



**GEOSPATIAL INFORMATIONAL SECURITY RISKS AND CONCERNS OF
THE UNITED STATES AIR FORCE GEOBASE PROGRAM**

THESIS

Scott A. Bryant, Major, USAF

AFIT/GEM/ENV/07-M1

**DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY**

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

**GEOSPATIAL INFORMATIONAL SECURITY RISKS AND CONCERNS OF
THE UNITED STATES AIR FORCE GEOBASE PROGRAM**

THESIS

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the
Degree of Master of Science in Information Resource Management

Scott A. Bryant, BS

Major, USAF

March 2007

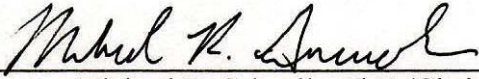
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

AFIT/GEM/ENV/07-M1

GEOSPATIAL INFORMATIONAL SECURITY RISKS AND CONCERNS OF THE
UNITED STATES AIR FORCE GEOBASE PROGRAM

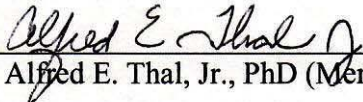
Scott A. Bryant, BS
Major, USAF

Approved:



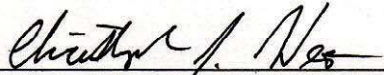
Michael R. Grimala, PhD (Chairman)

14 MAR 07
date



Alfred E. Thal, Jr., PhD (Member)

14 MAR 07
date



Christopher West, PhD (Member)

15 Mar 07
date

Abstract

Technological advancements such as Geospatial Information Systems (GIS) and the Internet have made it easier and affordable to share information, which enables complex and time sensitive decisions to be made with higher confidence. Further, advancements in information technology have dramatically increased the ability to store, manage, integrate, and correlate larger amounts of data to improve operational efficiency. However, the same technologies that enable increased productivity also provide increased capabilities to those wishing to do harm.

Today's military leaders are faced with the challenge of deciding how to make geospatial information collected on military installations and organizations available to authorized communities of interest while simultaneously restricting access to protect operational security. Often, these decisions are made without understanding how the sharing of certain combinations of data may pose a significant risk to protecting critical information, infrastructure or resources. Information security has been an area of growing concern in the GeoBase community since, by definition, it is required to strike a balance between competing interests, each supported by federal policy: (1) the availability of data paid for by tax dollars and (2) the protection of data as required to mitigate risks.

In this research, the security implications of the US Air Force GeoBase (the US Air Force's applied Geospatial Information System) program will be explored. The rapid expansion of the use of GeoBase to communities outside of the civil engineering field necessitates an examination of the intrinsic and extrinsic security risks of the

unconstrained sharing of geospatial information. This research will explore difficulties encountered when attempting to rate the sensitivity of information, discuss new policies and procedures that have been implemented undertaken to protect the information, and propose technical and managerial control measures to facilitate sharing geospatial information sharing while minimizing the associated operational risks.

To my Wife & Family

Acknowledgements

I would like to express my sincere appreciation to my advisor, Dr Michael Grimaila, and thesis committee members, Dr Alfred Thal, Jr., and Major Christopher West. Their guidance, insight and support throughout the course of this thesis effort were invaluable. I would also like to thank my previous commanders and fellow civil engineers for the wonderful examples they set and their help instilling in me the importance of graduate work.

I am also indebted to the GeoBase community, and the leaders, teachers, and inspirers, such as: Chief MSgt Dwight Badgett, Mr. Mark Cave, Lt Col Jeth Fogg, Ms. Jane Goldberg, Ms. Susan Kil, Lt Col Andrew Lambert, Mr. Steven Luttrell, Lt Col (Ret) John McDermon, Mr. Ben McMillan, Maj John Thomas, Mr. Greg Turner, and Mr. Rich Updike. It was through their valuable insight, experience, and willingness to share their experiences that laid the cornerstones of this research. It is the people like these, those they work with, and those that are to follow in their footsteps that enable and strengthen the Air Force mission through their valuable skills and leadership they bring to the GeoBase program and the Air Force.

Finally, it is also with my deepest gratitude and honor to be sharing this milestone with my wife whose faith, hope, and love, will remain with me forever and always.

Scott A. Bryant

Table of Contents

	Page
Abstract	iv
Acknowledgements	vi
List of Figures	vii
List of Tables	ix
 I. Introduction	 1
Overview	1
Motivations for Research	2
Targeted Research Area	3
Research Goals	4
Overall Approach to Research	4
Primary Research Questions	3
Focused Objectives	3
Benefits / Implications of Research	4
Thesis Overview	5
 II. Background	 7
Introduction	7
What is Information Security?	7
What is Geospatial Information?	8
GeoBase History	8
Emerging Geospatial Technologies	11
A New Paradigm	11
New Paradigms, New Problems	12
New Problems, New Policies	17
Post 9/11	18
Geospatial Information and the Law	20
Identifying Security Risks	24
Top Challenges	27
Defining the Sensitivity of Information	28
Information Sharing	32
Inconsistencies in Policies and Guidance	34
 III. Methodology	 36
Purpose and Organization	36
Developing the Research Strategy	36
Case Study Research	38
Why an Exploratory Case Study?	39

	Page
Case Study Design	39
Step 1: Define and Design.....	40
Developing the Research Questions	41
Context and Case Selection	42
Defining the Units of Analysis	42
Data Collection Protocol.....	43
Using Multiple Sources of Evidence	43
Creating the Case Study Database	44
Maintaining a Chain of Evidence	50
Step 2: Prepare, Collect, and Analyze.....	50
Conducting Units of Analysis.....	51
Writing the Embedded Analysis Report	53
Step 3: Analyze and Conclude	53
Potential Pitfalls	55
Summary of Methodology	57
IV. Analysis	58
PG1 What is the nature of the security risk posed by GeoBase?	58
What are the geospatial assets in need of protection?.....	59
What are the top security concerns of GeoBase today?.....	59
What Security Controls are available?.....	61
What are the ways in which GeoBase offices are controlling information today?.....	63
PG2 What information is sensitive that poses a risk to security?	67
How is geospatial information classified?	68
Who defines the classification of geospatial information?	72
What types of information are considered sensitive?	73
How is security information tracked in GIS?	74
PG3 What impacts might information security concerns affect information sharing.	76
What are the reasons for not sharing?.....	76
How is GeoBase overcoming sharing barriers?.....	80
PG4 What are the key information system security constructs and their interrelationships?	82
PG5 What are the impacts of information security on information sharing within the GeoBase community?	91
Whom are we sharing geospatial information with?	91
What is the geospatial information used for?	92
How are we sharing geospatial information?.....	96
Who are the primary GeoBase customers using and sharing geospatial information?	97
How does sharing information impact risk?	100
What are the impacts of sharing geospatial information?.....	101
PG6 What are the costs and benefits of either limiting or providing access to the data? Do they outweigh the risks?	104
Financial Investments	104
Non-Monetary and Mission Benefits.....	107

	Page
V. Conclusions and Recommendations	111
Conclusions and Recommendations	111
Appendix A: Approach to Research Overview	116
Appendix B: Investigation Protocol.....	117
Background	119
Key Documents.....	119
Research Enablers	120
Field Procedures.....	120
Setting up the interview	120
Immediately prior to the interview:	121
At the start of the interview:	121
Following the interview:	122
A Guide for the Study Report	123
Appendix C: Thesis Research Overview (Sent to Interviewees).....	124
Appendix D: Interview Outline	130
Appendix E: Relative Laws & Executive Orders (1950 to Present).....	133
Appendix F: Relative Policies and Guidance	141
Bibliography	142

List of Figures

Figure	Page
Figure 1. Targeted Area of Research	4
Figure 2. Research Design	2
Figure 3. Top Geospatial Data Producers	14
Figure 4. Federal Agencies Producing Geospatial Data	15
Figure 5. Geospatial Information on the Rise	16
Figure 6. Identifying Risks	24
Figure 7. Decision Tree for Providing Appropriate Access to Geospatial Data in Response to Security Concerns.....	31
Figure 8. Relevant Situations for Different Research Strategies	37
Figure 9. Single-Case Study (embedded) Method (Phase 1).....	41
Figure 10. Case Study Design.....	42
Figure 11. Building the Case Study Database	45
Figure 12. Single-Case Study (embedded) Method (Phase 2).....	51
Figure 13. Single-Case Study (embedded) Method (Phase 3).....	54
Figure 14. Classification Distribution in GeoBase	69
Figure 15. Impact of Security Concerns on Information Sharing.....	78
Figure 16. Perceived Barriers Preventing Federal Agencies from Sharing Information	79
Figure 17. Multiple Mission Uses of Installation & Environment (I&E).....	93
Figure 18. Air Force Geospatial Centers of Gravity	98
Figure 19. Case Study of Ramstein AB ArcIMS.....	99
Figure 20. Impact of Familiarity with Geospatial Assets on Amount of Information Shared and Risk to Security	100
Figure 21. Information Sharing and Security Risk Relationship.....	101

Figure	Page
Figure 22. Information Demand-Provision Gap following an emergency event.....	103
Figure 23. Accelerating information availability to keep closer pace with demand	103
Figure 24. Government Security Classification Costs Estimate Fiscal Year 2005..	105
Figure 25. Graph Comparing Total Costs for Government and	106
Figure 26. Timescale of Costs and Benefits of GIS Investments	107
Figure 27. Information Restriction and Mission Accomplishment Relationship	109

List of Tables

Table	Page
Table 1. Six Sources of Evidence: Strengths and Weaknesses.....	44
Table 2. Common Control Categories	47
Table 3. Summary of Potential Pitfalls	56
Table 4. GeoBase’s Primary Security Concerns.....	60
Table 5. Primary Security Controls	61
Table 6. Security Control Classes and Families	62
Table 7. Tabular Metadata Security Information Template.....	75
Table 8. Reasons for not wanting to share information	77
Table 9. Top Ten Perceived Barriers to Sharing Information	80
Table 10. Potential Impact Definitions of Security Objectives for Categorization ...	84
Table 11. Security Constructs	85
Table 12. Potential Uses of Geospatial Information.....	94
Table 13. Information Sharing Methods and Concerns	97
Table 14. Impacts of Sharing Information.....	102
Table 15. Suggestions for Further Study	114

GEOSPATIAL INFORMATIONAL SECURITY RISKS AND CONCERNS OF THE UNITED STATES AIR FORCE GEOBASE PROGRAM

I. Introduction

Overview

Over the last decade, advancements in information technologies have dramatically reduced the costs involved with storing, managing and disseminating large amounts of data. These advancements have led to the development of Geospatial Information Systems (GIS) within the civil engineering community to share information with larger communities of interest, enabling complex decisions to be made more efficiently, with fewer resources, and at higher confidence levels. Military leaders face the challenge of deciding how to make their geospatial information readily accessible to authorized parties while mitigating the risks associated with information sharing. Unfortunately, many times these decisions are made without consideration of the underlying risks to critical information, infrastructure, and/or resources.

With increasing focus in the Air Force on quick, useful and accurate information, the GeoBase concept of “One Installation, One Map” has quickly emerged to provide an integrated common installation picture (CIP) to decision makers. As advancements in information technology continue to develop, so increases the ability to store, manage and integrate larger amounts of data. As problems of limited resources of *time*, *money*, and *manpower* continue to preoccupy organizations, technological advancements such as Geospatial Information Systems (GIS) and the internet have made it easier and more affordable to share information once considered unthinkable, allowing complex decisions

to be made with a more efficient use of resources and at a higher confidence. However, the same information technologies that allow those that need the information to accomplish their mission also may provide sensitive information to people with different agendas. Concerns continue to grow as the geospatial infrastructure makes it easier to incorporate sensitive information such as the USAF mission data sets (MDS) and regional information picture (RIP) information. The balance between information assurance and information sharing is delicate and the community is still sorting out the best ways to maximize security while encouraging users to share information in order to provide the widest benefits to the customers and the mission.

Motivations for Research

Motivations for this research stems from the researcher's personal interest in the GeoBase program. Having served in a command which embraced the technology early and instilled at the lowest levels the concepts, potential, and power of GeoBase, the researcher was among the first to help implement and shape the base-level GeoBase concepts in Alaska. During the initial implementation new questions were raised about the existing business practices about sharing these detailed installation maps. These issues became even more prominent in experiences in Korea, working with multiple agencies with high turn over rates. Information sharing was essential, yet often requires access across multiple disclosure levels such as for official use only (FOUO), secret (US only), and secret (releasable to Republic of Korea, RELROK). The struggle to utilize all available information while maintaining appropriate levels of classification became a challenge. Merging information to provide a better decision picture is necessary;

however, concerns abound about giving information to contractors or other outside requestors. Those challenging questions are the essence of this research.

Information sharing is essential, yet is hastened by the required multiple levels of disclosure. With the increasing amounts of geospatial information our military has been producing, one of the biggest challenges is ensuring that sensitive information is secure for its intended purposes. As users of the data, we are awed by its availability and demand quicker, more reliable, accurate, access. In the eagerness to see the potential for good, we do not always necessarily weigh the potential for bad.

Targeted Research Area

The targeted areas for this research is to review what is known about information security, risk management, and current USAF policies and guidance applied to geospatial information found within the USAF GeoBase program as denoted in Figure 1 below. A focus of this research is to also examine the progress that has been made in efforts to secure GeoBase's geospatial information in order to better map out what will be needed in the future.

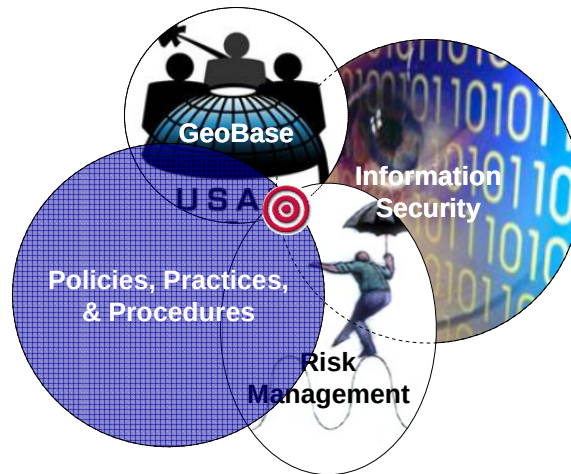


Figure 1. Targeted Area of Research

Research Goals

The overall research goal is to improve the general understanding of importance of balance between securing and sharing information in order to maximize USAF mission processes and minimize customer inefficiencies. By learning what works well and what does not work well from existing guidance and current problems, we can begin to see areas rich for improvement. As resources become increasingly limited, it becomes more important to secure and share them. Understanding the nature of the security risks posed by GeoBase the Air Force will be better equipped to balance the scales of information security and information sharing.

Overall Approach to Research

The overall approach to this research is to start with the motivations for research and develop primary research questions that relate to specific focused objectives which more broadly describe the intent of what is to be accomplished. Once the questions and

objectives are defined, then two types of literature reviews will be accomplished. The first literature review will cast a wide net to learn as much as possible about the topic of geospatial information, security and information sharing as well as subjects that touch or impact the topic of the thesis. These key concepts include, but are not limited to:

- USAF GeoBase Program
- Geospatial Information Systems (GIS)
- Information Security
- Information Assurance
- Information Sharing
- Critical Information
- Data-sharing policies
- Data Stewardship
- Risk Management
- Security Measures
- Sensitive / Critical data access controls
- Data protection
- Digital terrorism
- Digital Rights Management
- Information Life Cycle
- Vulnerability Studies
- Terrorism, Information Technology, and Vulnerability
- Knowledge Management
- National Map Efforts
- Global Information Grid (GIG)
- Freedom of Information Act
- User Rights and Privileges
- Internet Map Servers (IMS)
- Data Integration (Security)
- DoD Information Policies
- Information Resource Management (IRM)

The second literature review will be geared towards the research methodology and trying to discover the best way to find the answers we are seeking. Understanding the pitfalls and possibilities of certain types of research methodologies will help to target the right tools to accomplish this complicated task. We will learn more about why the exploratory case study was chosen in the context of our understanding about this topic and where the GeoBase program office is in its current life cycle and why an exploratory look is needed. Other considerations for choosing this type of research methodology were the researcher's background and interest, the audience, the limited available literature, and the

amount of time available for this study. These decision criteria strongly favor this type of qualitative approach. The difficult part, which encompasses chapters three and four, will be in developing the framework on how to collect and analyze information. The conclusions drawn from this framework will help provide answers to our questions so that we may begin applying this new knowledge in our decisions for the future. Figure 2 below provides a graphical view of this approach to research and will serve as the road map for this research effort (see also Appendix A).

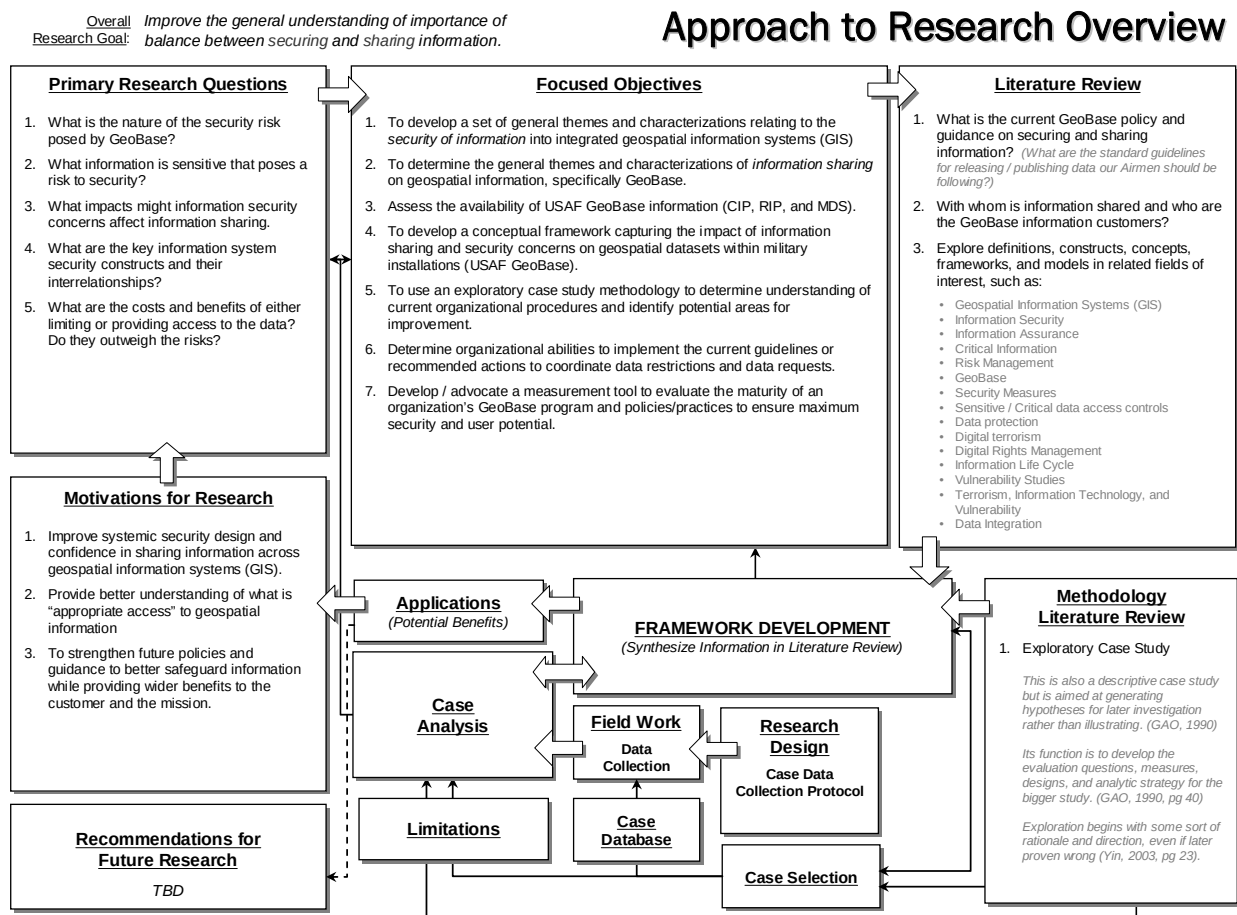


Figure 2. Research Design [adapted from (West, 2006)]

Primary Research Questions

Six primary research questions, listed below in Table 1, support and strengthen this overall research goal and form the primary goals (PG) of this research.

Table 1. Primary Research Questions

Primary Research Question	Description
PG1	What is the nature of the security risk posed by GeoBase?
PG2	What information is sensitive that poses a risk to security?
PG3	What impacts might information security concerns affect information sharing?
PG4	What are the key information system security constructs and their interrelationships?
PG5	What are the impacts of information security on information sharing within the GeoBase community?
PG6	What are the costs and benefits of either limiting or providing access to the data? Do they outweigh the risks?

Focused Objectives

The following seven focused objectives (FO), in Table 2, help to concentrate on how the primary research questions and the potential benefits of the research come together. These help to give a better idea of the direction and actions that this research will strive to accomplish.

Table 2. Focused Objective Questions

Focused Objectives	Description	Primary Research Questions Addressed	Potential Benefits of Research Addressed (see Table 1.3)
FO1	To develop a set of general themes and characterizations relating to the sharing of information and relative security concerns into integrated geospatial information systems (GIS)	PG1	PB1, PB2, PB3, PB5
FO2	To determine the general themes and characterizations of information sharing and security on geospatial information security concerns relating to the impacts of geospatial information, specifically GeoBase mission data sets (MDS).	PG2	PB1, PB2, PB4, PB5
FO3	Assess the availability of USAF GeoBase information (CIP, RIP, and MDS).	PG1, PG2	PB1, PB2, PB3, PB4, PB5
FO4	To develop a conceptual framework capturing the impact of information sharing and security concerns on geospatial datasets within military installations (USAF GeoBase).	PG1, PG2	PB3, PB4, PB5
FO5	To use an exploratory case study methodology to determine understanding of current organizational procedures and identify potential areas for improvement.	PG1, PG2	PB1, PB2, PB3, PB4
FO6	Determine organizational abilities to implement the current guidelines or recommended actions to coordinate data restrictions and data requests.	PG1, PG2	PB1, PB2, PB3, PB4
FO7	Develop / advocate a measurement tool to evaluate the maturity of an organization's GeoBase program and policies/practices to ensure maximum security and user potential.	PG1, PG2	PB1, PB2, PB3, PB4

Benefits / Implications of Research

This research will provide insight as to issues associated with the accuracy, access, and availability of geospatial information. These insights into the current challenges of information security and information sharing that the GeoBase program faces help to provide a more accurate target for the implementation of new policies and guidance, measures of control, or reengineering efforts of existing business processes. Table 3, below, identifies six specific benefits, but does not limit future possibilities.

