01/03 from <http://www.oecd.org/pdf/M00030000/M00030907.pdf>
- OECD. (2002b). *Measuring the Information Economy 2002*. Paris, France: Author.
- Oliver, C. (1990). Determinants of Interorganizational Relationships: Integration and Future Directions. *Academy of Management Review* 15(2), 241-265.
- OECD. (1997). *Managing Across Levels of Government*. Unknown: Author.
- Olsen, C. H. (2003). "Guest Commentary: Review of the Use of Statistics in Infection and Immunity. *Infection and Immunity*. 71(12), 6689-6692
- Osborne, S. (2001). FBI Briefs Homeland Task Force on Cyberterrorism. *County News Online*, 33 (23).
- O'Toole, L. Jr., Hanf, K. I., & Hupe, P. L. (1997). Managing Implementation Processes in Networks. In W. J. M. Kickert, E. H. Klijn, and J. F. M. Koppenjan (Eds.), *Managing Complex Networks* (137-151). London: Sage Publications.
- O'Toole, L. Jr. (1997). Treating Networks Seriously: Practical & Research-based Agendas in Public Administration. *Public Administration Review*, 57 (1), 45-52.
- Pagano, M. A. & Johnston, J. M. (2000). Life at the Bottom of the Federal Food Chain: Examining City and County Revenue Decisions. *Publius*, 30 (1) (159-70).
- PCCIP. (1997). *Critical Foundations: Protecting American's Infrastructure*. The Report of the President's Commission on Critical Infrastructure Protection. Unknown: Author.
- PDD63. (1998). *White Paper on Presidential Decision Directive 63*. Office for State and Local Domestic Preparedness Support.
- Pew Internet and the American Life Project (2003). The Ever-Shifting Internet Population: A new look at Internet Access and the Digital Divide. Washington DC: Author.
- Pew Internet and the American Life Project (2001). Fear of Online Crime: Americans support FBI interception of criminal suspects' email and new laws to protect online privacy. Washington DC: Author.

- Perlman, E. (2002a). *Policy, Politics, and Leadership*. Retrieved 11/10/02 from <http://www.governing.com/mtech2cr.htm>
- Perlman, E. (2002b). Network Security- Digital Nightmare: What if terrorists break into critical state and local networks and wreak havoc? *Governing Magazine*. April 2002.
- Perry, J. L. & Kraemer, K. L. (1999). The Implications of Changing Technology. In F. S. Lane(Ed.) *Current Issues in Public Administration* (6th ed.) (182-200). Boston: Bedford/St. Martin's.
- Phoha, V. V. (2002). *Internet Security Dictionary*. New York: Springer-Verlag New York Inc.
- Posner, P. L. (2002). *Effective Intergovernmental Coordination Is Key to Success (GAO-02-1012T)*. Testimony Before the Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform, House of Representatives. Washington D.C.: U.S. General Accounting Office.
- Powell, W, Koput, K. W., & Smith-Doerr, L. (1996). Interorganizational Collaboration and the Locus of Innovation: Networks of Learning in Biotechnology. *Administrative Science Quarterly*, 41, 116-145.
- Pratt, M. (2002). All Together Now. *American City & County*. November, 13.
- Public Technology, Inc. (2000). *Risk and Reward: Helping Local Government Leaders Understand Technology Risk and Liability Issues*. Washington DC: Author.
- Radcliff, D. (2002). "Security Under the Gun: The Security Skills Mirage". Retrieved 05/13/03 from <http://www.computerworld.com/securitytopics/security/story/0,10801,71579,00.html>
- Radin, B. (2000). Intergovernmental Relationships and the Federal Performance Movement. *Publius*, 30(1), 143-158.
- Rathmell, A. (2000). International Perspectives on Infrastructure Protection. In A. D. Campen and D. H. Dearth (Eds.) *Cyberwar 3.0 Human Factors in Information Operations and Future Conflict* (233-244). Fairfax VA, AFCEA International Press.
- Reames, J. E. (2000). Computer Crimes, Hacking, and Cybernetic warfare. *Journal of California Law Enforcement*, 34(1), 17-26.