Table 3. Potential Benefits of Research

Potential Benefit	Description
PB1	Identify needs and priorities for future investigation
PB2	Provide background research for the development of evaluation questions or measurement strategy (metrics)
PB3	Strengthen future information security / assurance policies
PB4	Improve confidence in system = willingness to share more information
PB5	More shared information = wider benefits to customers and mission
PB6	Establish a baseline of present organizational policies to compare effectiveness of new policies

Thesis Overview

This thesis includes five chapters and supporting information found in the appendices. This first chapter has provided an introduction and overview to the research questions. The second chapter will provide a more detailed review of the existing literature and begins to examine the context of what geospatial information is, introduce the Air Force's GeoBase program, and discuss problems, policies, risks, challenges, and touch on some of the recommended solutions and current control measures. Chapter 3 will then discuss the research strategy and why the exploratory case study methodology was selected, evaluate potential pitfalls to research, and explain how this case study was designed. Chapter 4 will then begin analyzing the case database, populated by sources of evidence and investigative protocol discussed in the case study design section of chapter three to answer the primary research questions. Chapter 5 will include further discussion

and recommendations along with possible limitations and future research ideas. Readers can find additional supporting information for this research in the back of this report under the appendices, bibliography, and researcher's vita.

II. Background

Introduction

The literature review contains detailed information on topics that are relevant to this research effort. This chapter will introduce information security, explain what geospatial information is, give a brief history of the GeoBase program; the emergence of geospatial technologies; the new paradigms, problems, and policies that have materialized; and provide a comprehensive review of the most recent information security and information sharing literature.

What is Information Security?

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), define information security as that which “protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities” (ISO/IEC 17799, 2000). Since information is a valuable asset, particularly in a national security and military environment, it must be protected. “Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected” (ISO/IEC 17799, 2000). This research will later discuss the different controls that can and are being implemented to achieve information security in the GeoBase program. We will explore the different policies, practices, procedures, organizational structures and software functions established to ensure that the specific

security objectives of the GeoBase program are met. (ISO/IEC 17799, 2000). This research will explore these forms as they relate to geospatial information.

What is Geospatial Information?

Geospatial information can be defined as any information that identifies the geographic location and characteristics of both natural and man-made earth-bound features. (Zettler, 2002). The types of geospatial information range from specific latitude and longitude coordinates to a general description of where something is located. These can take on the form of maps, overhead images, datasets, websites, addresses (Baker et al, 2004). “Geographic location is a key feature of 80-90% of all governmental data (Federal Geographic Data Committee, 2005). The Air Force has begun to use geospatial information to manage their installation infrastructure assets, for example, the locations of power distribution, water, sewer, telecommunications, and roads are stored within a database. Although geospatial information is diverse, it is still information, which is why it is important to understand the laws and policies that form the basis for rule sets used for managing both geospatial and non-geospatial information (Cullis, 2004).

GeoBase History

The art of mapping has not changed much over the centuries, but the understanding of the world, new tools, and improved technologies have enabled us to communicate better and know more about the environment that have served as the catalyst for the evolution of mapping. The most recent advances in technology and policy have culminated in innovative ways in which the U.S. Air Force approaches the process of mapping installations. These new applied technologies have enabled more informed decisions

through the comprehensive new mapping and information strategy for the USAF known as GeoBase. “The GeoBase program, officially launched in the summer of 2001 by the Air Force Civil Engineer, has transformed the traditional surveying and mapping process into an invaluable information resource for the larger installation mission, both at the home station and in the deployed environment” (Cullis and Tinsley, 2004).

GeoBase was the result of a structural, strategic, and tactical improvement. At the heart of this massive new reengineering effort was the customer.

“To realize the full benefits of the knowledge revolution, the geospatial information user community must redesign and improve how it does its business. This will require significant changes in culture, organization, education, and processes. For example, the geospatial information technology professional must become a full partner with the customer in defining operational needs for information, and exploring promising new technologies.”

- 3 CES Geospatial Information System Strategic Plan, 1999

Although GeoBase was not directly touted directly as a reengineering effort, it certainly can be classified as one as it held central to its mission and the end user (customer). This thesis will in part examine *why* a complete reengineering approach was needed, *how* the Air Force was able to successfully incorporate change in a culture steeped in resistance, as well as *what* some of the challenges management faced in making such a radical shift in the way in which bases are mapped and information is provided.

Just because converting bases over to GIS had not worked, it did not mean it was not the right strategy for the Air Force. By the late 1990s, several things had changed. Technology had advanced addressing previous customer concerns and was becoming much more affordable. Leaders throughout the different commands emerged; in particular, a leader emerged who understood what GIS could do for the Air Force and its mission.

Additionally, this person understood the need for paradigm shift in the way the Air Force executes its mapping business. In the fall of 1998, Colonel Brian J. Cullis coined the term “GeoBase” and had a clear vision of what the future could be and was well prepared to accept the challenge of being a change agent. One of the first things that was needed was to clearly separate the negative reputation that GIS was receiving due to the previous failed management attempts. The distinguishing new GeoBase concept was something new, it carried with it a clear vision and well developed plan for implementation. This new vision, “*One Installation...One Map*”, required a complete redesign of the way business was done. Implementation Plans were customized to each installation to help them traverse the path of change. The art of communication, education and persuasion were essential in helping the highest-ranking General to the newest Airman understand why there was a need for change and what they could do to help enable the required reengineering efforts.

From the beginning, it was clearly articulated that GeoBase is not a system, package, program, button, or particular software application, but rather a process or a complete integration effort. In essence, it was to be a new way of thinking about the data we use and collect. This new way of thinking included a way to use maps to display and integrate data, leveraging the best available commercial off-the-shelf GIS and GPS technologies to produce a composite Common Installation Picture (CIP). The CIP serves as the one picture portraying different databases across multiple functions. The concept of “*One Installation...One Map*” enables existing stovepipes to begin cross ventilating without having to overhaul the entire piping infrastructure.

Emerging Geospatial Technologies

In the mid 1980s and early 90s the Air Force began adopting different types of information technology to aid in the drafting and design of construction projects and base maps. Computer Aided Design and Drafting (CADD) is an enabling technology solution that helped address some of the initial problems of drafting by hand. Just as the organizations were determining the possibilities of having a digital CADD map, innovations in technology were being made in quantum leaps. Innovations such as Global Positioning Systems (GPS), affordable handheld GPS receivers, aerial and commercial satellite imagery, and Geospatial Information Systems (GIS) began opening the doors to new possibilities in the world of mapping.

A New Paradigm

The Air Force has made changes through the years from hand-drafted maps to computer-aided drafting, to today's revolution in utilizing Geospatial Information Systems (GIS) in the reengineered efforts of military mapping and decision-making.

“For the past three years, I’ve been immersed in managing change—change in how we employ geospatial information technologies to best support the defense installation mission. There is much written about the difficulties of leading change across large organizations with their many parochial interests. However, I have discovered that if you focus on what these disparate organizations have in common, such as the need for a map, it is much easier to achieve a broad consensus for change. And whether it’s the

young engineer assistant in the utilities shop at an Air Force base or an undersecretary of defense at the Pentagon, they are all eager and willing to learn of practical ways to employ geospatial technologies to perform their assigned missions more effectively” (Fuhr, 2004).

*Col Brian Cullis
Executive Manager, Defense
Installation, Spatial Data
Infrastructure (DISDI)*

It is due to the understanding of the customer needs and mission requirements, and the culture for change, which allowed the Air Force to embark on a reengineering to make such substantial improvements in their processes. As an organization, the Air Force must continue to seek improvements and maintain vigilance of its *customers, competition*, and be willing to *change* in order to stay on top.

New Paradigms, New Problems

The Air Force’s mission has been defining its direction since its inception in 1947. In December 2005, Secretary of the Air Force Michael W. Wynne and Air Force Chief of Staff Gen. T. Michael Moseley issued a joint Letter to Airmen stating, "Today, our world is fast paced, constantly shifting, and filled with a wide range of challenges. Our mission is our guiding compass, and now more than ever we need it to be clear and precise. Therefore, we have rewritten the Air Force’s mission statement to define where and what we do...The mission of the United States Air Force is to deliver sovereign options for the

defense of the United States of America and its global interests -- to fly and fight in Air, Space, and Cyberspace.” (Moseley and Wayne, 2005).

The new mission includes two new concepts, “sovereign options” and “cyberspace”. The incorporation of cyberspace into the mission recognizes the importance of information security and information sharing. In the new world of cyberspace, geospatial data makes up approximately one-half of the nation’s domestic economic activities and provides the edge in international competitiveness (Cullis, 2004). Once made strong by abundant natural resources and industrial revolution, countries and businesses are finding power in a new information revolution. For the military, international competitiveness is the ability to fly, fight, and win. As industrial resources become more readily available and begin to equalize the playing field, today’s world competitors seek to differentiate themselves through their abilities to manage information and knowledge. The demand for information and knowledge drives the need for new data. As the data and the dependency on data continue to increase, new problems and demands arise. In 2005, a survey of the metadata in the nation’s geospatial depository, Geospatial One-Stop, shows the federal government as the largest geospatial data producer, see Figure 3.

Metadata Records in Geospatial One-Stop as of 2005

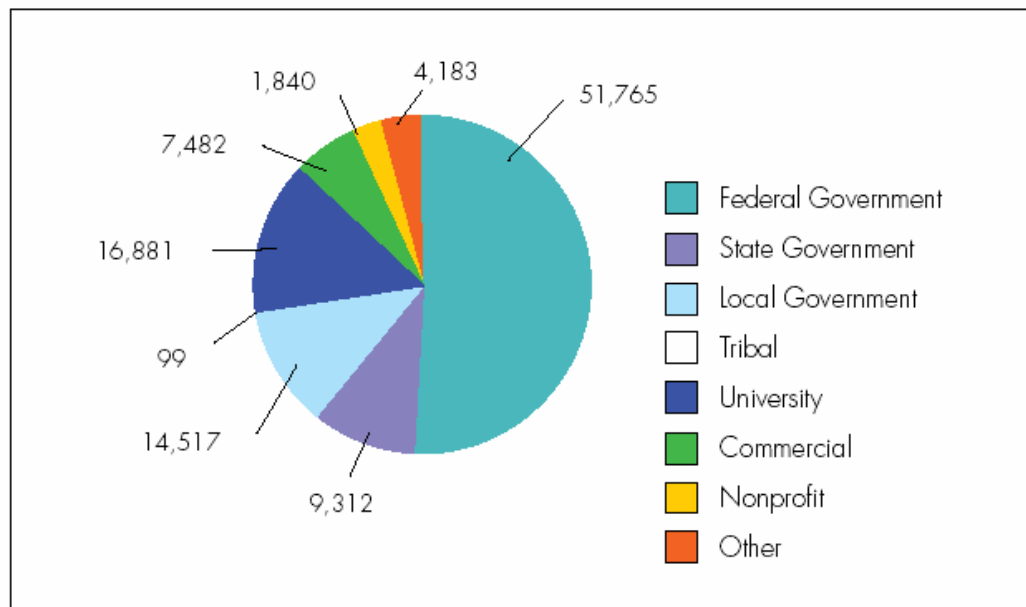


Figure 3. Top Geospatial Data Producers (Federal Geographic Data Committee, 2006)

Within the federal government, the Department of the Interior is the largest producer of geospatial data, as shown in Figure 4. The Department of Defense has invested heavily in information systems over the last few years and is producing a significant amount of geospatial data, much of which is not loaded in the Geospatial One-Stop system.

Metadata Records in Geospatial One-Stop by Federal Agency (as of 2005)

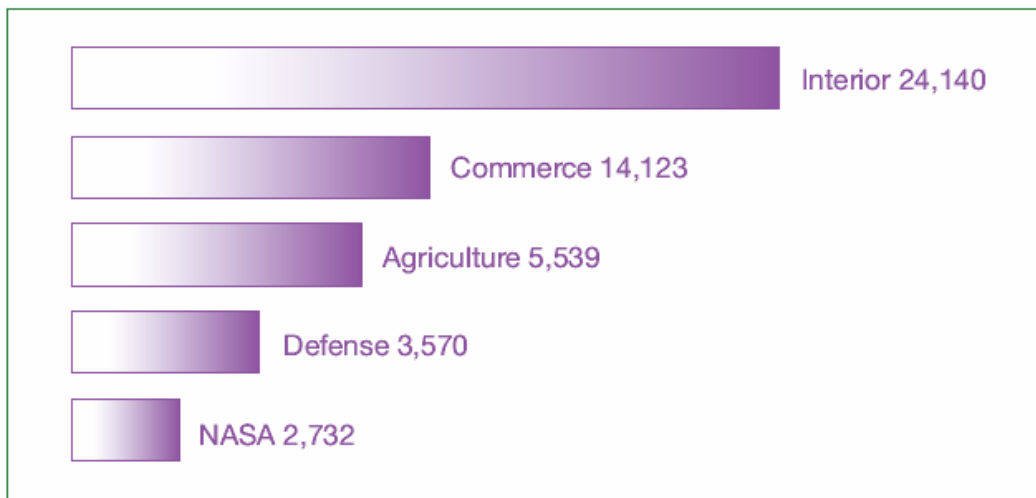


Figure 4. Federal Agencies Producing Geospatial Data (Federal Geographic Data Committee, 11 Aug 2006)

Geospatial information has continued to increase exponentially, as seen over the past ten years in Figure 5.

Global Clearinghouse Growth

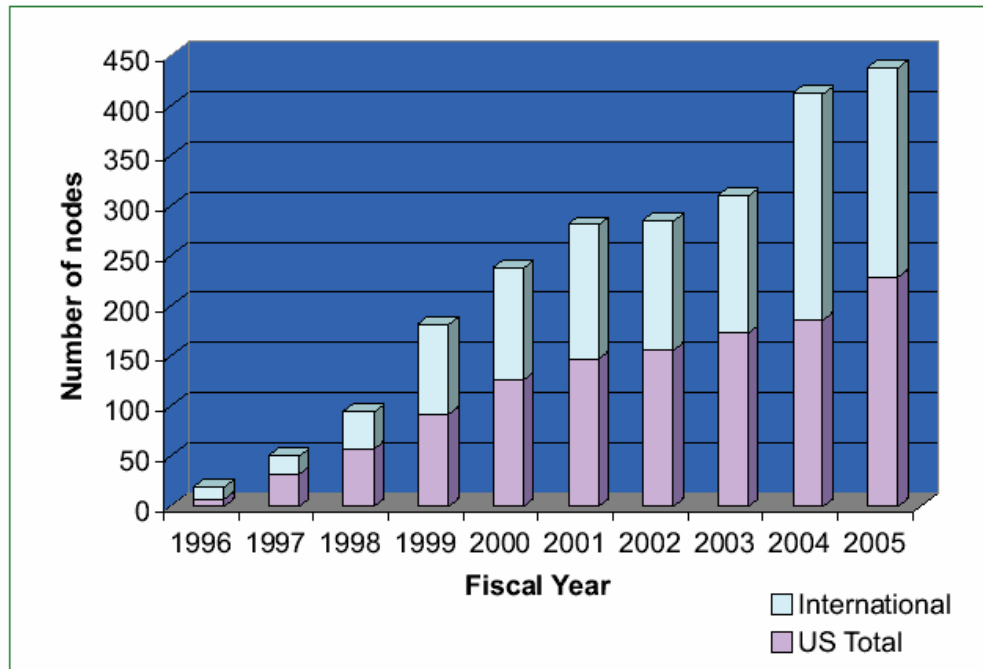


Figure 5. Geospatial Information on the Rise (Federal Geographic Data Committee, 2006)

As geospatial information systems have been rapidly expanding in the civilian sector, the USAF GeoBase program has witnessed tremendous growth as the need for minimizing fiscal waste and maximizing decision power has grown. This growth stemmed from the Air Force Civil Engineering (CE) community, whose need to provide accuracy, access, and accountability of installation assets drove an investment in the required equipment, skills, and additional data to form the geospatial information infrastructure called GeoBase.

Additional evidence of the expansion of geospatial information can be seen in the formation of the Defense Installation Spatial Data Infrastructure (DISDI) program in late 2004. This program was set up in the fall of 2004 to “organize the broad geospatial data

investments found across the business mission area of the DoD's Global Information Grid.” (B. J. Cullis, Jul 26, 2005). DISDI's successes in helping to provide focus to the entire DoD came as a result of seeing the need to reign in individual IT efforts across its massive organization. “DISDI is described today as a DoD mission capability comprised of those people, policies and practices necessary to acquire, steward and share “best available” installation and environmental geospatial data assets across the Global Information Grid—a system to provide users a seamless, secure, and interconnected information environment, for the real-time and near real-time needs of both the warfighter and the business user” (B. J. Cullis, Jul 26, 2005). Through the collected efforts of DISDI and GIS communities, a common direction and enterprise solution was adopted. Today, there is an establishment of not only the Air Force's GeoBase program, but also DoD GIS efforts that include the Navy's GeoReadiness, the Marines' GeoFidelis, and the Army's GIS-R, which is the Army's Installation Geographic Information & Services (IGI&S) program office. The expansion of program offices and mission related applications just within the last five years shows the need for accurate geospatial information technologies that provide critical information which enables decision makers, supports war fighters, aids planners, and increases overall situational awareness.

New Problems, New Policies

As new technologies emerged, government began to quickly feel the need to set policies and procedures to govern the use and application of the emergent technologies. Mapping efforts were becoming a more collaborative effort and needed cohesive management practices due to individual bases developing best practices. The problem

escalates when Airman Jones PCSs (changes duty assignments) and had been trained a certain way to accomplish the job and when in a new environment she must be retrained. The cost to retrain and relearn skills from one base to another was adding undue stress to an increasingly lean organization. Therefore, in the interest of finite resources a lowest common denominator approach became the applied practice, which did not warrant government funding or training.

New trepidations arose as the GeoBase program was implemented throughout the major commands. The same information technologies that allow those that need the information to accomplish their mission also may provide sensitive information to people with different agendas. Concerns continue to grow as the geospatial infrastructure makes it easier to incorporate sensitive information such as the USAF mission data sets (MDS) and regional information picture (RIP) information. The balance between information assurance and information sharing is delicate and the community is still sorting out the best ways to maximize security while encouraging users to share information in order to provide the widest benefits to the customers and the mission.

Post 9/11

No one event helped solidify those fears more than the September 11 2001 attacks. “After terrorists attacked the Pentagon and World Trade Center buildings, most governmental agencies hastily withheld map data and other records from the public, thus curtailing citizens’ ability to inform themselves” (Tombs, 2005). New requirements and guidance were needed for the management of data and federal information assets that relate to geographic locations. Some agencies do not recognize that geospatial data is public

record. “Legal cases at both the federal and state levels have nearly ended that assertion, which is now codified by many state public records acts and FOIA (Freedom of Information Act)” (Tombs, 2005). It has taken three years for the different arms of the government to publish *Guidelines for Providing Appropriate Access to Geospatial Data in Response to Homeland Security Concerns* (Federal Geographic Data Committee, Jun 2005).

The challenge now is defining the legal guidelines for what is “sensitive information”. Sensitive information has been defined as “Information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under the Privacy Act, and information not releasable under the Freedom of Information Act.” (Swanson, Hash, Wilson, and Kissel, 2005:C-10). In times of fear, such as during the war on terrorism, new emphasis has been placed “on undefined ‘potential’ and ‘possible’ risks to ‘sensitive’ or ‘critical infrastructure’ in prohibiting public spatial data access. While deliberating what records are ‘sensitive’ and ‘who’ should be prohibited access, records custodians are improperly using the ‘homeland security’ excuse to ignore records access laws” (Tombs, 2005).

Prior to 9/11, many of these concerns had never come into question. New laws continue to influence the evolution of how managing and protecting information, to include the Air Force’s GeoBase data for its installations and expeditionary sites. The Homeland Security Act of 2002 and the Federal Information Security Management Act of 2002

brought new definitions affecting information systems and security. Information security is defined in public law as:

“...protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and availability, which means ensuring timely and reliable access to and use of information.” - Federal Information Security Management Act – Public Law 107-347.

It is interesting in looking at the timeline of laws passed to see how definitions have changed over the years and are reflective of the major concerns and events of history, see Appendix E. Ultimately, we are all affected by the courts decisions. Appendix F offers a history of policy and guidance that has directly shaped and impacted the implementation and development of the USAF GeoBase program.

As the development of new technologies and concern for how those technologies are applied develop, so expands the social and legal structures within which they exist. This work will explore the supporting legal structures that attempts to set the boundaries for society to ultimately insure the safety and security of its citizens by looking at the laws and policies that affect the existence of the USAF GeoBase program.