- Rhodes, K. (2001). *Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures. (GAO-01-1073T)*. Testimony Before the Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform, House of Representatives. August 29, 2001. Washington DC: US General Accounting Office.
- Rivlin, A. M. (1999). The Evolution of American Federalism. In F. S. Lane(Ed.) *Current Issues in Public Administration* (6th ed.) (74-92). Boston: Bedford/St. Martin's.
- Roberts, P. (2003). *Fluffi Bunni worked for Siemens*. Retrieved 05/15/03 from <http://www.nwfusion.com/news/2003/0508fluffbunni.html>
- Roos, R. (1998). *Disarmament and Security Committee: International Policies on Information Warfare*. Retrieved 05/15/03 from <http://www.stanford.edu/group/smun/oldversion/oldversion/simun98/briefings/info-war.html>

- Rowe, K. (2002). The measurement of latent and composite variables from multiple items or indicators: Applications in performance indicator systems. Background paper prepared for keynote address presented for the Royal Melbourne Institute of Technology Statistics Seminar Series!. Retrieved 01/14/04 from <http://www.acer.edu.au/research/programs/documents/Measurement%20of%20Composite%20Variables.pdf>
- Ruthfield, S. (1995). *The Internet's History and Development From Wartime Tool to the Fish-Cam*. Retrieved 11/12/00 from <http://info.acm.org/crossroads/xrds2-1/inet-history.html>
- Sager, I., Hamm, S., Gross, N., Carey, J., & Hof, R. (2000). Cyber Crime. *Business Week*, February Issues. 37-44.
- Sarkar, D. (2003). Locals want More Help, Less Baloney. *Federal Computer Week*, January 28.
- Sarkar, D. (2002). Officials Nurture Relationship: Feds Give State, Local CIOs a Seat at the Table. *Federal Computer Week*, July 15.
- Schiavo-Campo, S., & Sundaram, P.S.A. (2001). To Serve and To Preserve: Improving Public Administration in a Competitive World. Asian Development Bank.
- Schumacher, H. J. & Ghosh, S. (2000). Network Security Framework. In J. Webster (ed.) *Wiley Encyclopedia of Electrical and Electronics Engineering Online*. Retrieved 04/22/01 from <http://www.interscience.wiley.com:83/eeee/38/5338/W.5338-2.html>
- Sewell, C. (2002). One Network Under Gov. *Telephony*, 242(1), 30-34.
- Shachtman, N. (2003). *Tech Firms Eye Juicy Contracts*. Retrieve 05/15/03 from <http://www.wired.com/news/politics/0,1283,58747,00.html>
- Shachtman, N. (2002). *Study Makes Less of Hack Threat*. Wired News. Retrieved 11/21/02 from <http://www.wired.com/news/politics/0.1283.56382.00.html>
- Shim, R. (2003). *130 arrested in Net fraud crackdown*. Retrieved 05/17/03 from http://news.com.com/2100-1018_3-1003833.html
- Singleton, R. & Straits, S. (1999). *Approaches to Social Research*, 3rd Edition. New York, NY: Oxford University Press.
- Smart Computing. (2001). *How the Internet Works*. Lincoln, NE: Sandhills Publishing Company.
- Smith, G. (1998). *How Vulnerable is Our Interlinked Infrastructure?*. Issues in Science and Technology. Fall 1998. Retrieved 11/19/2001 from <http://205.130.85.236/issues/15.1/smith.html>
- Solomon, A. (1995). *A Brief History of PC Viruses*. Retrieved 07/14/03 from http://www.claws-and-paws.com/virus/papers/solomon_history.shtml
- SPSS. (1999). *SPSS Base 10.0 Application Guide*. Chicago, IL: Author.
- Stambaugh, H., Beaupre, D., Icové, D. J., Baker, R., Cassaday, W., & Williams, W. (2000). *State and Local Law Enforcement Needs to Combat Electronic Crime* (183451). Washington D.C.: National Institute of Justice.