Geospatial Information and the Law

As early as 1950, the federal government recognized the importance of managing information and established the Federal Records Act of 1950 which appointed the National Archives and Records Administration (NARA) as the primary agency responsible for management and oversight which cultivated the framework for records management

programs for all federal agencies. The importance of ensuring that nationally important transactions are recorded and safeguarded against loss remains a constant even as the government shifts from paper to e-government. Federal laws and regulations have helped establish common good practices for creating, using, and maintaining information that may be useful in making future decisions. As technology grows, so has the capability to store, maintain, and share information. One of the major concerns rising from the amassing of information was privacy. In 1974, the Privacy Act was established to regulate the “collection, maintenance, use, and dissemination of personal information by federal executive branch agencies and generally characterized as a “code of fair information practices” (United States Department of Justice, 2004). However, the Act's ill-defined language limited legislative case law history and made it difficult to interpret and apply. This is particularly notable as the laws are beginning to catch up with the capabilities of new information technologies and new systems, with particular interest in the growing utilization of geospatial information systems (GIS).

As the need to find more efficient ways to do business and manage increasing resources, the legislature passed new public laws to herd agencies into being more publicly accountable for reducing the mounting burdens of required paperwork and red tape. In 1995, Public Law 104-12, the Paperwork Reduction Act was signed, which eventually lead to the Government Paperwork Elimination Act in 1999. The Paperwork Elimination Act was monumental as the first law to establish guidance for the use of electronic signature technology, requiring “when practicable, Federal agencies use electronic forms, electronic filing, and electronic signatures to conduct official business with the public by 2003. In

doing this, agencies will create records with business, legal and, in some cases, historical value” (National Archives and Records Administration, 2000).

As agencies received guidance from their governing bodies, many organizations, including the Air Force began to realize the opportunities these laws created in fulfilling goals and requirements to eliminate waste and increase efficiency. As the government has spent over \$27.9 billion on information technology annually, laws have been passed to help ensure that departments are making sound investment decisions which effectively align IT projects with their business planning and measurement processes. The Clinger-Cohen Act (CCA) of 1996 “provides that the government information technology shop be operated exactly as an efficient and profitable business would be operated. Acquisition, planning and management of technology must be treated as a "capital investment." While the law is complex, all consumers of hardware and software in the Department should be aware of the Chief Information Officer's leadership in implementing this statute” (United States Department of Education, 2004). These new laws set the new standards forcing organizations to develop and organize information management capabilities to meet the different missions of government agencies.

As the Air Force found new uses for the GPS and GIS technologies and the GeoBase program emerged, these laws laid the groundwork for putting into perspective the need for change. GeoBase was the product of the combination of these laws, policies, and executive directives that has now helped to organize and streamline geospatial information into a powerful situational awareness and decision maker’s tool.

Soon, Geospatial Information System Strategic Plans began to emerge which reflected new priorities and attitudes within government. Each plan was custom tailored to

each base and designed to conform to multiple governmental directives such as the Government Performance and Results Act (GPRA), Paperwork Reduction Act (PRA), and Office of Management and Budget (OMB) mandates and guidelines. “These bodies of laws and regulations created the opportunity to move from budget and acquisition centric decision making to mission, architecture, service, and performance decision making” (Geo InSight International, Inc., 1999). In 1996, the Information Technology (IT) Management Reform Act was passed, which required federal agencies, including DoD, to identify a Chief Information Officer (CIO) and regulate IT investments. This was the first time “organizations were now required to strategically plan IT purchases and link them to specific mission goals” (Cullis and Tinsley, 2004).

Geospatial information offers new and exciting opportunities in expanding fields of interest. Accuracy, access, and accountability are the demands of the future and many different points of view will drive the need for the future legal clarifications and guidance (Schomper & et al, 1996). Examples of debates over geospatial information today include, personal privacy, sensitive vs. classified information, and liability on information provided, need for shared information (such as emergency responders and environmental care takers). GIS analysts and technicians continue to discover new applications and resume aggregating once lonely islands of information with the powerful bridging tools that geographic information systems provide.

These new applications of technology in to the GeoBase concept help to broaden our knowledge and expanding our capabilities. With new capabilities come new responsibilities. Future laws, policies and procedures will help information users and data stewards to continue to weight the fine balancing act of the need for national information

security and information sharing in an increasingly demanding environment for accuracy, access, and accountability.

Identifying Security Risks

As the military seeks to make more informed decisions based on information from geospatially related data, there are increasing concerns that this reliance may be exploited. To better understand the risk, the threats and vulnerabilities to the system must be understood. Solomon and Chapple define a vulnerability as “a weakness in a system that may be exploited to degrade or bypass standard security mechanisms” and a threat as “a set of external circumstances that allow a vulnerability to be exploited” (Solomon and Chapple, 2005). When vulnerabilities and threats overlap, this relationship defines what the risks are, as seen in Figure 6.

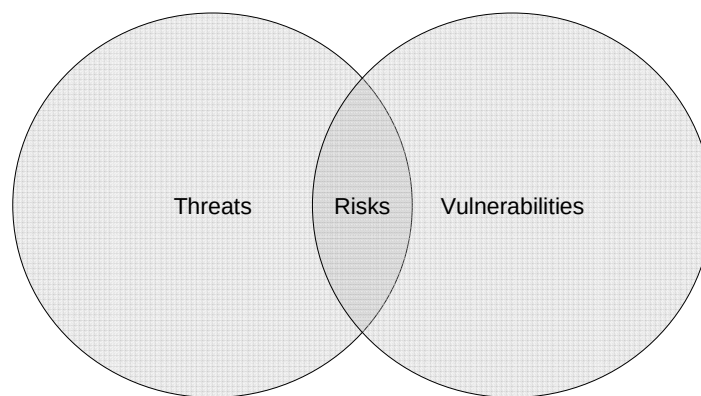


Figure 6. Identifying Risks (Solomon and Chapple, 2005)

There are a wide variety of common computer threats from viruses, worms, Trojan horses, port scanning, file share attacks, Operating System (OS) attacks, scams, spamming,

phishing, denial of services attacks, password guessing, backdoors, sweepers, sniffers, packet forge spoofing, IP spoofing, to the most obscure such as social engineering (Speed, Ellis, & Korper, 2002). However, concerns regarding the interception of data, theft / release of sensitive or confidential information, unauthorized access to privileged information, theft of other computer hardware or devices, system penetration by an outsider, laptop and hand held computer thefts, computer system and network abuse, and sabotage of sabotage of data or networks are also among the top breaches of security (Australian Institute of Criminology 2006, 2006). Among these real threats, the greatest risk to the security policies is not the physical network, but rather the accountability of the people within the organization. By far, our human nature is our greatest danger. However, we can help mitigate this threat by physically designing the network to be safer, educating our airmen and enforcing the standards set out by the security policies and defined by routinely conducted vulnerability assessments.

The Air Force must also consider the physical security of the system itself, the management of the database and its integrity, as well as the type and scope of access to the database. Protection of the availability of services and information is important to ensuring that users have access to the information when it is needed. The issue that geospatial information is available publicly is not the only security risk, in 2000 there were a reported 25,000 attempted intrusions into the defense system. Of those attacks, 245 of them were successful. Of this less than 1% of successful attacks, 96% of those were found to be preventable if users had followed established protocols (Onley, 25 April 2004). The network security on which the GeoBase data relies is heavily monitored and network

personnel continue to strive to improve network security by limiting the access to the system and implementing policies such as mandating firewall protection, confidential user accounts and passwords, no shared accounts, password-protections, locating computers and servers in a physically secure environment, establishing file permissions and user rights on certain files and folders, and separating classified information on separate systems. Beyond the security of the network, let us discuss the primary issues that are more closely related to the risks of geospatial information and the capabilities that these systems provide.

Only recently has public access to information become a perceived concern (Tombs, 2005). Following the attacks on 9/11, almost overnight, federal officials became worried that some public information is now too public and “agencies cut off access to thousands of documents on the Internet, ordered certain information in government libraries to be withheld or even destroyed, and simply stopped providing some information that used to be routinely released to the public” (Matthews, 2002). The concerns over providing a terrorist access to information that would help him develop or use a weapon of mass destruction lies at the heart of our fears. “Thus, digital maps are no longer available online from the National Imagery and Mapping Agency, a CD-ROM containing information on the nation's water supplies was ordered destroyed at depository libraries, and tens of thousands of documents vanished from government Web sites. The information clampdown has touched off a sprawling debate over how much information should be — and legally can be — withheld from the public” (Matthews, 2002). Soon after, the National Imagery and Mapping Agency (NIMA), now the National Geospatial-Intelligence Agency (NGA), asked the RAND Corporation to assist in developing a framework to

assess the security implications of publicly available geospatial information. This study remains among the few to address these specific types of implications and provides a broad base for future research. Their studies began to put into perspective the scope of federal geospatial information, finding it to be widespread across “465 programs, offices, or major initiatives at 30 different federal agencies and departments that make various types of geospatial information publicly accessible” (Baker et al, 2004). RAND concluded that very few (6% of the 629 datasets studied) appeared to be capable of fulfilling possible terrorist’s needs. Even fewer sites (less than 1%) were found to provide critical information, both useful and unique, by their definition to potential terrorists. They also noted that in so many cases, since geospatial information exists in numerous ways, alternate forms of the same information existed readily in the public domain, beyond the control of federal sources” (Baker et al, 2004).

The level of risk that we are willing to take hinges on the values that we place on the following three strategic factors of information: data accuracy, access, and accountability (Schomper et al, 1996). Evaluating the impacts of not having accurate information, timely access to it when needed, or responsible ways of accounting for the demands of information will help in the understanding of the risks that are willing to accept. This game of risk is one of compromise.

Top Challenges

The goal of reducing the security risks and increasing the range of access across communities and knowledge seekers is not sought without challenge. The primary

challenges discussed in this section are not unique to only the GeoBase program, but are challenges that leaders in information management face when dealing with information security and information sharing. The first hurdle that must be overcome is in how we define, or do not define, the sensitivity of information. We will look at issues surrounding the classification of information, sharing information, and the inconsistencies of policies and guidance and see how these add to the top challenges of creating a defensible geospatial information strategy.

Defining the Sensitivity of Information

Among the top challenges in the balance of information security and information sharing is defining the sensitivity of information. In times of fear, such as during the war on terrorism, new emphasis has been placed “on undefined ‘potential’ and ‘possible’ risks to ‘sensitive’ or ‘critical infrastructure’ in prohibiting public spatial data access. While deliberating what records are ‘sensitive’ and ‘who’ should be prohibited access, records custodians are improperly using the ‘homeland security’ excuse to ignore records access laws” (Tombs, 2005). Concerns over how the government chooses to define “sensitive but unclassified” information fuel hesitation to share information. Government watchdogs fear that a new sensitive information category could give agencies a way to hide embarrassing information from public scrutiny (Matthews, 2002). There are so many factors to be considered when deriving a definition of sensitive information. Even if something is considered “sensitive”, geospatial data has a tendency to change over time. As the environment and value of the information changes, so do the risks to security. It is not viable to make one decision in the lifespan of the data, but a constant litmus test must be

made which can alter the decisions about access. These decisions affect not only the originating organization, but also the entire chain of users both up and down the information stream (Federal Geographic Data Committee, 2005).

The classification of data has been the most effective way to manage the differences in the level of risk that certain data bears. Once the challenge of identifying what information is sensitive, there becomes multiple challenges in applying a designation to information. Overprotecting data severely hinders users that depend on using that information on a day-to-day basis in doing their job and accomplishing the mission. Restricting information has tremendous costs, in not only the added time and maintenance costs that it takes to manage that information, but also the expanded personnel safety risks. For example, consider electrical or natural gas distribution lines that are part of the critical infrastructure of an installation. If these distribution lines are classified as “SECRET”, it would result in a tremendous impact on the electricians and utility personnel responsible for maintaining those lines, not to mention the safety hazards for construction crews getting ready to dig in an area where utility lines have not been identified to them. Limiting access to information may have greater risks associated. It is very important to select data protection measures that are commensurate to all the risks; in order to classify or restrict access to data; the risks must outweigh the benefits (United States Air Force, Air Mobility Command, 2005).

Air Force policy towards restricting access to geospatial data is the exception rather than the rule (Dunn, 2005). These restrictions “must be approved by the appropriate Headquarters Air Force (HAF) functional manager and must be based on public law, security classification or other DoD regulatory publication” (Dunn, 2005). Restrictions are

to “only be applied to the data identified and not the entire system or collective group of data in which it resides or is produced” (Dunn, 2005). Problems with this type of policy reside in the burden of management to track and communicate the necessary restrictions across multiple agencies and changing personnel.

The challenge to data owners and stewards is to define what “sensitive information” is explicitly. The current guideline that is offered to the geospatial data community for identifying sensitive data, determining their risks, and assessing benefits is based on three factors: 1) risk to security, 2) uniqueness, and 3) net benefit of disseminating the data. These three factors were central to the Federal Geographic Data Committee (FGDC) as they developed a decision tree intended to act as a guideline to help organizations decide on what is reasonable access to sensitive data as shown in Figure 7 (Federal Geographic Data Committee, 2005). It remains important to launch discussions within organizations so that they can begin to ask the initial questions to evaluate the content of their information. Guidelines such as these help to provide an evaluation method that offers a hope for consistency.

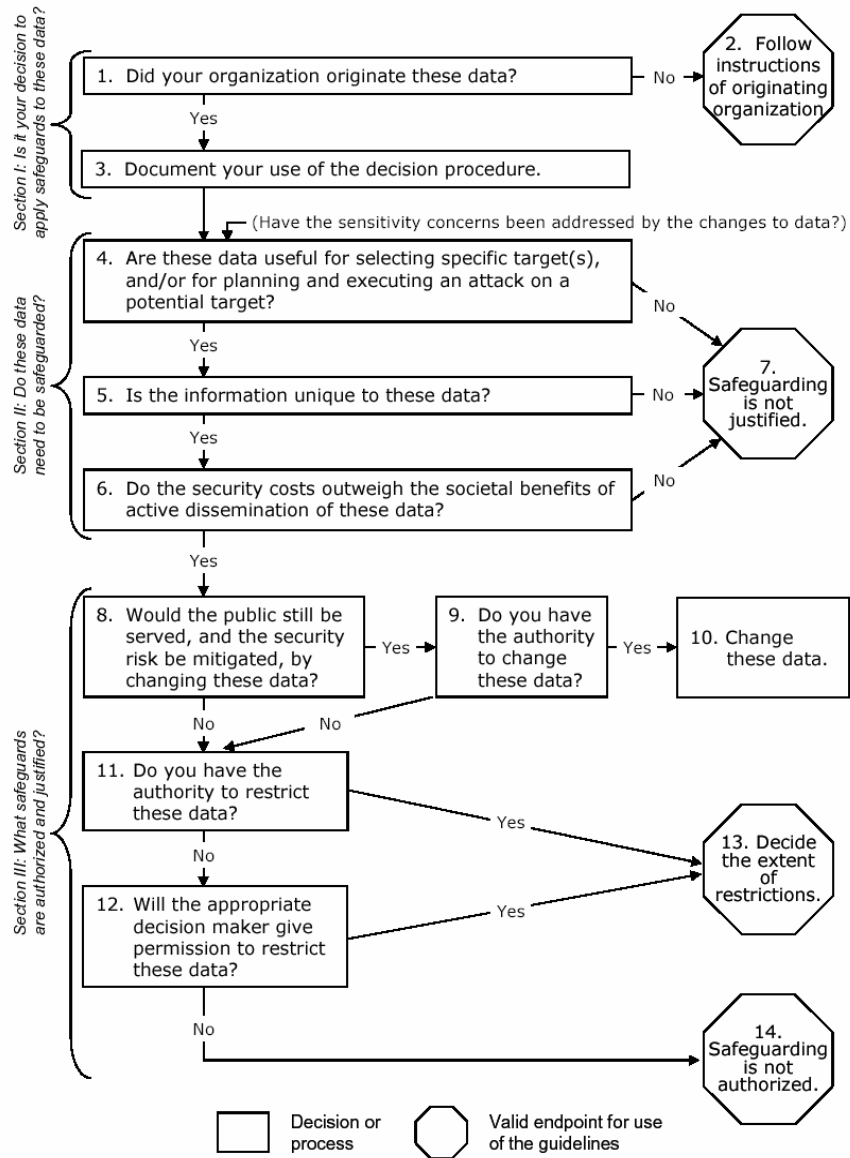


Figure 7. Decision Tree for Providing Appropriate Access to Geospatial Data in Response to Security Concerns (Federal Geographic Data Committee, 2005)

The sensitivity of derived geospatial data offers additional challenges. There are no established and validated mathematical formulas that can estimate the values of sensitivity when combining or querying multiple datasets. The same thought process in determining the sensitivity of the original work should be applied each time data is extracted or

combined to create a new way of looking at the information it provides (Federal Geographic Data Committee, 2005). Concerns over these derived geospatial datasets supplicate the trepidations of aggregating information. At what level of aggregation does information become sensitive? The GeoBase program recognizes that there are some instances where storing and providing access to aggregated data would constitute a vulnerability, but work diligently to provide protection. Currently, each installation is responsible for performing periodic reviews on all datasets and combinations thereof to determine if they come together and constitute an unacceptable risk (United States Air Force, Air Mobility Command, 2005).

Information Sharing

Although on smaller scale, the GeoBase offices have experienced the same type of challenges the Department of Homeland Security (DHS) is facing in encouraging organizations to voluntarily share information. There is a sense of hesitation and uncertainty among data owners to share information, perhaps over fear liability, embarrassment, or a fear of loosing power or control. Regardless, the importance of sharing is paramount to ensuring consistent, well-informed decisions are being made. Failing to provide information, leaves data users to pursue and use less reliable sources. The U.S. Government Accountability Office (GAO) captures the sentiment of many organizations in their March 2006 report entitled, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism Related and Sensitive but Unclassified Information*. Their report highlights the problems that offices such as the GeoBase office in the Air Force faces as an information broker, both a user and provider of

geospatial information. One of the biggest challenges is in the identification and designation of sensitive information. The GAO study found that over 26 federal agencies surveyed, there were 56 different sensitive but unclassified designations (Powner and Larence, 2006). Typically, GeoBase offices are faced primarily with the following three designations: Classified (SECRET), For Official Use Only (FOUO), and Unclassified. The challenges of managing classified information have been discussed, but we can quickly see how intertwined these challenges are and the need to overcome these hurdles in the quest of sharing information. For example, consider emergency responders and command and control functions, such as the Survival Recovery Center (SRC) or Damage Control Groups (DCG), abilities to coordinate a safe cordon around a hazardous chemical spill without informative maps and critical geospatial information. If information is not shared and available for the people who need it to respond to emergencies or make command decisions, we have failed to secure ourselves by giving the most to the situation we possibly could. Geospatial information provides the security of knowing that the people making decisions have the tools they need to ensure our safety.

An initial challenge of the GeoBase community was getting other organizations to understand the benefits of sharing information and realizing the power of a collective information bank. If information owners had a negative experience or the collective system did not satisfy their requirements, the willingness to share was gone, thus the potential to leverage their information against others has vanished. Most concerns associated with sharing information were related to the ability to ensure their information would be protected with at least the same level of effort (Powner and Larence, 2006).

The development of multi-level agreements would help users understand the responsibilities and the organization understand what information should be given out and to whom. Examples of multi-level agreements are every time the Air Force collaborates with commercial entities, such as engineering design and construction firms, which require data for contract execution. Often times, sharing data between services such as the Air Force and the Army, causes its own set of problems, creating duplicate datasets between services is against the “one installation, one map” motto. Serving overseas and working with a host nation has created difficulties in reaching agreements. Multiple systems, often found overseas, require careful attention in detailing what can and cannot be shared. There is data that different agencies and countries need to be able to share, but in some situations this is not happening. Once the data is shared, there are very few controls that remain in place. Some of the major architectural-engineering firms have files and files of critical geospatial information in their project files and reference libraries. Although there are signed agreements, disclaimers, and consents, which are given at the time of data conveyance, the reality of the business process is that the government just has to trust that others understand the costs to security.

Inconsistencies in Policies and Guidance

The inconsistency of policies and guidance that drive business process continue to add complication to the information security challenge. Numerous existing studies, policies, instructions, guidance, recommendations, and directives have been issued at nearly every level of the Department of Defense (DoD). For the longest time, the guidance was deferred to each installation commander or relied on existing vague guidance from

other communities such as public affairs, operations security, or communications. No one policy or guidance lends assurance to geospatial data security and information sharing, each is interwoven and at times leaves room for interpretation or are contradictory. Even within the Air Force, the major commands, wings and squadrons differences exist in the way these documents are interpreted. Many installations have developed their own local policies to address their needs. Now, multiply these differences every time organizational leadership boundaries are crossed or as leadership within organizations change.

Problems exist beyond the initial guidelines. For example, whose authority is it to change or restrict data? Is it different for each data layer? Who is to say that the data is useful for planning and executing an attack? The yes / no decisions are not as simple as the decision tree presents. Until organizations have a mutual level of understanding on how to make the complex qualitative decisions required for safeguarding information, there will continue to be added challenges. We are getting better, but there is still much work to do. The latest draft security policies, currently being vetted through the Air Force do much to help focus past inconsistencies. More than anything, having the conversation about security concerns and the need to share information is most important. The more information we can share on the challenges of security, the more we will be able to understand the problem and can begin to develop solutions to incorporate both in policy and in practice.

III. Methodology

Purpose and Organization

There are many ways in which research can be conducted, research methods such as experiments, surveys, archival analysis, case studies, and historical research are like tools in a carpenter's toolbox and the researcher must intelligently choose the most useful research tool from the toolbox to get the job done. Choosing the wrong tool could lead to criticism of the conclusions. Worse yet, selecting the wrong methodology wastes time in finding the answers to the researcher's problem. In developing a research strategy it is important to understand what tools are available and how they work to answer the questions. This chapter discusses the approach to developing the methodology to provide the best way to answer the research questions, the value of the case study research strategy, and why an exploratory case study is the best approach for this research.

Developing the Research Strategy

Robert Yin, a respected researcher and expert in applied social science research methods, suggests that researchers should select strategies based off three situational factors "(a) the type of research question posed [the "who", "what", "where", "how", and "why" questions], (b) the extent of control an investigator has over actual behavioral events, and (c) the degree of focus on contemporary as opposed to historical events" (Yin, 2003:5). Figure 8 represents the basic research strategies that one can select from based upon the situational factors in the research.

Strategy	Form of Research Question	Requires Control of Behavioral Events?	Focuses on Contemporary Events?
Experiment	how, why? ☒	Yes ☐	Yes ☒
Survey	who, what, where, how many, how much? ☐	No ☒	Yes ☒
Archival Analysis	who, what, where, how many, how much? ☐	No ☒	Yes/No ☒
History	how, why? ☒	No ☒	No ☐
Case Study	how, why? ☒	No ☒	Yes ☒

Figure 8. Relevant Situations for Different Research Strategies (Yin, 2003:5)

Based upon this taxonomy of research strategies, the characteristics of this research are reviewed to determine which research methodology to employ. In this research, the form of research questions have taken on the form of “How and why questions are more explanatory and likely to lead to the use of case studies, histories, and experiments as the preferred research strategies” (Yin, 2003:6). This helped further lead the research in the direction of a case study.

The Extent of Control

This research has very little or no control over the actual behavioral events. The researcher cannot manipulate any of the behaviors or decisions and is far enough removed from the context of the organizations to exert any influence on the outcomes of the study. The experiment is the only strategy that requires the control of behavior. There is currently not enough data or knowledge to set up a controlled experiment regarding this complicated subject.

The Degree of Focus

The third factor in considering selection of research strategy is the degree of focus on contemporary as opposed to historical events. Although it is important to understand the history and reasons why decisions were made, the research intent is to understand the contemporary events found within the Air Force community. The nature of the problem in itself is contemporary, as the Air Force has never faced the extent of these challenges brought about by technology and culture.

Considering these situational factors, the researcher's conclusion was that the best tool to tackle the intricacies of these research objectives is the *case study method*.

Case Study Research

The case study is one of many strategy tools for the researcher and has three basic purposes: explanation, description, and exploration. "Doing a good case study is more than just looking at what is happening in a few instances. It is a special systematic way of looking at what is happening, of selecting the instances, collecting the data, analyzing the information, and reporting the results" (Datta, 1990:23). A case study is useful for learning about complex circumstances and is the preferred strategy "when the investigator has little control over events, and when the focus is on a contemporary phenomenon within some real-life context" (Yin, 2003:1). In this particular case, since GeoBase is relatively a new concept for the Air Force and has not been researched, applying case study strategy will help to contribute to the body of knowledge on the technical and cultural aspects of geospatial information systems. Learning how GeoBase fits into the greater context of security and sharing is the goal of this case study research.

There are three predominant types of case study research: explanatory, descriptive and exploratory case studies. The conditions of the study will again dictate which type of case study is most appropriate. The explanatory is used to explain a course of events, whereas the descriptive study aims at presenting a complete description or overview of a phenomenon within a certain context. In exploring the possibilities, the exploratory case study must both be able to explain and describe in order to have an in-depth understanding of the different aspects involved. Sometimes it is necessary to explore questions and reach beyond the surface to develop measurement constructs for further research.

Why an Exploratory Case Study?

The exploratory case study is the most useful for evaluating programs where uncertainty exists and is designed to assist in the development of future evaluation questions, elements of measure, and new strategies. Before investing in costly investigations, an exploratory case study can help pin point areas which may provide greater returns on investments in both time and money. An exploratory case study helps to narrow the scope of future research so that it yields greater understanding and a logical place to start (Datta, 1990:40). Case studies are the perfect tool, “aimed at defining the questions and hypotheses of a subsequent study or determining the feasibility of the desired research procedures” (Yin, 2003).

Case Study Design

This research employs a single-case with multiple units of analysis. This embedded type of design was selected for several reasons. First, its unique ability to be representative of the how geospatial information is treated in the military and “to capture the

circumstances and conditions of an everyday or common situation” in the Air Force (Yin, 2003:41). Another reason behind this rationale is that this particular case is revelatory, meaning that there has been relatively current changes in technology and the limited time and opportunity for researchers to study these newly raised problems. A third advantage to the single-case study is that this will help to set a benchmark identifying issues and current processes that may aid in future longitudinal studies that can help compare two points in time (Yin, 2003:42). The main unit of this case study is the US Air Force GeoBase community as a whole. The embedded units of the headquarters element, different major commands (MAJCOMs), the relationship to joint services and other customers will be important to consider. Depending on the level of analysis required on each embedded element, different data collection techniques will be used in order to enhance what is found in the single case environment.

The framework to support this single-case (embedded) method is threefold: 1) define and design, 2) prepare, collect, & analyze, and 3) analyze and conclude. These next sections will discuss the requirements, suitability, and selection of the case design.

Step 1: Define and Design

The initial stage of this research sets the foundation and direction for this case study (see Figure 9 below). There are three sub stages important to understand before continuing into the rest of the research: 1) develop research questions, 2) select context and case, and 3) define what are to be the units of analysis and design protocol for data collection.

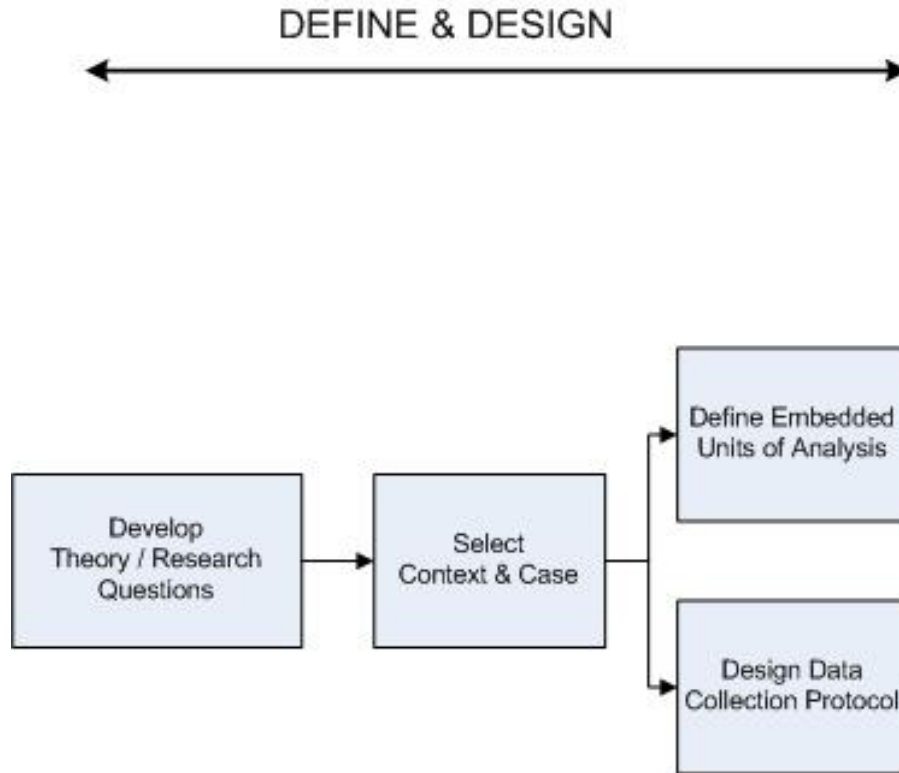


Figure 9. Single-Case Study (embedded) Method - Phase 1 (Yin, 2003:50)

Developing the Research Questions

In the first stage, a specific definition of the problem helps to establish boundaries and reign in what type of case selection would be the most helpful in answering those questions. In this research, the question focuses on seeking an understanding of information security and information sharing processes of geospatial information in the US Air Force GeoBase program.

Context and Case Selection

The context of the case becomes clearer as we better understand what it is we want to accomplish. The context and case of the GeoBase program office within the Air Force seems a natural case selection in the quest to find how we can get the most out of our GeoBase provided geospatial information while maintaining security (see Figure 10 below).

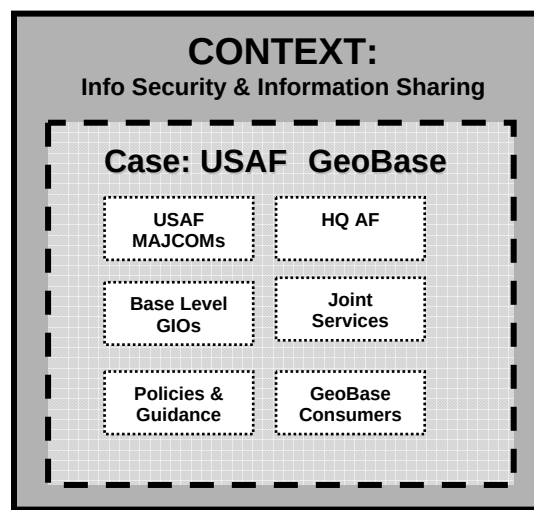


Figure 10. Case Study Design

Defining the Units of Analysis

Defining the units of analysis and designing the data collection protocol becomes the third biggest decision in setting up this research. This research could take many directions dependent on the selection of the context and case. For instance, we could have chosen to look at one particular major command or a specific unit. Likewise, we could have broadened our context and broadened our scope to look at the entire Department of Defense. Perhaps, these may be areas of interest for future research. The focus of the primary research questions help to dictate what the appropriate unit of analysis should

become. Instead, it seemed more appropriate to include in the exploration the entire US Air Force GeoBase program and examine the entire organization, from the Air Staff down to the unit level, as the unit of analysis.

Data Collection Protocol

Designing the data collection protocol further commits the focus of the research down a path, where we hope to find the most useful tools and evidence to develop answers to the complex research questions. Yin discusses three principles case study researchers should follow to help deal with problems of validity and reliability (Yin, 2003:85). These three principles: “(a) using multiple, not just single sources of evidence; (b) creating a case study database; and (c) maintaining a chain of evidence” are particularly important to the collection of data in case study research (Yin, 2003:85). In this section, we will examine these three principles and explain their importance in the development of this research’s investigative protocol, identified in Appendix A.

Using Multiple Sources of Evidence

Therefore, the case data collection protocol for this research was established with both these principles and requirements of the human subjects review board in mind. Within the context of the questions, traces of evidence had to be found in order to corroborate converging ideas. Yin cites six sources of evidence (see Table 1) and offers insight into their different strengths and weaknesses to consider when building supports for the case database.

Table 1. Six Sources of Evidence: Strengths and Weaknesses

Source of Evidence	Strengths	Weaknesses
Documentation & Archival Records	• Stable – can be reviewed repeatedly • Unobtrusive – not created as a result of the case study • Exact – contains exact names, references, and details of an event • Broad coverage – long span of time, many events, and many settings • Precise and quantitative	• Retrievalability – can be low • Biased selectivity, if collection is incomplete • Reporting bias – reflects (unknown) bias of author • Access – may be deliberately blocked • Accessibility due to privacy reasons
Interviews	• Targeted – focuses directly on case study topic • Insightful – provides perceived causal inferences	• Bias due to poorly constructed questions • Response bias • Inaccuracies due to poor recall • Reflexivity – interviewee gives what interviewer wants to hear
Direct Observations	• Reality – covers events in real time • Contextual – covers context of events	• Time-consuming • Selectivity – unless broad coverage • Reflexivity – event may proceed differently because it is being observed • Cost – hours needed by human observers
Participant Observation	• <i>(same as direct observations)</i> • Insightful into interpersonal behavior and motives	• <i>(same as direct observations)</i> • Bias due to investigator's manipulation of events
Physical Artifacts	• Insightful into cultural features • Insightful into technical operations	• Selectivity • Availability

(Yin, 2003:86)

Creating the Case Study Database

These sources of evidence are weighed against the nature of the case selected and begin to become the supporting structures in the construction of the case database. This section will examine how the case study database will be populated, as noted in Figure 11.

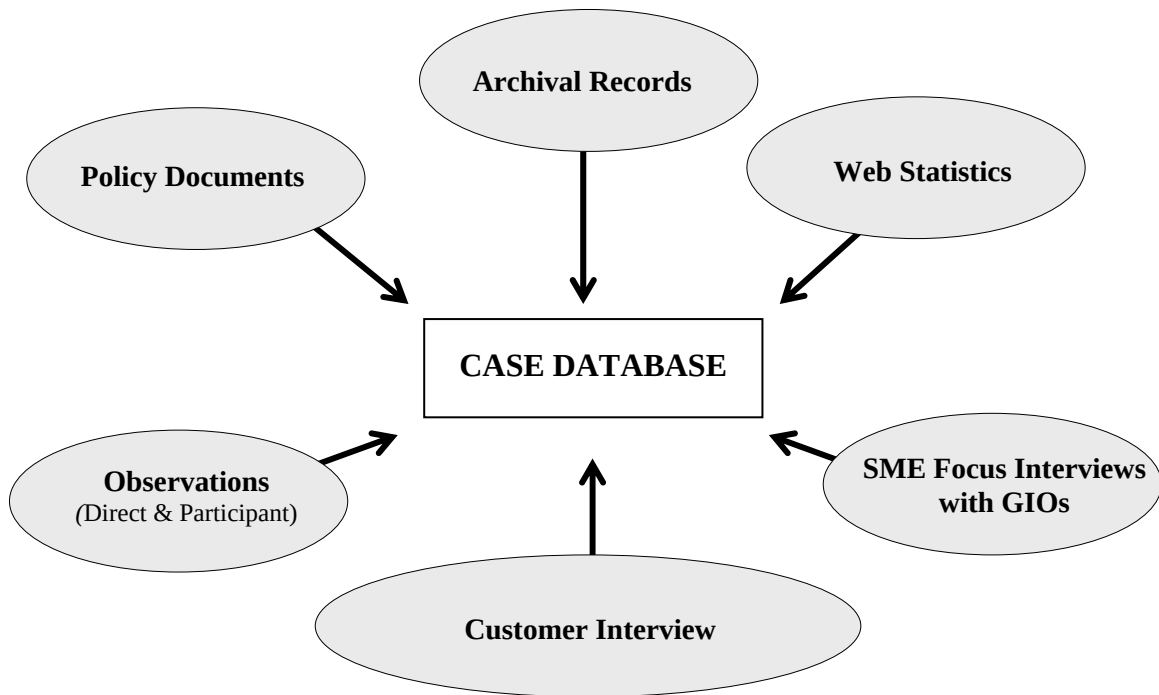


Figure 11. Building the Case Study Database

Subject Matter Expert (SME) Focus Interviews

The case study interviews were not selected at random, but rather with careful consideration for the level of expertise, experience, and recognition as subject matter experts (SME). Those interviewed represented a combination of military and civilian leaders/managers perspective that have primary responsibilities for GeoBase program. The interviews were spread across different commands of the Air Force GeoBase Community. Interviews were conducted between the October 2006 and February 2007 timeframe. Interviews were conducted over the phone. As per the human subjects review board exemption requirements, no identifying information obtained from the survey information or through interviews will be recorded, retained or reported in the final thesis. This is to protect individual's data from being disclosed outside the research setting so that it could

not be interpreted or used in such a way which would be damaging to the subject's financial standing, employability, or reputation. The formal interview protocol can be found in Appendix B.

Interview questions were developed and organized by the following common security categories: Administrative, Logical / Technical, and Physical controls, and further defined in Table 2.

Table 2. Common Control Categories

Control Category	Description	Example
Administrative	Policies and procedures designed to enforce security rules	- Hiring practices - Usage monitoring and accounting - Security awareness training - Data Sensitivity Matrices - Risk Assessment - Planning - System and Services Acquisition - Certification, Accreditation, and Security Assessments
Logical / Technical	Object access restrictions implemented through the use of software or hardware	- User identification and authentication - Encryption - Segregated network architecture - Personnel Security - Physical and Environmental Protection - Contingency Planning - Configuration Management - Maintenance - System and Information Integrity - Media Protection - Incident Response - Awareness and Training
Physical	Physical access to hardware limited	- Identification and Authentication - Access Control - Fences - Walls - Locked doors - Audit and Accountability - System and Communications Protection

derived from (Solomon and Chapple, 2005; Swanson, Hash, and Bowen, 2006.)

These categories lead to the arrangement of the different questions guiding the interview discussion.

Policy Documents

Policy documents are physical evidence and can be used to help corroborate information from other sources and triangulate in on situational facts (Yin, 2003:87). These documents play a key role in evaluating the current expected business practices policy makers place on organizations to drive actions towards information security and information sharing. An examination of the Air Force policies and their timeline regarding the GeoBase program may provide insight into patterns or causes of practices that help or hinder the intent. As this research will further discuss in chapters four and five, how the organization chooses to construct, interpret, and implement policy will lead to certain actions and responses from the affected organizations. The strength, weaknesses, or lack of policy all together will influence the program's behavior. The final analysis will incorporate what was found in this exploratory case study. Appendix F lists the relevant policies and guidance documents found in this research.

Archival Records

Very similar to the documentation of policy documents, archival records are often seen in the form of service records, organizational records (charts and budgets), maps and charts, lists, survey data, and personal records (calendars, phone lists, memorandums) (Yin, 2003:89). Any archival records found will be used to help support and lend further credibility to the chain of evidence.

Customer Interviews

As we study the geospatial information processes, particularly in the GeoBase environment, it is important to recognize the customer, whom receives the final benefit.

Hammer and Champy describe processes as “...a collection of activities that takes one or more kinds of input and creates an output that is of value to the customer” (Hammer and Champy, 2003). If part of the primary goal of this research is to “maximize USAF *mission* processes and minimize *customer* inefficiencies”, then it becomes very important to understand our customer’s perspective as we form opinions and policy. This research will consider a few key customers in the GeoBase process, but will not have time to exhaust the list of many who receive value from receiving geospatial information.

Observations

By being aware of the things that are happening around oneself is made in part to the observations that take place. “Such observations serve as yet another source of evidence in a case study” (Yin, 2003:92). Observations of how geospatial information systems (GIS) work can be invaluable at understanding the technologies being used and the problems or limitations that might be encountered (Yin, 2003:93).

Web Statistics

Although statistics may be grouped as a type of archival records, in this case, there was enough of a distinction to try to find usage statistics of the web servers from each of the primary GeoBase / GeoReach web servers. Using the web statistics from each of the commands may help in understanding who the primary customers are; where, when, and what they are using geospatial information for; and if there are any patterns or outliers that may help to streamline their user experience and reduce risks to the information. Although this information may be helpful, there were difficulties in collecting such information. As

web statistics become more prevalent and more appropriate metrics are used and understood, this information will become more useful in the future. Some basic information, which could be shared, was discussed in the interviews.

Maintaining a Chain of Evidence

In order to ensure that the case database maintains its reliability, everything that goes into the case database must be from reliable evidence. To help ensure reliability of the database, the third principle of maintaining a chain of evidence was employed. This “chain of evidence” helps to link the case study questions to the final case study report through the protocol, citations to sources, and the integrity of the case study database. What is desired is that the research has “been able to move from one part of the case study process to another, with clear cross-referencing to methodological procedures and the resulting evidence” (Yin, 2003:105). The ability for the research audience to trace evidence up and down the chain will strengthen the conclusions of the research.

Step 2: Prepare, Collect, and Analyze

The second stage of this research builds upon the foundations set in the first stage by preparing, collecting, and analyzing that which was laid out in the definition and design of the protocol. This phase consists of two basic actions, conduct and write the embedded analysis, and is repeated for each identified unit of analysis, as identified below in Figure 12.

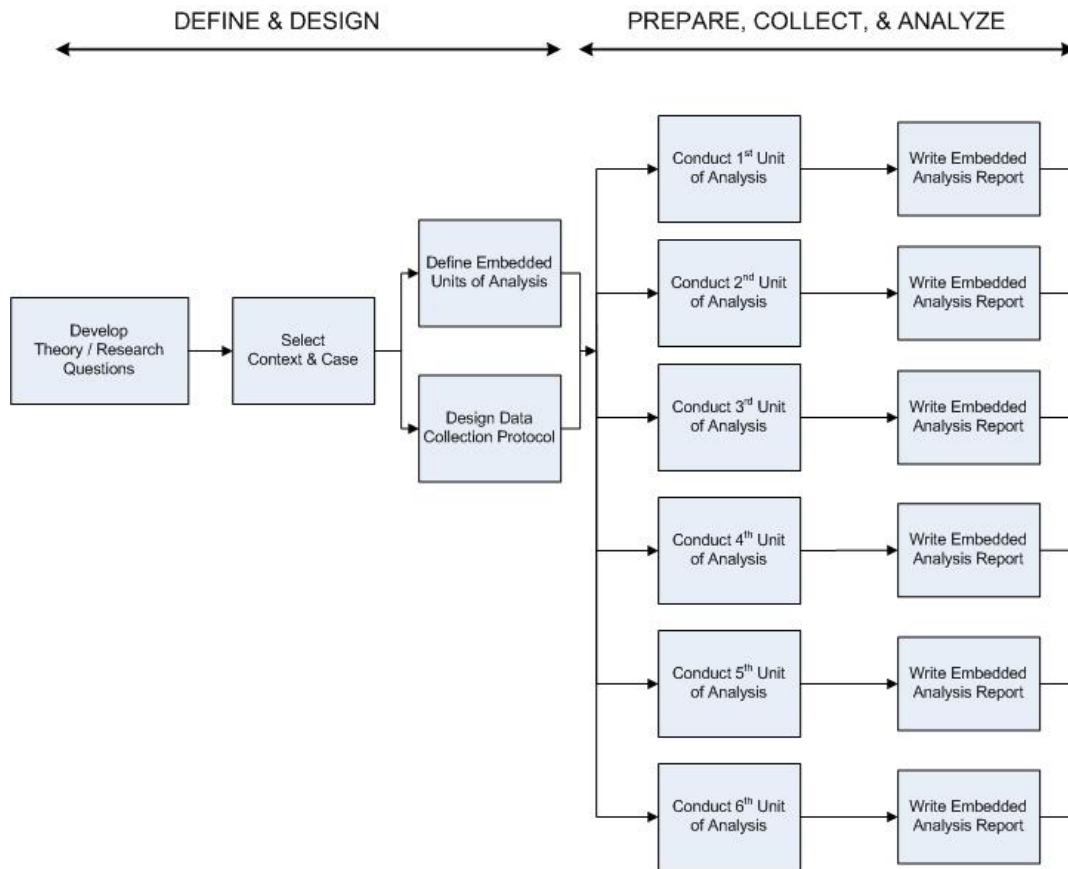


Figure 12. Single-Case Study (embedded) Method - Phase 2.(Yin, 2003:50)

Conducting Units of Analysis

Conducting each unit of analysis would draw upon the data collection protocol, which taps into all the sources of evidence that could be found. In this case, knowing that with these particular research questions and the nature of the organization the data would come primarily from conducting personal interviews with leaders in the field who had a good understanding and reputation in their areas of experience and expertise. Conducting this type of personal investigation would lean heavily on the understanding of the following five basic investigative skills: 1) question asking, 2) listening, 3) being adaptive and flexible, 4) grasp of the issues being studied, and 5) lack of bias (Yin, 2003:59).