- Staten, C. L. (1999). *Results of ERRI/EmergencyNet News Local/County/State Computer "Hacking" Survey-May/June, 1999*. Emergency Response & Research Institute. Chicago, IL. Retrieved 09/09/03 from <http://www.emergency.com/1999/hackrslt.htm>
- Stanton, J. J. (2000). Is the Country Ready for Cyberwarfare. *Security Management*, 44(8), 148-151.
- Stark, R. & Roberts, L. (1998). *Contemporary Social Research Methods* (2nd Ed.). Bellevue, WARFARE: Micro Case Corporation
- State of Florida. (2001). *Constitution of the State of Florida*. Retrieved 11/10/02 from <http://www.leg.state.fl.us/Statutes/index.cfm?Mode=Constitution&Submenu=3&Tab=statutes#A08>
- Stenberg, C. W. (1984). Beyond the Days of Wine and Roses: Intergovernmental Management in a Cutback Environment. In D. S. Wright and H. L. White (Eds.) *Federalism and Intergovernmental Relations* (68-89). Washington D. C.: American Society for Public Administration.
- Stever, J. (1993). The Growth and Decline of Executive-Centered Intergovernmental Management. *Publius: The Journal of Federalism*, 23, 71-84.
- Sundquist, J. L. (1969). *Making Federalism Work: A Study of Program Coordination at the Community Level*. Washington, DC: Brookings Institute.
- Sunshine, C. A. (1999). *Internetworking*. Wiley Encyclopedia of Electrical and Electronics Engineering [Online Version] . John Wiley & Sons, Inc.
- Symantec. (2003). *Internet Security Threat Report: Volume 3, February 2003*. Cupertino, CA: Symantec Corp.
- Symantec (2000). *The Government and Internet Security*. Retrieved 03/18/01 from <http://enterprisesecurity.symantec.com/article.cfm?articleid=270>
- Toffler, A. & Toffler, H. (1993). *War and Anti-War: Survival at the Dawn of the Twenty-First Century*. New York: Warner Books.
- Transition Office of the President's Commission on Critical Infrastructure Protection & the Critical Infrastructure Assurance Office. (1998). *Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures*. Washington, DC: Authors.
- Triagaux, R. (1998). *The Underbelly of Cyberspace*. St. Petersburg Times. Retrieved 10/10/01 from http://www.sptimes.com//Hackers/underbelly_of_cyberspace.html
- Tritak, J. (2001a). *Protecting America's Critical Infrastructures: How Secure are Government Computer Systems?* Testimony Before the Subcommittee on Oversight and Investigations Hearing, House Committee on Energy and Commerce 04/05/2001. Washington DC: U.S. House of Representatives.
- Tritak, J. S. (2001b). *Critical Infrastructure Protection: Who's in Charge*. Statement before the Senate Committee on Governmental Affairs. October 4, 2001. Critical Infrastructure Assurance Office.
- Turner, R. S. (1990). Intergovernmental Growth Management: A Partnership Framework for State-Local Relations. *Publius: The Journal of Federalism*, 20, 79-95.

- Tyrrell, P. J. (2000). Protecting the National Critical Infrastructure: The Human Dimension from a Government Perspective. In A. D. Campen and D. H. Dearth (Eds.) *Cyberwar 3.0 Human Factors in Information Operations and Future Conflict* (49-75). Fairfax VA, AFCEA International Press.
- University of Central Florida Institutional Review Board. (2003). *Principle Investigators Manual*. Orlando, FL: Author.
- U.S. Advisory Commission on Intergovernmental Relations. (1993). The Techniques of Intergovernmental Relations. In L. J. O'Toole, Jr. (Ed.) *American Intergovernmental Relations: Foundations, Perspectives and Issues*. (2nd ed.) (290-296). Washington, D.C.: CQ Press.