This case study has been developed to include six embedded units of analysis within the case of the USAF GeoBase program and make up the different aspects of the GeoBase program that may be of interest of information security and information sharing. They are:

- 1) Headquarters' Air Force (HQAF)
- 2) USAF Major Commands (MAJCOMs)
- 3) Base Level GeoBase Integration Offices (GIOs)
- 4) Joint Services
- 5) Policies & Guidance
- 6) GeoBase Consumers

Methods of Analysis

Once we obtain the data for each of the individual units of analysis, a cross-functional analysis will take place. This research will employ three techniques, recommended by the GAO Case study Guidance, to take and analyze the data, in an attempt to make out what it might mean. The first technique will be to pool together all the different sources of evidence, across the entire case database, from interviews, observations, documents, and policies for an extensive or “thick” analysis. (Datta, 1990:20). The second technique will be to analyze the data through triangulation, or as Yin describes as “convergence of evidence” (Yin, 2003:100). By identifying matching patterns or themes may be useful in building explanations. The third technique employed will be

the comparison of evidence for consistency. Depending on the type of data found, a categorical matrix, charts, graphs, tables, or timelines may help to substantiate conclusions.

Writing the Embedded Analysis Report

Conducting each unit of analysis would draw upon the data collection protocol, in which the written report will be in the traditional question-answer narrative format. With as many research questions posed from the beginning, it seems logical to follow through with the same organization style. Yin notes advantages of this style as “a reader need only examine the answers to the same question or questions within each case study to begin making cross-case comparisons. Because each reader may be interested in different questions, the entire format facilitates the development of a cross-case analysis tailored to the specific interests of its readers” (Yin, 2003:148). “A series of questions can be posed, with the answers taking some reasonable length...and can contain all the relevant evidence and can be augmented with tabular presentations and citations” (Yin, 2003:148).

Step 3: Analyze and Conclude

The third and final stage of this research methodology consists of taking everything that we set out to learn in the first stage and what we discovered in the second stage and process the ideas and knowledge into something new (see Figure 13 below).

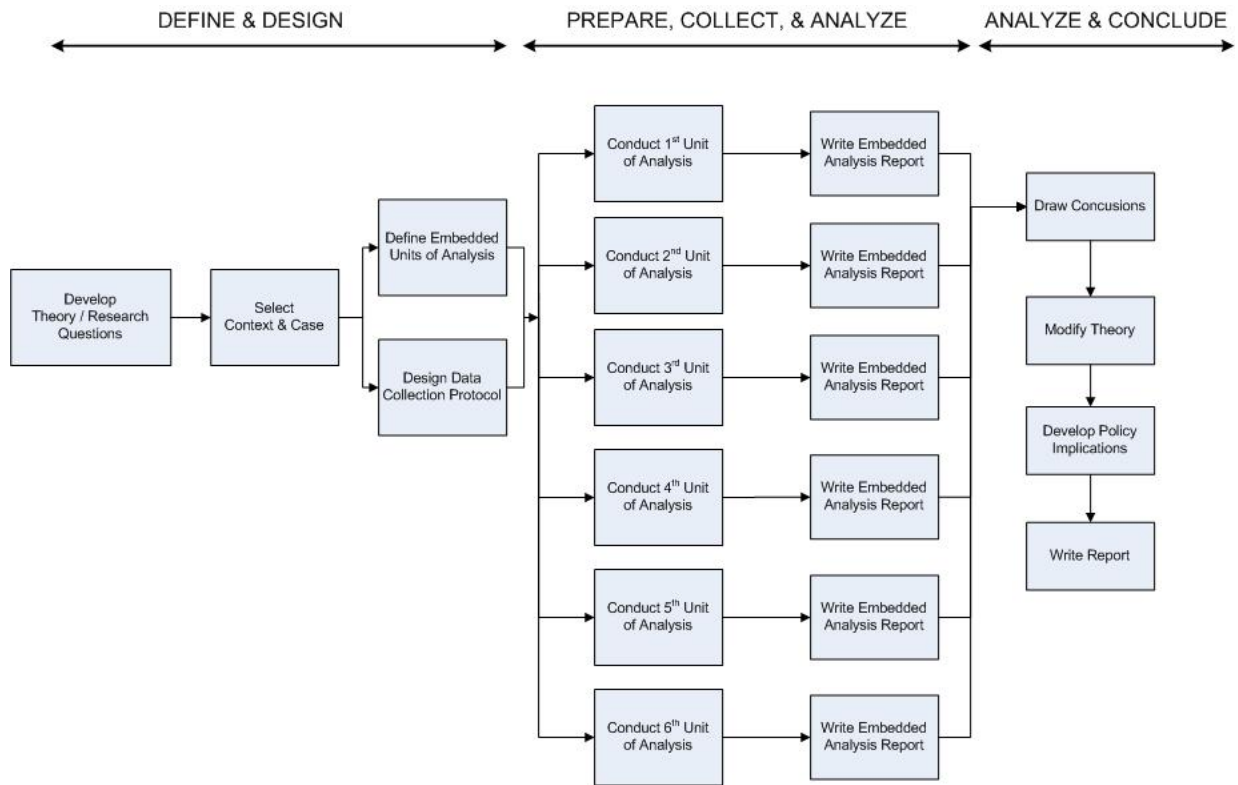


Figure 13. Single-Case Study (embedded) Method - Phase 3 (Yin, 2003:50)

This stage often is just the beginning of new questions and new theories. As conclusions are drawn and the original theory modified, these new understandings will enable us to make better-educated decisions about the subject in the future, such as new policies and guidance or focus for funding. This is why it is important to capture these conclusions, theories, and implications into a written report to communicate this new understanding to others with similar and overlapping interests and questions.

This third step will begin to manifest itself in chapter four, where the discussion will be directed at answering the primary research questions, drawing conclusions from the case database, and developing an idea of what kind of implications may be drawn from the findings. There are five general characteristics of exemplary case studies and are measures

of how this report will be gauged. These five characteristics are that the case study must 1) be significant, 2) be complete, 3) consider alternative perspectives, 4) display significant evidence, and 5) be composed in an engaging manner (Yin, 2003:160).

Potential Pitfalls

Limitations, strengths and weaknesses are inherent in all types of research. The purpose of this section is to present the boundaries of the research and so that the reader may understand where these potential pitfalls may lie. There are three main categories which will be examined; “those relating to the researcher himself, those related to the researcher’s perspective of the subject matter, and those related to the data being collected by the case study researcher” (West, 2006:155). Some researchers warn of the temptation to spend too much time on the exploratory phase of research or do not cast a wide enough net either out of convenience or because the exploration does not cover the problem adequately. In addition, it may be too early to begin exploring, thus understand the maturity level of the program or organization is essential. There have also been instances where the researcher becomes over involved and the research only seeks to confirm personal views rather than test them. Another caution is that sometimes case study evidence does not pan out the way in which it was originally thought and can potentially change the case. It is important to investigate all possible concerns prior to committing to a particular case to avoid misrepresentation (Yin, 2003:42). Table 3 summarizes the potential pitfalls of case study research.

Table 3. Summary of Potential Pitfalls

Pitfalls	Limitations, Strengths and/or Weaknesses
Researcher	• Adequate exploration / investigation • Over involvement • Personal bias • Researcher's assumptions • Competency • Expertise (Grasp of the issues being studied) • Ability to adapt to situations • Flexible • Influences • Judgment & Intuition • Investigative Skills ○ Interview/question asking ○ Listening ○ Note taking ○ Data collecting
Subject Matter Perspective	• Subject complexities • Context (What's happening around the subject) • Richness and detail • Technical skill requirements • Breadth and depth • Experience • Understanding of subject • Knowledge of patterns and causes
Data	• Reliability • Commitment (length & time) • Captures context • Interpretation • Lack of variety of data types • Number of variable and data points • Qualitative • Objectivity • Verifiability • Comparability • Quality control • Impartiality • Relationship between data collected and research question • Publication basis may severely limit generalization • Inadequate or uncertain quality of original data • Inadequate methods of relating findings • Quality of data-reduction procedures may be very difficult to determine the effects of changes in many contextual factors over time may be difficult to separate from effects of the programs • Insufficient attention to management and data reduction • Inefficiency, lateness, incomplete use of data

derived from (West, 2006:155) and (Yin, 2003)

Summary of Methodology

This chapter discussed the approach taken in the development of the research methodology, designed to provide the most appropriate way to answer the research questions. Research into different methodologies led to the case study research method due to the contemporaneous nature of the subject. Since focus on geospatial information has primarily been focused on the creation and application of the data, we are just beginning to explore the ramifications of this newly applied technology and the way we share and secure information. The exploratory case study method was the best way to learn more to positively impact the future direction of the field. This chapter also has discussed the three steps of the case study design and walked through how this research effort has been defined and designed, data preparation, collection and analysis, and sets the stage for the outcomes and conclusions that will be found in the following chapters.

IV. Analysis

The purpose of this chapter is to present the case database and bring about a better understanding to the six primary research questions set forth in chapter one. The research is comprised of an exploratory case study that involves multiple interviews, collection of policy, memorandums, and guidance documents, as well as GeoBase conference papers and presentations, as discussed in chapter three. Analysis of the case database will be presented using a question-answer narrative format. The primary research question will be presented and answers will draw on all available sources of evidence from the developed case database.

PG1 What is the nature of the security risk posed by GeoBase?

As in the literature review, the nature of the security risk posed by military geospatial information, like that which the GeoBase program office manages, is not any different from other types of geospatial information. However, the information being produced for the garrison and expeditionary installation equate to details of the Air Force's primary war-fighting weapon system. Air Force installations can be considered more like a naval aircraft carrier rather than an Army installation, for the air base is the platform from which the Air Force mission is won. Just as the details of the strengths and weaknesses of the aircraft carrier would be protected, so too should the details of the Air Force installation. With as many airmen, civil servants, contractors, and dependents that are a part of each installation, it becomes increasingly difficult and easier to forget this is a war-fighting platform, not a place of business or the neighborhood around the corner. Military

installations face different threats and have their individual vulnerabilities. Together, they create risks to the system and people operating that system.

What are the geospatial assets in need of protection?

Four primary groups make up the geospatial data assets that the information security programs seek to protect. They include, 1) the geospatial data itself, including all vector, raster, associated attribute tables, and metadata; 2) the software applications that power the GIS capabilities; 3) the installation network capabilities which provide accessibility to the information, to include the Air Force portal; and 4) the GIS products themselves, such as maps, websites, videos, and reports. (Lachman, 2006).

What are the top security concerns of GeoBase today?

To understand the nature of the GeoBase security risks, let us first identify the primary problems found in this field (see Table 4 below). Several interesting discussions emerged as the top issues, which include:

Table 4. GeoBase’s Primary Security Concerns

Primary Security Concerns	Description	Security Control Family
1. Awareness of vulnerabilities and threats (risks)	With many, the many unknowns about the vulnerabilities and threats to geospatial information drive fears that link to a managerial instinct to “turn it off” or hide it. These fears impede potentially useful information from making it into the hands of those who can make the most from it. Information users don’t realize the value and how careful we need to be with geospatial data People are not familiar with the different threats and vulnerabilities to the system and information. In many cases they are unknown Maps and information are becoming commonplace and people and INFOSEC and OPSEC	AWARENESS TRAINING & RISK ASSESSMENT
2. Classification determination of aggregated information (policy and business process)	No process in place to determine classification of data layers The more we combine data, the higher the risks. Comm has a good understanding of that as they have traditionally placed more security on their comm. data than CE has ever put on our utility data. As we compile layers of information together, what makes it classified and what does not? Where is the policy that says whether it is classified or not and who is to say what classify level that information is. To date Intel (or each stovepipe) does their stuff, but as far as the agile combat support world, they do not touch it. This is all very dynamic process as we are constantly developing new data and information, as well as adding and combining (weave or braid) this information together. Reviewing and monitoring these aggregated maps are a challenge with no standard policy or process in place.	RISK ASSESSMENT & ACCESS CONTROL
3. Access Policy	Information systems are opening up broader access to so many more people than in the past. Before you had to go and ask for copies of the base map tabs from CE, now that information is provided straight to your desktop with no questions asked. Although, this is not a bad thing, it is something to be aware of as the program continues to develop and business practices are laid through policy. Individual data stewards are on their own to determine need to know.	ACCESS CONTROL

4. Release of data to contractors / non-government entities	Contractors do not have access to the network of information that they must have to do the work required of them (design / construction). CDs of information are handed over to contractors with nothing more than a clause in the contract agreement saying that they will destroy or return all data when the job is complete. However, once the information walks out the door, there is no control over it. Often not considered are the security policies, networks, and practices of the offices of both the contractors and subcontractors hired to work on the projects.	ACCESS CONTROL
5. Improper or unauthorized access to critical infrastructure or security data.	Organizations making data publicly available without going through appropriate channels. Foreign release to foreign governments without access to our secure systems. (GCCS, COIN, etc). This is a major gray area in what and how to share with allied governments.	ACCESS CONTROL & ID AUTH & PERSONAL SECURITY SYSTEMS & SERVICES

What Security Controls are available?

In exploring what types of risk that GeoBase geospatial information poses on to this war-fighting system, three primary classes of risk were found that could be controlled (see Table 5):

Table 5. Primary Security Controls

Control Type	Description
<u>Technical</u>	“those aspects of the computer system which define security requirements for the applications and assist in detecting violations to prevent unauthorized access or misuse
<u>Managerial</u>	which focus on the management controls and element of managing risk
<u>Operational</u>	the way managerial and technical decisions are put into operation and are mostly people driven versus system driven” (Swanson et al, 2006:25).

After reviewing the literature on information security, there was a noticeable connection in what was being discussed in the interviews, which spanned the experience from the

different levels of the GeoBase organization, to that which federal information system security experts have begun to examine. It is clear that the problems and concerns of the GeoBase program is experiencing fits well into the families of security control categories as identified in the *Guide for Developing Security Plans for Federal Information Systems* (Swanson et al, 2006.) and the recently released special publication of *Recommended Security Controls for Federal Information Systems* (Ross et al, 2006) (see Table 6 below).

Table 6. Security Control Classes and Families (Swanson et al, 2006)

Class	Control Family Name	Identifier
Technical	Access Control	AC
	Audit and Accountability	AU
	Identification and Authentication	IA
	System and Communication Protection	SC
Operational	Awareness Training	AT
	Configuration Management	CM
	Contingency Planning	CP
	Incident Response	IR
	Maintenance	MA
	Media Protection	MP
	Personnel Security	PS
	Physical and Environmental Protection	PE
	System and Information Integrity	SI
Management	Certification, Accrediation, and Security Assements	CA
	Planning	PL
	Risk Assessment	RA
	Systems and Services Acquisition	SA

The identified seventeen security control families were similar to the areas of high-risk areas identified in the interviews of the case study database. Organizing the top topics found in the case study database by security control family reveals the primary areas of risk. Identifying these security control factors, researchers are able to begin to provide

guidance and develop metrics for mapping different types of information and information security categories.

What are the ways in which GeoBase offices are controlling information today?

The GeoBase offices rely on two separate systems and their ability to maintain an appropriate level of information assurance. If any piece of information is classified, then it is separated out and stored on the SIPRNet classified system. The Secret Internet Protocol Router Network (SIPRNET) is the primary network for U.S. only secret-level (SECRET-NOFORN) data. Unclassified information is controlled on the NIPRNet, “the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) provides seamless interoperability for unclassified combat support applications, as well as controlled access to the Internet” (DISA, 2006). Today, each of these systems, access is restricted primarily by the smart military identification card, known as the Common Access Card (CAC). These cards “store 64KB of data storage and memory on a single integrated circuit chip (ICC). This CAC technology allows for rapid authentication and enhanced security for all physical and logical access. Public Key Infrastructure (PKI) certificates embedded in the card enable cardholders to “sign” documents digitally, encrypt emails, and establish secure online network connections” (Department of Defense). CAC Cards can only be issued after the following physical background checks have been accomplished:

- “A SF-86 Form has been completed and submitted to the appropriate Personnel Security Representative
- A Federal Bureau of Investigation (FBI) fingerprint check has been completed and approved

- A National Agency Check with Inquiries (NACI)* background security check is in the process of being completed” (Department of Defense).

Access to the common installation pictures (CIPs), once provided directly from MAJCOM GeoBase servers, and now are made available via the Air Force Portal, where users must have an Air Force Portal account and CAC login. At the installations, beyond the CIP, further access restrictions are put on the GeoBase service depending on the data and functional owner of that data and purpose of the mapping service. For example, the integrated base defense viewer, communications viewer, anti-terrorism force protection viewer, are limited at the service level and limited to only authorized users on the network as determined by the owning organization’s data steward. For the majority of the GeoBase customers, access is granted via CAC login.

Base maps have been accessible over the Air Force Portal and base local networks (intranets) before CAC technology was available and GIOs relied on local password control systems and access from a .mil account, which allowed the GIO to limit access to the system. Access control lists are cumbersome and difficult to maintain. Someone is required to maintain an access database, which then ties to ArcIMS, that contains a list of separate login names and passwords. This database resides on a server with its own inherent vulnerabilities. As users come and go or Ops tempo increases, this list is difficult to maintain and is not as secure as it could be. Other ways of restricting access, though not necessarily a security measure, was to assign an obscure URL address that helps in decreasing traffic to the site. Over the last few years, the need for control has grown. Since much of the initial data that was being collected were internal to the civil engineering

organization, it was much easier to control and know who needed what and why. As the need and collection of data has expanded beyond the civil engineering center of gravity, there is an increased need for new controls measures.

As policies and technology have enabled the standard CAC identification tools, PKI certificates, and combined with the advantages of the portal's active directory controls for network logins and passwords, the GeoBase leaders are better assured their information is making into trusted hands. GeoBase is becoming more integrated into the Portal and using the Portal access manager, which allow for the same tools that Portal is using now to govern who gets access to what and trickles down to the layer and attribute levels. This allows GeoBase administrators to begin to more efficiently customize access to any part of the information. Now, instead of giving someone access to the entire geodatabase, administrators can fine-tune access, providing only the knowledge required. For example, it could allow someone who is getting ready to dig in an area the ability to see that there is a utility line in the way, but would not disclose the attribute details of the utility line, such as if it is a T1 or T5 communications line, classified, unclassified, or what facilities it services.

By CAC authentication and setting up a user group policies defined by data stewards, or subject matter experts (SMEs), and controlled by active directory group policies using the CAC certificate. Each SME tells the GIO who needs to be included in those groups. Most commands make available what information is available, but do not provide access unless the data steward, responsible for that data grants the GIO permission to provide access. Data not available provides contact information on how and who

authorization is needed. Each individual data steward determines the requestor's need to know, then advises the GIO on who to allocate permissions and for how long. Based on the web solution, it is possible to lock down individual features and/or attribute layers.

MAJCOMs are testing a more robust "Secure Map" application (beta test being worked), to be used to help restrict access on the portal by CAC logon down to the layer and attribute level. For example, if you are in security forces and have a security forces role (need to know), then when you log on with your CAC card, you will be able to see all data and attributes defined as of interest to security forces, perhaps it is security camera locations, access routes, entry control points, or other type of information in the security forces mission data set (MDS). However, if you are not part of that role, then you can only see the CIP and will not have access the other information. In this case, the owner of the information must assign roles and define access limitations. These limitations are set using either individual ids or associated group settings, just like email groups such as "SRC members" or "Command Post Personnel".

CAC controls such as these help add layers of security onto the installation's basic three-tiered firewall system that are set up to limit users to: 1) base only personnel, 2) MAJCOM domain only, or 3) .mil only. Users with .mil access cover the widest range of access to GeoBase information, the CIP.

Security controls for the web-based side of providing information are completely different from the non-web based networks for the more savvy GIS user. These users tend to work directly off the hard drive space, memory stick, CD/DVD, and with paper copies.

How they manage security is different from how security is managed for the web-based networks.

The nature of the security risks associated with GeoBase is multifaceted and complex, just like risks other information systems face. Geospatial information is to the installation as your personal finance information is to you. Just as someone can do damage with the information of your bank account, they too can do damage knowing critical information about the base. It is important to safeguard the information, but as in business, if you want to get paid account information must be shared. Sure, there is an element of trust, but we understand the risks and the safeguards in place for our finances. We must come to understand the technical, operational, and managerial security aspects of the geospatial information with which we work.

PG2 What information is sensitive that poses a risk to security?

This question is one that continues to plague the experts. The sensitivity of information depends directly with the capabilities that a piece of knowledge of information opens up to someone with access. Things have become so much more common and available to the public through multiple media outlets, especially the in the use of the internet. So much of our environment that was once limited knowledge, like information about our installations, now have expanded beyond a limited community network and into public domain where anyone can access this information. This is why it has become increasingly more important for us to identify and control information early on that needs to remain in a protected environment. “Identifying data sensitivity is critical for determining the security controls that should be used to protect the connected systems and

the data” (Grance, Hash, Peck, Smith, and Korow-Diks, 2002:3-3). As the GeoBase community continues to collect and consolidate information, they do so under the same guidelines that they have been familiar to them in the past. Under this question, it is also important to explore how geospatial information is currently being classified, who defines the classification of this information, what type of information are considered sensitive, and how security information is being tracked in the GIS system.