- U.S. Advisory Commission on Intergovernmental Relations. (1996). *Preliminary ACIR Report on Federal Mandates*. Retrieved 02/05/03, from <http://www.library.unt.edu/gpo/acir/mandates.html>
- U.S. Army (2004). *Florida Zones*. Retrieved 12/15/03 from <http://www.flmars.org/zones.htm>
- U.S. Census Bureau. (2003). *State & County QuickFacts*. Retrieved 09/19/03 from <http://quickfacts.census.gov/qfd/>
- U.S. Census Bureau. (2002a). *Government Units in 2002*. Retrieved 11/08/02 from http://www.census.gov/govs/cog/2002COGprelim_report.pdf
- U.S. Census Bureau. (2000a). *County and City Data Book: 2000*. Retrieved 11/08/02 from <http://www.census.gov/prod/www/ccdb.html>
- U.S. Census Bureau. (1998). *Pre-testing Policy and Options: Demographic Surveys at the Census Bureau*. Washington D.C.: U.S. Department of Commerce.
- U.S. Department of Commerce. (2003). *E-stats*. Washington, DC: Economic and Statistic Administration, U.S. Census Bureau.
- U.S. Department of Commerce. (1999). Computer Attack: What They are and How to Defend Against Them. *ITL Bulletin*. May Issue. Gaithersburg, MD: National Institute of Standards and Technology.
- U.S. Department of Commerce. (1998). Information Security and the World Wide Web. *ITL Bulletin*. February Issue. Gaithersburg, MD: National Institute of Standards and Technology.
- U.S. Department of Justice (1999). *Kevin Mitnick Sentenced to Nearly Four Years in Prison: Computer Hacker Ordered to Pay Restitution to Victim Companies Whose Systems were Compromised*. Retrieved 04/08/03 from <http://www.usdoj.gov/criminal/cybercrime/mitnick.htm>
- U.S. General Accounting Office. (2003). *Information Security: Progress Made, but Weaknesses at the Internal Revenue Service Continue to Pose Risks*. Report to the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform, House of Representatives May 2003. Washington DC: Author.
- U.S. General Accounting Office. (2001a). *Information Sharing: Practices That Can Benefit Critical Infrastructure Protection (GAO-02-24)*. Washington, D.C.: Author.
- U.S. General Accounting Office. (2001b). *Maximizing the Success of Chief Information Officers: Learning from Leading Organizations (GAO-01-376G)*. Washington, D.C.: Author.

- U.S. General Accounting Office. (2001c). *Combating Terrorism: Selected Challenges and Related Recommendations (GAO-01-822)*. Washington, D.C.: Author.
- U.S. General Accounting Office. (1996a). *Information Technology: Best Practices Can Improve Performance and Produce Results*. Washington, DC: Author.
- U.S. General Accounting Office. (1996b). *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (AIMD-96-84)*. Washington, D.C.: Author.
- Vatis, M. A. (2001). *Cyber Attacks During the War on Terrorism A Predictive Analysis*. Hanover, NH: Institute for Security Technology Studies at Dartmouth College.
- Verton, D. (2003a). *Offshore Coding Work Raises Security Concerns*. Retrieved 05/15/03 from <http://www.computerworld.com/securitytopics/security/story/0,10801,80935,00.html>
- Verton, D. (2003b). Reducing Software Flaws Key to Security, Users Say. *Computer World*. Retrieved 07/20/03 from <http://www.computerworld.com/securitytopics/security/story/0,10801,78721,00.html>
- Verton, D. (2002). Critical Infrastructure Systems Face Threat of Cyberattacks [Electronic Version]. *Computerworld*,36(2).
- Verton, D. (2001). *U.S. Infrastructure Shaken By Terrorist Attack*. *Computer World*. Retrieved 09/11/01 from http://www.computerworld.com/cwi/story/0,1199,NAV47_STO63719,00.html
- Vijayan, J. (2003). *Security Problems Persist with Instant Messaging*. Retrieved 05/15/03 from <http://www.computerworld.com/softwaretopics/software/groupware/story/0,10801,81104,00.html>
- Volusia County Government Online. (2003). *Personnel Services*. Retrieved 09/17/03 from <http://volusia.org/personnel/default.htm>
- Wakeley, J. H. (1983). Managing People and Systems: The Management Skills. In W. B. Eddy (Ed.) *Handbook of Organizational Management (171-191)*. New York: Marcel Dekker, Inc.
- Walker, D. (2002). *Homeland Security: Critical Design and Implementation Issues (GAO-02-957T)*. Statement before the Select Committee on Homeland Security, House of Representatives 07/17/02. Washington, D.C: U.S. General Accounting Office.