How is geospatial information classified?

Currently, information is categorized into two main levels of classification, based on the individual merits of the information as either *Classified* or *Unclassified*. However, information that is unclassified is routed into one of three subcategories: 1) Sensitive, but Unclassified, 2) Unclassified, For Official Use Only (FOUO), or 3) Unclassified, Public Information (FOIA). “The fact that this guide indicates that some information may be unclassified does not imply that that information is automatically releasable to the public. Unclassified information...intended for public release must be reviewed for sensitivity and processed through appropriate channels for approval in accordance with DoD Instruction 5230.9, “*Clearance of DoD Information for Public Release*””(Stenbit, 2003).

“Classification is reserved for specific categories of information or the compilation of related information as defined in Executive Order 12958” (Stenbit, 2003). GeoBase is quickly falling into this gray area of classification by compilation and to date has not been determined as classified, as most compilations are not. “However, in certain circumstances, information that would otherwise be marked UNCLASSIFIED may become classified when combined or associated with other UNCLASSIFIED information, if the

compiled information reveals an additional association or relationship. See DoD Regulation 5200.1-R. Under such circumstances, it is the combination or compilation of information that is classified, not the individual items of information. Users of this SCG must be aware of such a possibility when compiling UNCLASSIFIED information. Likewise, the compilation of classified information must be classified, at a minimum, at the highest classification within the aggregated data, but may become a higher classification if the compiled information reveals an additional association or relationship” (Stenbit, 2003). The graph below (Figure 14) estimates how geospatial information in the GeoBase program is distributed into these classification categories.

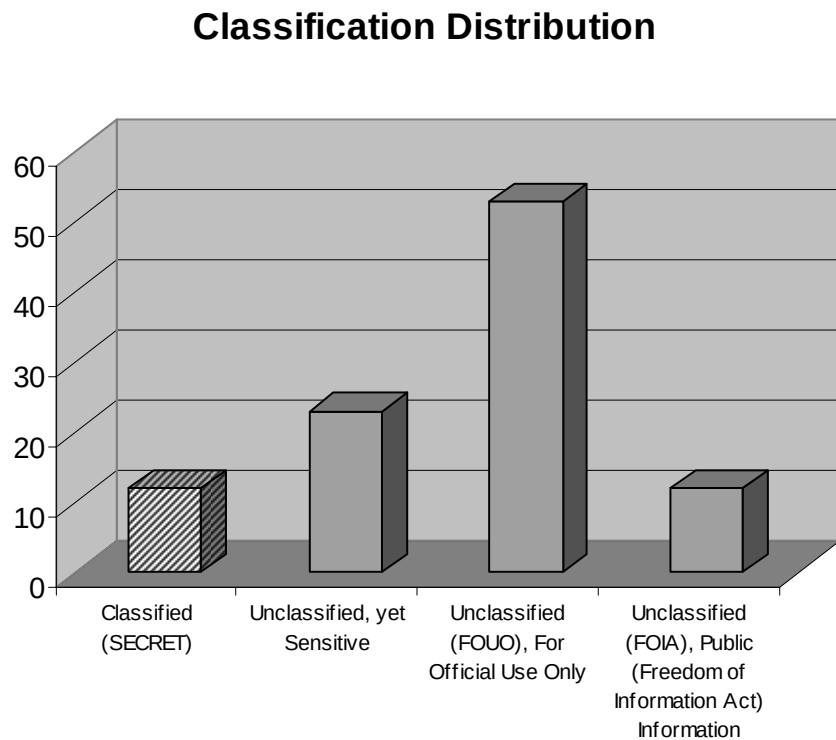


Figure 14. Classification Distribution in GeoBase

It is important to note that although the level of work being classified as SECRET, the majority of the information is not imagery or data related, but rather troop locations and vulnerabilities tied to a specific operation or wartime plan in base support plans. There are extensive rules, policies, and training on who, what, why, and how long information becomes classified at the SECRET level. Title 32 of the Code of Federal Regulations, part 2001 provides explicit reasons why information should be classified. This Executive order “prescribes a uniform system for classifying, safeguarding, and declassifying national security information. It also establishes a monitoring system to enhance its effectiveness. This Directive sets forth guidance to agencies on original and derivative classification, downgrading, declassification, and safeguarding of classified national security information” (Information Security Oversight Office, 2003). Information falling into any of the categories below should be considered for a classification decision:

- “military plans, weapons systems, or operations
- foreign government information
- intelligence activities (including special activities), intelligence sources or methods, or cryptology
- foreign relations or foreign activities of the United States, including confidential sources
- scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism
- United States Government programs for safeguarding nuclear materials or facilities
- vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism
- weapons of mass destruction” (Information Security Oversight Office, 2003).

However, little has been done to examine and evaluate information that does not necessarily meet the criteria for the TOP SECRET, SECRET, or CONFIDENTIAL classified data, but is still sensitive. Wading into the “Sensitive, but Unclassified” waters, one finds themselves over their head in muddy water. This is one of the biggest challenge areas the GeoBase program faces in the security of its operations. Especially as the Air Force continues to become more efficient in organizing their database systems. The power of organizing information together into one system has changed how the Air Force must gauge the sensitivity of information as well as how we must work to protect this new type of aggregated information, which we need to remain widely accessible to those needing the information. In following questions analysis is provided at some of the impacts and costs found in restricting access by classifying information.

Three primary major commands produce GeoReach information, which is expeditionary geospatial information (GeoBase-like) for forward operating locations which aim to deliver the “one map” for the contingency environment. The remaining commands depend on this GeoReach information as a customer. Even though so many aspects about what are associated with deployable locations are classified, the information these GeoReach maps are derived from are not necessarily classified. For example, if we had a GeoReach location in Mongolia, it is not necessarily about the data itself, but what the data implies. You can get the same information off Google Earth or other sources. For this reason, two of the three commands have posted their GeoReach data on the AF Portal, giving the same level of attention and detail to each, thus no way to jump to a conclusion that one is more strategically important. The other command has taken the approach that in

their command, the implications are too great and do not want conclusions to be made.

Part of the intent of GeoReach is to supply educated troops to the theater. Providing troops access to the information on the locations they are serving, there are only minute differences in whether they find it on the SIPRnet, Air Force Portal, or Google Earth.

There are still GeoReach and GeoBase information that will be used to tie classified information to a location, making it geospatial classified information and required to operate on the SIPRnet service to those with the appropriate SECRET level clearances.

Who defines the classification of geospatial information?

The data owner/steward of the information currently makes this determination with the help of the GeoBase administrator. The majority of the GeoBase offices do not deal with classified information, if they do, then they are not aware of it or it is yet to be determined. Individually, these mission data layers are classified at the FOUO level. Right now GeoBase offices are publishing a lot of geospatial information, if something looks like it should be sensitive, then the data owner is consulted and layer by layer, solutions are put into place.

The current security practices are an amalgamation of historical documents and business practices, agreements, policies, processes, and new requests by data stewards and the data layer owners. Although the GeoBase administrators and data stewards do their best, they cannot do it in isolation. The Air Force is notorious for allowing decisions to be made at the base level for the best interest of unique situations at each installation. However, with decisions on information classification, continuity amongst how information is to be classified is important across commands and across the service. The

GeoBase office and data stewards are not the only perspectives that this decision should be based. Other fields of expertise such as the Opsec, Infosec, and Commsec communities have valuable expertises that are not currently involved in the process. These determinations must be made and are the most difficult aspect of applying the technological controls. Someone has to make the call on who should be allowed to see what.

What types of information is considered sensitive?

As data is collected using the global positioning system (GPS) are tied to points, lines, and areas to particular places (latitudes and longitudes), within an accuracy of often less than 1m, in many minds this information can be considered sensitive. Examples of geospatial type information that may be considered sensitive and in certain cases, classified:

- QD Arcs (Explosive Safety zones)
- Crash Grids
- AICUZ Contours
- Archeological Locations
- Critical Infrastructures (Barker, Jun 2004.)
 - Agriculture and Food (Including farms and food processing plants)
 - Water (Including federal reservoirs and municipal waste water facilities)
 - Public Health (Including hospitals and federal health organizations)
 - Emergency Services (Including federal, state, and local response units)
 - Defense Installations and Defense Industrial Base
 - Telecommunications (Including switching and transmission/cable facilities)
 - Energy (Including electric, oil, and gas production , transmission facilities)
 - Transportation (Aviation, rail, highway, pipelines, maritime, mass transit)
 - Banking/Finance (Including federal services and FDIC insured institutions)
 - Chemical Industry/Hazardous Materials (e.g., chemical plants)
 - Postal and Shipping Facilities
- Key Assets (Barker, Jun 2004.)
 - Nuclear Power Plants
 - National Monuments and Icons
 - Dams
 - Government Facilities
 - Commercial Assets

- Troop locations
- Troop movements
- Asset allocations

The problem is that in many cases, the data is so readily available, whether the Air Force has created it or some commercial source creates it. If someone wants coordinates or any good level of accuracy, they could go to Space Imaging or other commercial site and find what they are looking for. What makes this palatable are that it is more difficult to find out which facilities are what, such as command posts, munitions storage, supply warehouses, etc. However, this type of information is slowly creeping from the private domain to the more public domain. The interviews expressed there have been incidents where investigators have had to take maps out of peoples' hands that they have made or had unauthorized access to. Examples in a deployed environment have included escorts finding and confiscating detailed maps from third country nationals (TCNs). Whether they have acquired it from the trash, find it on base, or have one that they have diagramed out on their own, pacing off specific details of the installation. It is much easier to point to the hard copy evidence such as maps found in possession of those without a good need to know, but as far as the electronic versions of maps and the network, it is much more difficult to evaluate the magnitude of security incidents.

How is security information tracked in GIS?

All geospatial information has two types of information that is stored and managed in a relational database management system (RDBMS). The first is information dataset; this is the primary attribute data table that stores information about each entity. The second

set of data it stores is data about the data, known as the metadata set. Both datasets store information about the security classification system and the security classification. In some instances, there may be a need to identify the primary data as “Unclassified” or “FOUO” but the metadata may contain information about how the data was collected and is classified as “Sensitive”. Table 7 is an example of the metadata security information from the Spatial Data Standards for Facilities, Infrastructure, and Environment (SDSFIE).

Table 7. Tabular Metadata Security Information Template (Headquarters Air Force Geo Integration Office, April 2006:20)

7.10 Metadata Security Information			
7.10.1	Metadata Security Classification System	The name of the classification system for the metadata	<i>Valid Value:</i>
7.10.2	Metadata Security Classification	The name of the handling restrictions on the metadata.	<i>Valid Values:</i> “FOUO” “Unclassified” “Sensitive”

The Air Force’s standards for the RDBMS data model is defined by the SDSFIE industry standard which “are developed and maintained by the CADD/GIS Technology Center for Facilities, Infrastructure, and Environment located in the U.S. Army Engineer Research and Development Center’s Topographic Engineering Office (ERDC TEC) in Alexandria, VA. The SDSFIE are developed in a collaborative fashion with input from DoD Services and other Federal organizations” (Headquarters Air Force Geo Integration Office, 2006).

PG3 What impacts might information security concerns affect information sharing.

Information sharing remains at the heart of the GeoBase any disruptions or barriers that affect information sharing will be of impact. Part of this case study was to ascertain if concerns over information security affects how people share or may not share information. In order to address this question appropriately, let us first assess if the GeoBase community has any problems with information sharing. If so, what are they and how is the sense of security tied to information sharing? Finally, evaluate how these concerns, or perceived barriers, affect information sharing.

What are the reasons for not sharing?

The research interviews indicated that each organization faced their share of challenges in establishing relationships that allowed for open exchange of information both within and between organizations. When asked of the problems they encountered, fear and the lack of understanding contributed the most to the hesitation to share information. Table 8 indicates the perceived problems for not wanting to share information.

Table 8. Reasons for not wanting to share information

Areas of Concern	Description
Ignorance	• Lack of understanding typically drives the fear, power, and control issues. • There are a lot of senior level decision makers and information controllers who are not familiar with the new information culture, the capabilities, and potential for both the positive and negative benefits that can come from sharing information.
Fear	• Natural tendencies are to keep a close hold of your data. Many users are afraid of the data / data quality and if they were to expose it they would lose control of the data. • People often fear that their data may not be correct and do not want others to see that their data is not right. • Fear of liability • Similarly, users fear that people won't understand the intricacies of their information and develop the wrong conclusions • Fear of losing either control of their information or the power they feel the information provides them.
Power	• The old adage knowledge is power still rings true. Some people consider the data theirs and without it their job or purpose within the organization will become lessened if they share it.
Control	• At the base level, some data stewards do not want to share data with those beyond their immediate organizations, often to maintain decision control over their turf.
Imposed Restrictions	• Particularly with sharing regional information picture (RIP) data and imagery, in the local counties whom have shared information and imagery through a memorandum of agreement. Often it comes down to licensing and agreements. We must recognize those agreements locally as well, thus motivated not to share information.
Compatibility Issues	• As connections are made, relatively simple hurdles often stand in the way of the willingness to share and tend to become excuses for not wanting to put the effort and energy into what may look to be more work.

Figure 15 illustrates as concerns grow, the willingness to share information drops or that people are more likely to share information when there are few concerns. The areas of concern are divided out as they were discussed or presented, notice how each are intertwined.

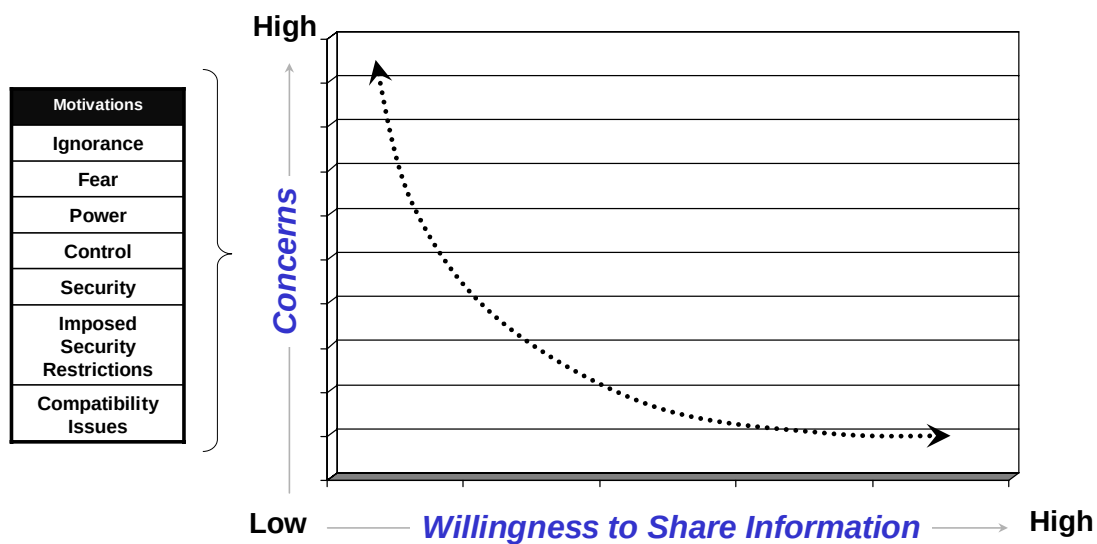


Figure 15. Impact of Security Concerns on Information Sharing

As these areas of concern are assessed, one has to consider how fears are fueled or calmed by the feeling of security. The blanket of security helps users feel secure enough to release fears or losing control, power, or that something is going to happen to the data. To overcome these fears and feel more secure about decisions about information, education has been the only way to combat this problem.

A post 9/11 GAO report to the Secretary of Homeland Security in August of 2003 on efforts to improve information sharing studied ten barriers that were perceived as a

hindrance to the information sharing process. Figure 16 highlights the ten barriers studied in the GAO survey and consolidates the average response of 16 federal agencies, 40 state agencies, 106 large cities, and 122 small cities to give an average percentage of perceived factors that hinder information sharing (Decker and Lepore, 2003).

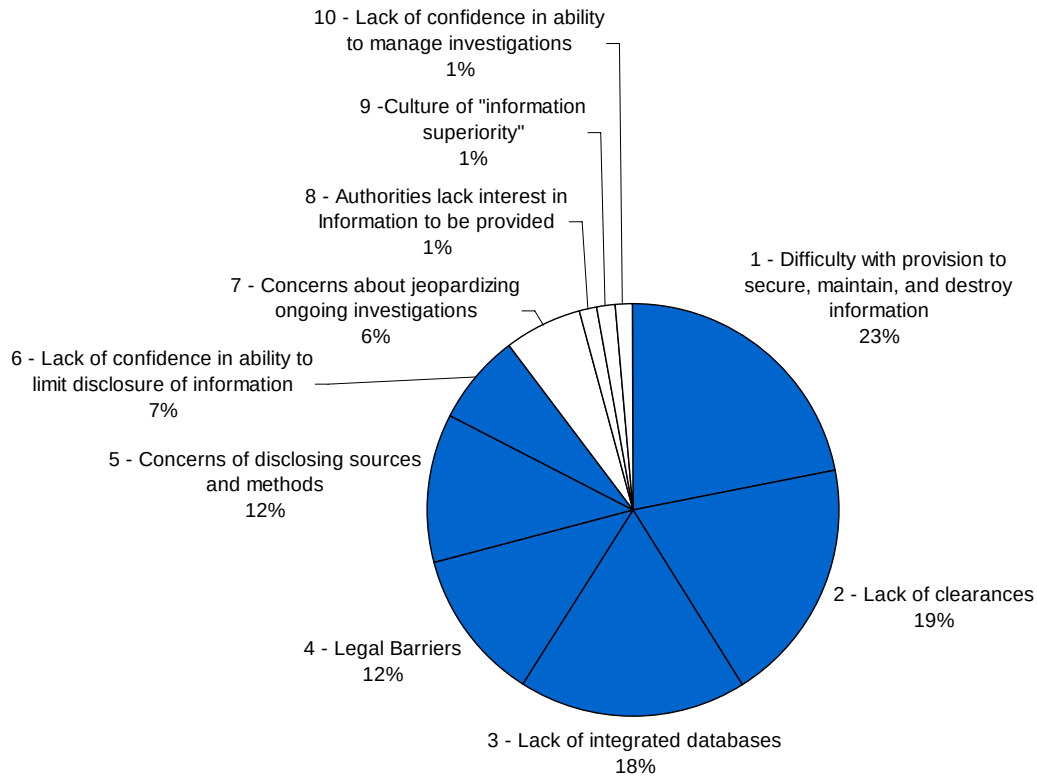


Figure 16. Perceived Barriers Preventing Federal Agencies from Sharing Information. derived from (Decker and Lepore, 2003)

Although the GAO report identified the lack of integrated database capability as the only significant barrier, it is interesting to note in Table 9, that the top six out of the ten barriers studied all have to do with the security of information.

Table 9. Top Ten Perceived Barriers to Sharing Information (Decker and Lepore, 2003)

- 1 Difficulty with provision to secure, maintain, and destroy information*
- 2 Lack of clearances*
- 3 Lack of integrated databases*
- 4 Legal Barriers*
- 5 Concerns of disclosing sources and methods*
- 6 Lack of confidence in ability to limit disclosure of information*
- 7 Concerns about jeopardizing ongoing investigations
- 8 Authorities lack interest in Information to be provided
- 9 Culture of "information superiority"
- 10 Lack of confidence in ability to manage investigations*

* *(Directly related to information assurance / information security values)*

These emphasize the problems with inconsistencies and different expectations of information sharing and information security between organizations. Overcoming barriers such as these will continue to test programs such as the USAF GeoBase program, which encounters similar challenges when working with internal organizations, joint services, local municipalities, civilian employees, and private contractors. Each of these groups is representative of the mission and need pieces of the information the others have to share. Determining ways to know who it is appropriate to share information with, defining their “need to know” and how the information will be used are among the difficulties in establishing consistent procedures.

How is GeoBase overcoming sharing barriers?

The GeoBase program has come a long way very quickly however, we are missing a lot in the education details. The expectation is that information sharing is also in a life cycle and willingness will continue to grow as the young company grade officers (CGOs) and non-commissioned officers (NCOs) grow up with a better understanding in this type of

open culture. For now, the GeoBase program is in a life cycle stage where there are many senior leaders and data stewards that do not understand the capabilities of the technology and potential for both the good and bad.

There are those who do not want information shared in the name of security. The MAJCOM GIOs are finding that their fears are being curbed the more they know about the needs to share information and the processes in place to control potential misuse. It is an education process. Often, the unknowns about security become the scapegoat for not accepting change. Security cannot be an excuse for not wanting to change. If there is a map sharing process were leaking and in need of repair, you do not let it continue to leak the same way it has always been without doing anything about it. Change is needed. Just because a new technology is introduced does not mean the broken underlying business process is fixed. In this case, GIS helped to highlight the problem and focus attention to the process that needs fixing. For years, maps and information have been walking off the installations or can be found publicly on the internet without any kind of control mechanisms in place. Although the perfect solution has not been found, it is better than what it was. There are inherent problems in the system and to be concerned to the point of wanting to stop the flow of information now is odd.

Although the Air Force GeoBase policy is to “facilitate sharing GeoBase knowledge, to the maximum extent allowable, both across and beyond the installation with other federal, state, or municipal agencies” (Zettler, 2002), the policy is very encompassing and is difficult to address specific instances. When the inevitable questions arise at the operational level concerning the release of information and the answer is not necessarily

clear, the current procedures are to raise the question up the chain of command.

Installation commanders have been given the “responsibility to establish protocols for handling their respective installations’ geospatial information to best satisfy their assigned missions” (Zettler, 2002). On occasion, data stewards and requestors reach an impasse and MAJCOM GIOs have become good at stepping in to help mediate the solution. They have typically found that problems can be resolved by expressing why data cannot be shared or what needs to be done in order to share the information. Usually, a compromise is reached with the data owner and still meets the need of the requestor by stripping out data attributes or specific information. Other times, the MAJCOMs will back the data owner and deny the request.

GeoBase administrators understand other’s concerns for not wanting to share information. Just like the GeoBase administrator, they have their concerns about whom they give their information to and what they are going to do with it. There is a lot more that can be learned on data sharing from civilian businesses and universities. Pinpointing these barriers in the military, and how they might be overcome, may be a good topic for future study.

PG4 What are the key information system security constructs and their interrelationships?

Information security is so intertwined with the processes, actions, and influences of so many things contributing to this nebulous concept of “security”. Rather than finding different aspects of information security specifically associated with geospatial information, the interviews, literature review, and policy documents all point back to the

standard characterizations of information security and the preservation of three particular constructs: “1) *confidentiality*, ensuring that information is accessible only to those authorized to have access; 2) *integrity*: safeguarding the accuracy and completeness of information and processing methods; and 3) *availability*: ensuring that authorized users have access to information and associated assets when required” (ISO/IEC 17799, 2000). Many, if not all, the guides and policies for the federal government use these characterizations as their primary security objectives and are used to extrapolate risk (potential impact). Table 10 shows the federal information processing standards (FIPS) and how federal information systems, such as GeoBase, can begin to categorize these security concepts into discrete impact categories into functions of low, moderate, and high risk.

**Table 10. Potential Impact Definitions of Security Objectives for Categorization
(Barker, 2004; Evans, Bond, and Bement, 2004; Swanson et al, 2006)**

	POTENTIAL IMPACT		
<i>Security Objective</i>	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

These general constructs help to broadly draw direction for Information Security (INFOSEC) and Operational Security (OPSEC) policies and procedures. However, Table 11 is a compilation different security constructs from multiple courses. As the GeoBase program continues to reach out and interconnect with other information technology systems, more security factors must be considered. By no means is this table complete, nor is it meant to be conclusive of all the important constructs. Instead, it is meant to pull together different thoughts from a variety of different fields and areas of expertise that

relate to the general security of information. All too often, organizations focus on only one or two aspects of security. As this table shows, multiple aspects must be incorporated into maintaining security. This table is broken into the primary security requirements of technical, operational, and management controls as discussed in Table 4.

Table 11. Security Constructs

TECHNICAL CONTROLS	
• Access Controls	Access Control Policy; <u>User Access Management</u>: user registration, password management; privilege management; review of user access rights; password use; unattended user equipment <u>Network Access Control</u>: policy on use of network services; enforced path; user authentication for external connections; node authentication; remote diagnostic port protection; segregation in networks; network connection protocols; network routing control; security of network services <u>Operating System Access Control</u>: automatic terminal identification; terminal log-on procedures; user identification and authorization; password management system; use of system utilities; duress alarm to safeguard users; terminal time-out; limitation of connection time. <u>Application Access Control</u>: information access restrictions; sensitive system isolation <u>Monitoring System Access and Use</u>: event logging; monitoring system use; clock synchronization <u>Mobile computing and teleworking access controls</u>: Whether a formal policy is in place, and appropriate security measures are adopted to protect against the risk of using mobile computing and communication facilities. (Thiagarajan, 2003; Thiagarajan, 2005)
• Audit and Accountability Trails	
• Hardware and Systems Software Requirements	“Identify hardware that will be needed to support the interconnection, including communications lines, routers, firewalls, hubs, switch, servers, and computer workstations. Determine whether existing hardware is sufficient, or whether additional components are required, especially if future growth is anticipated. If new hardware is required, select products that ensure interoperability” (Grance et al, 2002)

	“Identify software that will be needed to support the interconnection, including software for firewalls, servers, and computer workstations. Determine whether existing software is sufficient, or whether additional software is required. If new software is required, select products that ensure interoperability.” (Grance et al, 2002)
• Identification and Authentication	
• Security Controls	“Identify security controls that will be implemented to protect the confidentiality, integrity, and availability of the connected systems and the data that will pass between them. Controls can be selected from the examples provided in Section 4 or from other sources. Controls should be appropriate for the systems that will be connected and the environment in which the interconnection will operate” (Grance et al, 2002)
• System and Communication Protection	
OPERATIONAL CONTROLS	
• Awareness, Training, and Education	“Define a security training and awareness program for all authorized personnel who will be involved in managing, using, and/or operating the interconnection. The program may be incorporated into current security training and awareness activities. Identify training requirements, including frequency and scheduling, and assign responsibility for conducting training and awareness activities. Design training to ensure that personnel are familiar with IT security policy, procedures, and the rules of behavior associated with the interconnection. Require users to sign an acknowledgement form indicating that they understand their security responsibilities, if appropriate. If shared applications are used, ensure users know how to use them properly. If the interconnection is used to exchange or transfer sensitive data, ensure that users understand special requirements for handling such data, if required. See NIST Special Publication 800-50, <i>Building an Information Technology Security Awareness and Training Program</i>, for guidance” (Grance et al, 2002)
• Availability	“Ensuring timely and reliable access to and use of information...” [44 U.S.C., SEC. 3542]. A loss of <i>availability</i> is the disruption of access to or use of information or an information system” (Evans et al, 2004).
• Compliance	Identification and compliance with applicable legal requirements; intellectual property rights (IPR); safeguarding of organizational records; data protection and privacy of personal information; prevention of misuse of information processing facility; regulation of cryptographic controls; collection of evidence; review of security policies and technical compliance. (Thiagarajan, 2003)
• Confidentiality	““Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information...” [44 U.S.C., Sec. 3542]. A loss of <i>confidentiality</i> is the unauthorized disclosure of information.” (Evans et al, 2004).

• Configuration Management	
• Contingency Planning	“Each organization should have a contingency plan(s) to respond to and recover from disasters and other disruptive contingencies that could affect its IT system, ranging from the failure of system components to the loss of computing facilities. Determine how to notify each other of such contingencies, the extent to which the organizations will assist each other, and the terms under which assistance will be provided. Identify emergency points of contact (POC). Determine whether to incorporate redundancy into components supporting the interconnection, including redundant interconnection points, and how to retrieve data backups. Coordinate disaster response training, testing, and exercises. See NIST Special Publication 800-34, <i>Contingency Planning Guide for Information Technology Systems</i>, for more information” (Grance et al, 2002)
• Data Element Naming and Ownership	“Determine whether the data element naming schemes used by both organizations are compatible, or whether new databases must be normalized so the organizations can use data passed over the interconnection. In addition, determine whether ownership of data is transferred from the transmitting party to the receiving party, or whether the transmitting party retains ownership and the receiver becomes the custodian. As part of this effort, determine how transferred data will be stored, whether data may be re-used, and how data will be destroyed. In addition, determine how to identify and resolve potential data element naming conflicts” (Grance et al, 2002)
• Integrity / Accuracy (System and Information Integrity)	“Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity...” [44 U.S.C., Sec. 3542]. A loss of <i>integrity</i> is the unauthorized modification or destruction of information” (Evans et al, 2004)
• Data Sensitivity, Asset Classification and Control	“Identify the sensitivity level of data or information resources that will be made available, exchanged, or passed one-way only across the interconnection. Identifying data sensitivity is critical for determining the security controls that should be used to protect the connected systems and data. Examples of sensitive data include financial data, personal information, and proprietary business data. See NIST Special Publication 800-18, <i>Guide for Developing Security Plans for Information Technology Systems</i>, for further guidance.”
• Documentation	
• Hardware and Systems Software Maintenance	
• Incident Reporting and Response Capability	“Establish procedures to report and respond to anomalous and suspicious activity that is detected by either technology or staff. Determine when and how to notify each other about security incidents that could affect the interconnection. Identify the types of information that will be reported, including the cause of the incident, affected data or programs, and actual or potential impact. In addition, identify types of incidents that require a coordinated response, and determine how to coordinate response activities. It might be appropriate to develop a joint incident response plan for this purpose. For more information, see NIST Special Publication 800-3, <i>Establishing a Computer Security Incidence Response</i>

	<i>Capability (CSIRC), and Federal Computer Incident Response Center (FedCIRC) publications” (Grance et al, 2002)</i>
• Level and Method of Interconnection	“Define the level of interconnectivity that will be established between the IT systems, ranging from limited connectivity (limited data exchange) to enterprise-level connectivity (active sharing of data and applications). In addition, describe the method used to connect the systems (dedicated line or VPN).”
• Maintenance	
• Media Protection / Data Backup	“Determine whether data or information that is passed across the interconnection must be backed up and stored. If backups are required, identify the types of data that will be backed up, how frequently backups will be conducted (daily, weekly, or monthly), and whether backups will be performed by one or both parties. Also, determine how to perform backups, and how to link backups to contingency plan procedures. Critical data should be backed up regularly, stored in a secure off-site location to prevent loss or damage, and retained for a period approved by both parties. Similarly, audit logs should be copied, stored in a secure location, and retained for a period approved by both parties” (Grance et al, 2002)
• Personnel Security	Security in job definition, resourcing, and responsibilities; personnel screening policy; confidentiality agreements; terms and conditions of employment; user training; reporting, responding and learning of incidents, weaknesses, and malfunctions; disciplinary process (Thiagarajan, 2003)
• Physical and Environmental Security	Physical security, such as the separate network, locks, safes, secure rooms, etc. that support that system; maintaining a physical security perimeter, physical entry controls, securing offices, rooms and facilities, secure working environment, isolated delivery and loading areas. Equipment Security: equipment siting protection, power supplies, cabling security, equipment maintenance, securing of equipment off-premises (TDY, etc), secure disposal or re-use of equipment General: clearing desk and clear screen policies, removal of property (Thiagarajan, 2003)
• Production, Input/Output Controls	
• Rules of Behavior	“Develop rules of behavior that clearly delineate the responsibilities and expected behavior of all personnel who will be authorized to access the interconnection. The rules should be in writing, and they should state the consequences of inconsistent behavior or noncompliance. The rules should be covered in a security training and awareness program” (Grance et al, 2002)
• Services and Applications	“Identify the information services that will be provided over the interconnection by each organization and the applications associated with those services, if appropriate. Examples of services include e-mail, file transfer protocol (FTP), RADIUS, Kerberos, database query, file query,

	and general computational services” (Grance et al, 2002)
• Systems Development and Maintenance	The analysis and specification of security requirements
• Impact on Existing Infrastructure and Operations	“Determine whether the network or computer infrastructure currently used by both organizations is sufficient to support the interconnection, or whether additional components are required (e.g., communication lines, routers, switches, servers, and software). If additional components are required, determine the potential impact that installing and using them might have on the existing infrastructure, if any. In addition, determine the potential impact the interconnection could have on current operations, including increases in data traffic; new training requirements; and new demands on system administration, security, and maintenance” (Grance et al, 2002)
• User Community	“the community of users who will access, exchange, or receive data across the interconnection. Determine whether users must possess certain characteristics corresponding to data sensitivity levels, such as employment status or nationality requirements, and whether background checks and security clearances are required. ³ Devise an approach for compiling and managing the profiles of all users who will have access to the interconnection, including user identification, workstation addresses, workstation type, operating system, and any other relevant information. Each organization should use this information to develop and maintain a comprehensive database of its users” (Grance et al, 2002)
MANAGEMENT CONTROLS	
• Business Continuity Management	“Examining the business continuity processes, analysis of impacts; writing and implementing a continuity plan and framework; testing, maintaining and re-assessing the plan” (Thiagarajan, 2003)
• Certification, Accreditation, and Security Assessments	
• Change Management	“Determine how to coordinate the planning, design, and implementation of changes that could affect the connected systems or data, such as upgrading hardware or software, or adding services. Establish a forum with appropriate staff from each organization to review proposed changes to the interconnection, as appropriate. Coordinating change management activities will reduce the potential for implementing changes that could disrupt the availability or integrity of data, or introduce vulnerabilities” (Grance et al, 2002)
• Classification & Declassification Management	
• Communications and Operations Management	
• Costs and Budgeting	“Identify the expected costs required to plan, establish, and maintain the interconnection. Identify all associated costs, including labor, hardware, software, communications lines, applications, facilities, physical security, training, and testing. Also, identify costs for certifying and accrediting the interconnection after it is established, if appropriate. Develop a

	comprehensive budget, and determine how costs will be apportioned between the parties, if required” (Grance et al, 2002)
• Life Cycle	
• Planning	
• Review of Security Controls and Policies	
• Risk Assessment	
• Risk Management	
• Roles and Responsibilities	“Identify personnel who will be responsible for establishing, maintaining, or managing the interconnection, including managers, system administrators, application designers, auditors, security staff, and specialists from such fields as insurance and risk management. Choose personnel who have appropriate subject matter expertise. If contractors are involved, one or both organizations may be required to develop a nondisclosure agreement to safeguard the confidentiality and integrity of exchanged data” (Grance et al, 2002)
• Scheduling	“Develop a preliminary schedule for all activities involved in planning, establishing, and maintaining the interconnection. Also, determine the schedule and conditions for terminating or reauthorizing the interconnection. For example, both parties might agree to review the interconnection every 12 months to determine whether to reauthorize it for continued operation” (Grance et al, 2002)
• Organizational Security	
• Security Policy	
• Segregation of Duties	
• System Security Plan	
• Systems and Services Acquisition	
• Usefulness	“Consider the usefulness of the geospatial information to adversaries to include assessing the local threat environment, and installation vulnerability assessments” (Zettler, 2002)

derived from (Evans et al, 2004; Grance et al, 2002; Information Security Oversight Office, 2006; ISO/IEC 17799, 2000; Thiagarajan, 2003; Thiagarajan, 2005)

The case study did show that there was a need to identify security elements for the GeoBase program to assist with self-assessments and annual program reviews. Perhaps these constructs will provide additional thoughts on how to assess and develop metrics for measuring security successes throughout the different commands. Sharing lessons learned from these types of subject areas can only help to improve confidentiality, integrity, and availability as a whole.

PG5 What are the impacts of information security on information sharing within the GeoBase community?

Research question PG3 addressed the different information security concerns and how these barriers can get in the way of sharing information. Question PG5 will explore information sharing within the context of the GeoBase community in order to gain a better understanding of its impacts on information security. Six questions help to bring understanding of who uses and shares geospatial information within the Air Force and provide insight into the security requirements and controls needed for providing security.

The six questions we will explore using interviews, observations, and archived documents in this section are: 1) Whom are we sharing geospatial information with? 2) What is the geospatial information used for? 3) How are we sharing geospatial information? 4) Who are the primary GeoBase customers using and sharing geospatial information? 5) What are the impacts of sharing geospatial information? moreover 6) How do security concerns affect information sharing?

Whom are we sharing geospatial information with?

Installations do not operate in a vacuum and therefore cannot be expected to divorce itself from the local community. Users all over the base and local communities depend on information from each other for emergency, disaster response, and community planning efforts, open communication is needed and a trusting collaborative environment is required. GeoBase has fostered an open culture based on the benefits of information sharing. When asked about whom information is shared with, the answer comes back just shy of everyone.

Information is shared widely across different organizations and mission functions at the installations, up and down the chain of command amongst the different levels of an individual service, across the services, with other parts of the Department of Defense (DoD) and other federal agencies, state, local, and tribal governments, typically at a minimum classification of FOUO. (Headquarters Air Force Geo Integration Office, 2006). To varying degrees, the Air Force also shares its geospatial data assets with our allied governments, non-governmental organizations (NGOs), universities, and commercial sector contractors (Lachman, 2006).

One command noted that over the Air Force Portal they reach 600,000 to 800,000 users and receive in upwards of 350,000 hits per week to view the 16 common installation pictures (CIPs) posted. Although they have not been able to separate out the type of users by Air Force Specialty Code (AFSC) or general organization, they are getting back statistical reports that are becoming more useful, such as determining what areas and functions of the map and information have been most demand. If something happened where they needed to identify someone individually, they could. Over the SIPRnet, MAJCOMs can track unique individual users and know what they are doing on the map, such as calculating the parking area of an apron at Base X.

What is the geospatial information used for?

Ms. Beth Lachman, and her team at RAND National Defense Research Institute, is conducting research on “Assessing the Impacts of Sharing Geospatial Data Assets Across the Department of Defense (DoD)” (Lachman, 2006). In preliminary studies, her team

has identified 13 mission data uses, in Figure 17, associated with the base (shown in green) and another four uses associated more closely with warfighting (shown in blue).

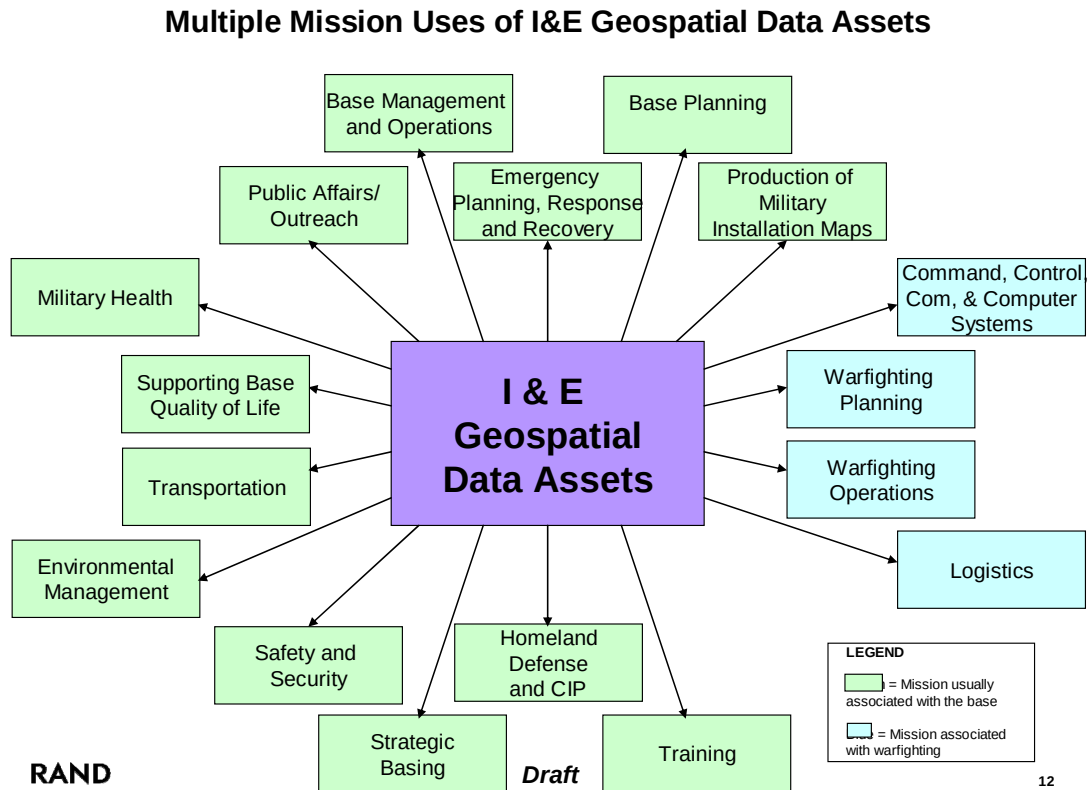


Figure 17. Multiple Mission Uses of Installation & Environment (I&E) (Lachman, 2006)

The following list (see Table 12 below) is a brainstorm of ideas and activities that include both actual and potential uses of what geospatial information is or could provide. These uses denote just the tip of the iceberg, but give an idea of the depth and breadth of the power of geographic information systems (GIS).