- WBAL-TV. (2003). *Worm Forces MVA Offices To Shut Down: Thousands Of Computers Affected By Infection*. Retrieved 09/09/03 from <http://www.thewbalchannel.com/news/2399847/detail.html>
- West, J. P. & Berman, E. M. (2001). The Impact of Revitalized Management Practices on the Adoption of Information Technology: A National Survey of Local Governments. *Public Performance & Management Review*, 24 (3), 233-253.
- White House, The. (2003). *National Strategy to Secure Cyberspace*. Washington DC: Author.
- White House, The. (2002). Executive Order on Critical Infrastructure Protection. Retrieved 05/23/03 from <http://www.whitehouse.gov/news/releases/2001/10/20011016-12.html>
- Willemssen, J. C. (2001). *Critical Infrastructure Protection: Significant Challenges in Protecting Federal Systems and Developing Analysis and Warning Capabilities, (GAO-01-1132T)*. Statement before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government reform, House of Representatives. Washington, D.C.: U.S. General Accounting Office

- Worthen, B. (2002). Doom for the NIPC?. *CIO Magazine: Washington Watch*, June Issue.
- Wright, D. & Cho, C. L. (2000). State Administration and Intergovernmental Interdependency: Do National Impacts on State Agencies Contribute to Organizational Turbulence? In J. J. Gargan (Ed.) *Handbook of State Government Administration* (33-66). New York: Marcel Dekker, Inc.
- Wright, D. (1998). Federalism, Intergovernmental Relations, and Intergovernmental Management: The Origins, Emergence, and Maturity of Three Concepts Across Two Centuries of Organizing Power by Area and by Function. In J Rabin, W. B. Hildreth, & G. J. Miller (Eds.) *Handbook of Public Administration* (2nd ed.) (381-448). New York: Marcel Dekker, Inc.
- Wright, D. (1993). Models of National, State, and Local Relationships. In L. J. O'Toole, Jr. (Ed.) *American Intergovernmental Relations: Foundations, Perspectives ad Issues*. (2nd ed.) (75-88). Washington, D.C.: CQ Press.
- Wright, D. (1992). Understanding Intergovernmental Relations. In J. M. Shafritz & A. C. Hyde (Eds.) *Classics of Public Administration* (3rd ed.) (550-563). Belmont: Wadsworth.
- Wright, D. (1983). Managing the Intergovernmental Scene: The Changing Dramas of Federalism, Intergovernmental Relations, and Intergovernmental Management. In W. B. Eddy (Ed.) *Handbook of Organizational Management* (417-454). New York: Marcel Dekker, Inc.
- Wright, D. (1982, 1988). *Understanding Intergovernmental Relations*. Pacific Grove, CA; Brooks/Cole Publishing Co.
- Wuensch, K. L. (2001). *Choosing an Appropriate Bivariate Inferential Statistic*. Retrieved 01/12/04 from <http://core.ecu.edu/psyc/wuenschk/docs30/appstat.doc>
- Wulf, W. A. (2001). *Cyber Security: Beyond the Maginot Line*. Testimony before the House Science Committee U.S. House of Representatives. October 10, 2001.
- Yim, R. A. . (2002a). *National Preparedness: Integration of Federal, State, Local, and Private Sector Efforts is Critical to an Effective National Strategy for Homeland Security (GAO-02-621T)*. Testimony before the Subcommittee on Economic Development, Public Buildings, and Emergency Management, Committee on Transportation and Infrastructure 04/11/02. Washington, D.C: U.S. General Accounting Office.
- Yim, R. A. . (2002b). *National Preparedness: Integrating New and Existing Technology and Information Sharing into an Effective Homeland Security Strategy (GAO-02-811T)*. Testimony before the Subcommittee on Technology and Procurement Policy, Committee on Government Reform, House of Representatives. 06/07/02. Washington, D.C: U.S. General Accounting Office.
- Zakon, R. H. (2003). *Hobbes' Internet Timeline v6.0*. Retrieved 05/25/03 from <http://www.zakon.org/robert/internet/timeline/#2000s>