Table 12. Potential Uses of Geospatial Information

Wing Staff

Facilities Database (XPR)
 Facility Treaty Inspection Areas (CCT)
 Future Modification Plans (XPR)
 Jurisdiction Maps (JAG)
 Radio Frequency Footprint (XPR)
 Range Site Codes (Range Ops)
 Real Property Database (START Insp Bldgs) (CCT)
 START Reports (CCT)
 Courtroom litigation (gather, analyze, present geographically-referenced evidence) (JAG)
 Congregation Demographic, Outreach (HC)
 Historic District Mapping (HO)
 Historic Event Locations (HO)
 Tying Key Event Details to Map Locations (HO)
 Relating Date-Stamped Photos to Map Locations (HO)
 Inspection Preparation Activities (IG)
 Public Announcements, Newspaper Mapping Requirements (PA)
 FOL Deployment Intel Briefings (A2)
 Daily Intel Briefs (A2)
 3-D modeling for flood management and tidal wave planning
 Analysis for emergency operation and evacuation plans
 Emergency planning for special events
 Training exercises, e.g. earthquake simulation and chemical response

Safety

Explosive Storage Locations (SE / LG)
 Explosive Haul Routes Routes (SE)
 Bird Air Strike Hazards (BASH) Management (SE)
 Confined Space Locations (SE)
 Explosive Safety Quantitative Distance (ESQD Arcs) Zone Maps/Explosive Permits (SE)
 TERPS (on base and off base airfield obstructions)
 Toxic Hazard Corridors (SE)
 Base Evacuation Plan (SE)
 Destruct Zones (SE)
 Impact Limit Lines (SE)
 Real Property Database (Penetrability) (SE)
 Railroad Traffic (SE)
 Off-Shore Oil Area Parcel Grids (SE)

Operations Group

Visualize Airfield Features, Obstructions, etc. to Aircrew
 NOTAM Maps
 Imaginary Surfaces/Aerodrome
 Flight Corridors (DOJ)
 Flight Path Maps (DOJ)
 ILS Area Definition (DOJ)
 Meteorology Tower Locations (DOW)
 Meteorology Data (DOW)
 Real Property Database (Range Bldgs) (Range)
 RF Frequencies (Range)
 Risk Assessment Codes (SE)
 Safety Equipment Inventory (SE)
 Safety Inspection/Audit File (SE)
 Seismic Data (DOW)
 Special Use Airspace (DOJ)
 Terminal Instrument Approach Procedures (DOJ)
 Toxic Hazard Corridors (DOW)
 Airspace Boundaries (Range)
 Antenna/Radar Tower Database (Range)
 Critical Launch Facilities List (Range)
 Elevations (LOS) (Range)

Aircraft Data
 Aircraft Parking
 Fuel Pit Status
 Mission Schedules
 Air Show Planning
 Integration with the other systems: GDSS, Global Procedures System (TERPS), FalconView, Aircrew Portal, CAMPS, TBMCS-UL, JOPES, SMS

Logistics Group

Real-Time Location of People and Cargo on the Installation,
 Location of Aircraft on Ramp and Readiness/Maintenance Status, ESSP/BSP
 Aircraft Parking and Status (integrated with Geo81 and CAMS)
 GFE Equipment (LSS)
 HAZMAT Pharmacy (LSS)
 Hypergolic Fuels Database (LSS)
 Hypergolic Process Safety Inspections (LSS)
 Standard Base Supply System (LSS)
 Integration with other systems: G081/CAMS, LOGCAT (EKB/STEP), LOGMOD?, PAX Systems (Passenger Manifest), ITV, RFID, GTN, GATES

Medical Group

Flight Health
 Injuries/Illness Report
 Monitoring Data (DW)
 Occupational Risk Assessments
 Drinking Well Locations
 Air Models
 Mold Surveys
 Disease Mapping (Public Health)
 Water Sampling and BioHazard Points/Results
 Ambulatory Service Reqmts and Response Locations Log
 Pharmacy Locations

Support Group

Security Forces

Restricted Areas (SF)
 Building Security Features (SF)
 Access Control Points
 Observation Points
 Emergency Routes

Communications (A6)

Comm Infrastructure Locations
 Mass Notification Systems Coverage Areas
 Office Location Linked to GAL
 Cable TV (SC)
 Communication Lines (SC)
 Communication Equipment (SC)
 Personnel/Address (SC)

Services

Recreational Facilities List (SVS)
 AAFES Locations (AAFES)
 Golf Course Management (SVS)
 Golf Course Irrigation (SVS)
 Fitness Center, jogging routes (SVS)
 Management of Self Storage Lot / Lemon Lot (SVS)
 Outdoor Recreational opportunities, locations, times, events (SVS)

SVS-Produced Lodging Guest Maps (SVS)

Engineering & Base Development

Base Layout Map (CEC)
Building Centroids (CEC)
Building Location and Height (CEC)
Building Maintenance (CEC)
Jurisdiction Maps (CEC)
Land Use/Zones (CEC)
Landscaping Plan (CEC)
Crash Grids (CEC)
Demographic Data(Occupancy) (CEC)
5-Yr Future Construction Map (CEC)
Topography (CEC)
Traffic Logs (CEC)
Transportation Routes (CEC)
Aerial Photography (CEC)
ACES-PM Data (CEC)
Historical Aerial Photography (CEC)
AICUZ (Noise Contours) (CEC)
Work Order Request (AF Form 332) (CEO)
AF Form 1391 (CEC)
Dig Permits (AF Form 103) (CEO)
Landfill Records (CEO)
Lightning Protections (CEO)
Monitoring Data (Landfills) (CEO)
Pavement Management (CEO)
Pesticide Management Plan (CEO)
1-2 Yr Planned Construction/Renovation (CEO)
Refrigerants (ODCs) Database (CEO)
Service Contracts (CEO)
Utilities (CEO)
Linked System Map to Media Files (.mpg) Showing Videos
From Inside Sewer System
Feature Location (Valves, Manholes, Transformers, etc)
Water Distribution (CEO)
Sanitary System (CEO)
Wastewater / Storm System (CEO)
High Temperature Hot Water System (CEO)
Liquid Fuels System (CEO)
Electrical System (CEO)
Natural Gas System (CEO)
Snow Removal (CEO)
WIMS HW Management Module (CEO)
Facility Manager Information (CEO)
Lead and Asbestos Surveys (CEO / CEV)
Roof Inspections (CEO)
Track Installation Damage Assessment (Airfield & Facilities)
(CEO)
UXO Cordon Areas (CED)
NBC Detector Locations and Status (CEX)
Plot Chemical Release plumes (CEX)

Resources

Floor Plans (CEC / CER)
Mineral Resource Management Plan (CER)
Economic Data (CER)
Demolition Plan (CER)
Real Property Database (CER)
Real Property Database (% Utilization) (CER)
Real Property Database (Building Use) (CER)
Real Property Database (useable life of buildings) (CER)
Facility Category Codes (CER)
Space Utilization Management (CER)

Fire Department

Emergency Dispatch (Visual Control) (CEF)
Combined Dispatch Use (CEF / SFS / MDG ER)

Earthquake Fault Maps (CEC)
Fire Evacuation Plan (CEF)
Fire History (CEF)
Digital Pre-Fire Plans (CEF)
Fire Hydrant Test Data File (CEF)
Monoco Fire Alarm System integration (CEF / CEO)
Floor Plans (Alarms, Hydrants) (CEF / CEC)
HAZMAT Routes (CEF)
Future Real-Time Location Tracking (GPS Transponders)
(CEF)

Environmental

Ground Cover Maps (CEV)
Hazardous Waste Sampling Data (CEV)
Hazardous Waste Tracking System (CEV)
HAZMAT Plan (CEV)
Hazardous Materials Management (Pesticides, ODS, PCB
mapping)
Historical Water Table Data (CEV)
Hunting/Fishing Maps (CEV)
Industrial Waste Loadings (CEV)
IRP Site Maps/Reports (CEV)
Landfill Loading Records (CEV)
Artifact Photos (CEV)
Asbestos Survey Database (CEV)
Background Concentrations (CEV)
Monitoring Data (Air) (CEV)
Contaminated Soil Locations (CEV)
Monitoring Data (Soil) (CEV)
Monitoring Well Locations (CEV)
Natural Resources Study Areas/Data (CEV)
NPDES Permits (CEV)
Opportunity Assessments for PP (CEV)
Chem Hazard Emerg Response Plans (CEV)
Coastal Zone Management Plans (CEV)
Depth to Groundwater (CEV)
Endangered and sensitive Species (CEV)
Invasive species monitoring (CEV)
Environmental Project List (CEV)
Prime and Unique Farm Lands (CEV)
Process Waste Quantities (CEV)
PSD Station (Air Monitor) Locations (CEV)
Resources (Natural, Cultural, Historical) (CEV)
SPCC- UST (CEV)
Species Maps/Lists (CEV)
Tank Database (CEV)
TIP Tape - '76 Vegetation Study (CEV)
TSDF Permits (CEV)
Vegetation Fuel Age Class (CEV)
Vegetation Maps (CEV)
Vent Stacks on Pads (CEV)
Waste Maintenance Tracking System (CEV)
Waste Profiles (SB14)
Waste Stream Analysis (CEV)
Waste Stream Data
Water Quality Reports (IWTP)
Wetlands (CEV)
Ambient Air Quality Data (CEV)
Ambient Water Quality Locations (CEV)
Water management (3-D modeling of runoff)
Flood management
Watershed modeling of burn area from accidental fire
Incinerator analysis
Natural resource management
Cultural resources, archeological mapping
Encroachment analysis with aerial imaging overlays
GIS-based Environmental Management System

How are we sharing geospatial information?

With as many different uses and sharing relationships exist, there are equally as many ways in which to physically use and share information. The internet and intranet are the primary means to share data. A6 (Communications) has established network protocols that allow network controls. The network essentially controls the gateway through which information is shared. Web viewers such as ArcIMS, a popular Internet Mapping Service with the GeoBase community, and ESRI's solution for delivering dynamic maps and GIS data and services via the Web. It provides a highly scalable framework for GIS Web publishing that meets the needs of corporate Intranets and demands of worldwide Internet access" (ESRI, 2006). These web services provide the GIS viewing capabilities for the average non-GIS familiar users without the use of expensive standalone GIS software. For the majority of the GeoBase users across the installation, web viewers provide both accessibility and functionality. For those users who require a more sophisticated analysis and editing tool, they turn towards GIS desktop applications, such as ArcView, ArcInfo, ArcAnalyst, ArcGIS or ArcMap (ESRI's desktop GIS software used by the Air Force). Other methods in which information is shared is over the non-web based network systems, such as shared drives and folders; the "sneaker net" method, using mobile storage media (CDs, DVDs, floppy disks, thumb drives, etc.) to move and share information from one user or location to another. Table 13 highlights the primary methods of sharing information in the GeoBase community.

Table 13. Information Sharing Methods and Concerns

Sharing Method (Lachman, 2006:10)	GeoBase Example	Security Concern
Web Viewer	- ArcIMS Web sever (via the Air Force Portal)	
Desktop Application	- ArcGIS	
Non-web based network systems	- Base network shared drives (X://Drive) - Email	
Sneaker-net (Mobile Media)	- Floppy disks - CD / DVDs - Thumb drives - Mobile hard drives - MP3 players	
Map and Document Products	- Printed Maps - PowerPoint - PDF - Screen-shots - Image files (.jpgs, tiffs) - Email attachments	
Video and Simulators	- Video files (.mpgs)	
Field technology applications	-	
Specialized mission studies	- Mission reports - Conferences - Briefings	

Who are the primary GeoBase customers using and sharing geospatial information?

It is interesting to map the spread of geospatial information as users GeoBase program reaches out to new users or vice versa. As discussed in chapter two, the GeoBase program grew out of the Civil Engineering community as a Wing mission support program. In the early stages, geospatial information centered on civil engineering type information such as the common installation picture (CIP) type of information. Since the Air Force environmental flight had a history and experience using GIS information, environmental was one of the first to align themselves with GeoBase. Because of this early adoption and continued organizational support, the now robust

environmental mission data sets receive much attention. Several commands now employ dedicated staff to manage the demand for environmental information. Other early adopters were the emergency responders, particularly the fire, security forces, and readiness communities. The graphic below (Figure 18) illustrates the geospatial information centers of gravity within the Air Force. This graphic shows the relationships and magnitude of key information users.

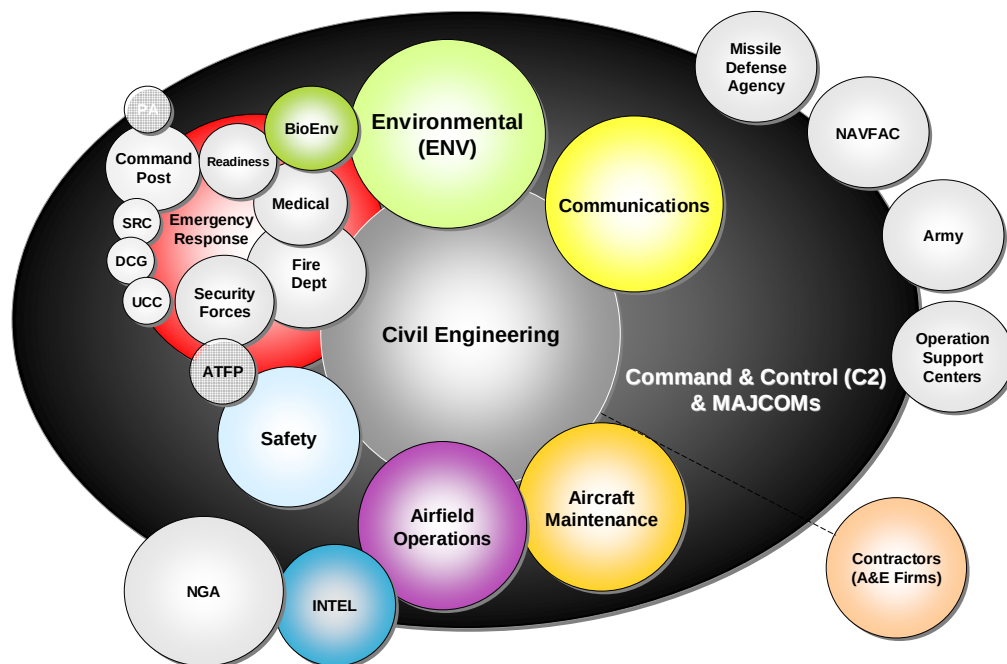


Figure 18. Air Force Geospatial Centers of Gravity

Notice how the nucleus of the information centered close to the operations of the mission and focused around the primary users of the installation warfighting platform. On the periphery, are the secondary users, the operations support centers, other services and organizations who have vested interests, information providers such as National Geointelligence Agency (NGA) and the Intelligence communities, as well as the

expertise and skills of contractors and non-governmental agencies which the installations rely. This later center of gravity notes an area of concern and will be discussed in more detail in another section.

The following graph (see Figure 19 below), from the RAND study, shows the distribution of users on one installation's ArcIMS web server and supports the above observations of defining the primary users.

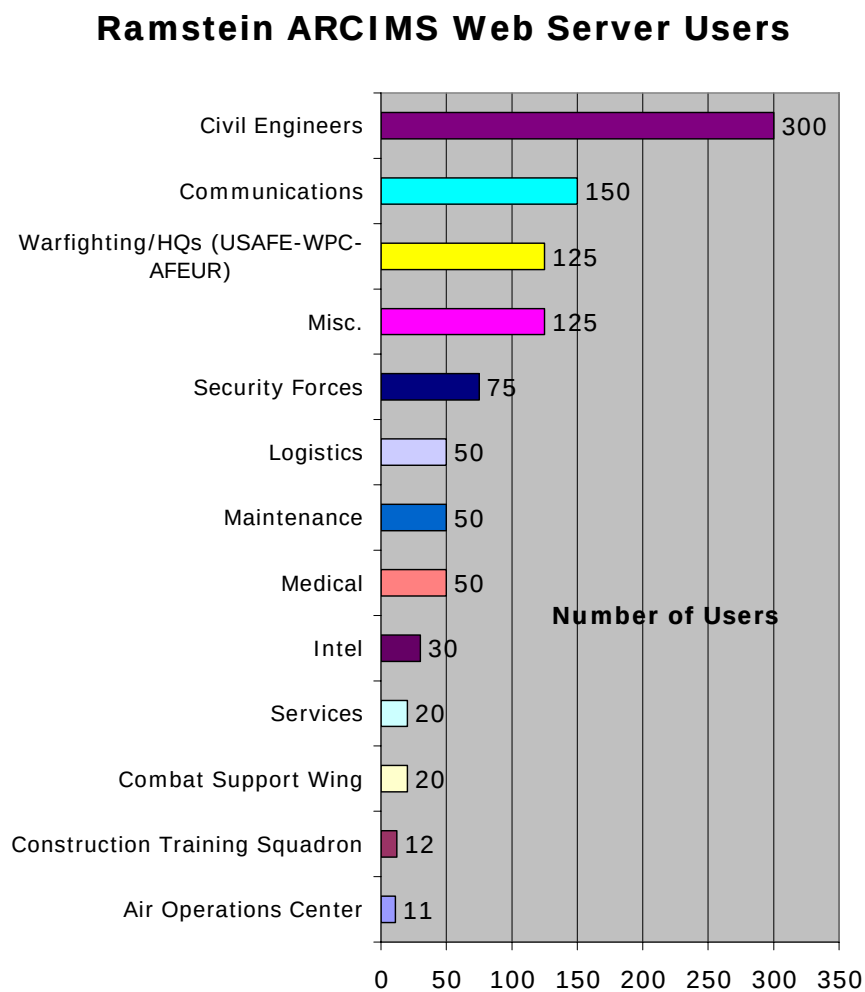


Figure 19. Case Study of Ramstein AB ArcIMS (Lachman, 2006)

If we can accept this installation as stereotypical of users across the command at other installations, then the conclusions on the primary GeoBase customers and users can be validated. Civil Engineering, Communications, Security Forces are shown as the top base-level users, while MAJCOM and higher-headquarters (consisting of fewer users) also remain as primary users. Arguably, as users become more familiar with the tools and information available, user's dependence on this type of information will continue to grow, as will threats and vulnerabilities. See the relationship between user familiarity and amount of information shared and risks to security in Figure 20 below.

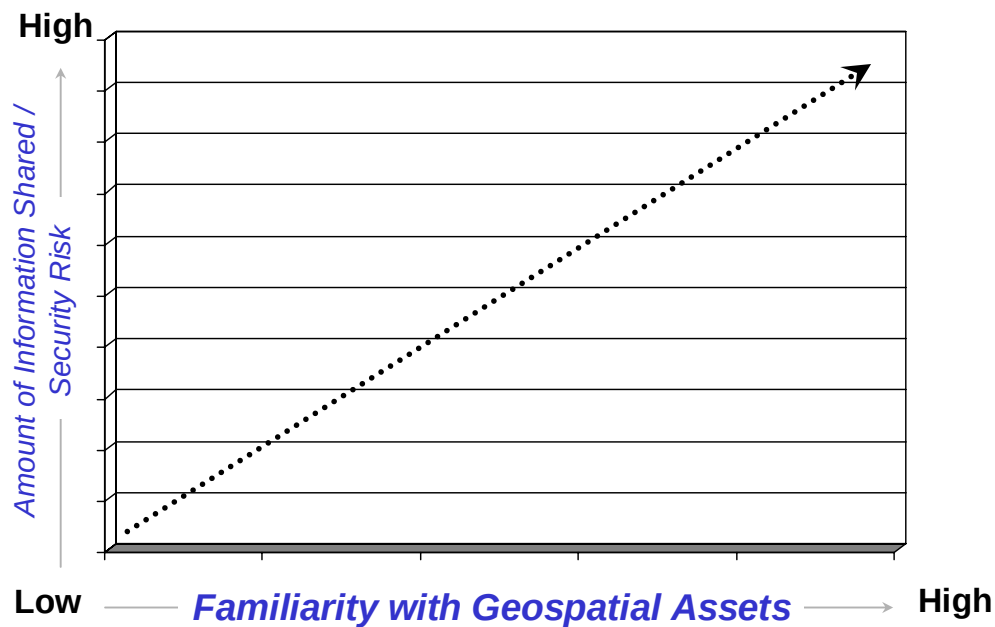


Figure 20. Impact of Familiarity with Geospatial Assets on Amount of Information Shared and Risk to Security

How does sharing information impact risk?

Vulnerabilities wait at each interchange and as demand for the interconnectedness spread, communications squadrons became more heavily involved, both as network

infrastructure providers and as customers who found their own benefit to managing information geospatially. As these networks become wider spread, the security controls become more complex, see Figure 21.

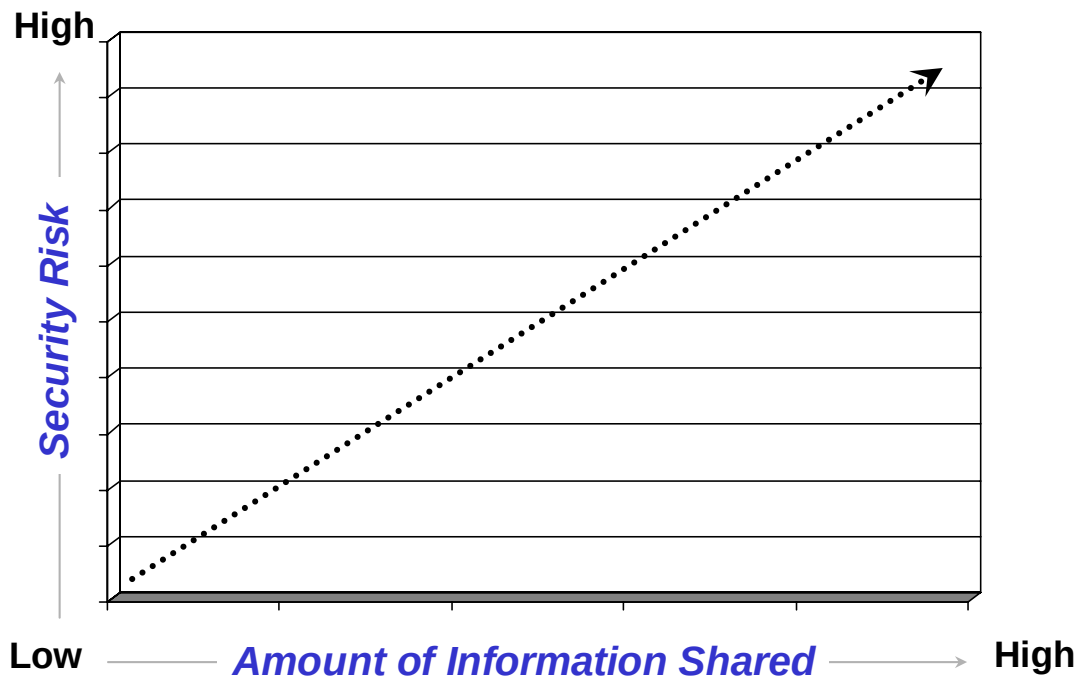


Figure 21. Information Sharing and Security Risk Relationship

What are the impacts of sharing geospatial information?

Now that we have seen how raising the amount of information shared also raises the risk potential. We know that completely cutting off the flow of information is unrealistic, but the tendency to start shutting down and limit the flow often happens without consideration of the other affects and benefits of sharing information. Table 14 begins to explore the additional benefits and impacts achieved through the sharing of information.

Table 14. Impacts of Sharing Information

Impacts (Lachman, 2006:10)	Benefits (Lachman, 2006:10)
Efficiencies	- Cost savings - Time savings - Manpower impacts - Improving contractor oversight
Effectiveness	- Improving operations, decision-making, and planning - Performing new task that would/could not be done before
Process Improvements	- Improving working relationships - Improving communications processes - Mostly automating a formerly manual process - Changing an analysis process
Affects to the Mission	- Policy impacts - Educational and training impacts - Public relations impact - Legal impact - Employee morale and productivity affects

Particularly in emergency situations, a high demand for information is required early in the response so that the right decisions and plans can be put into place. (MacFarlane, 2005:19). Figure 22 shows the typical information demand gap in the demand and availability of information.

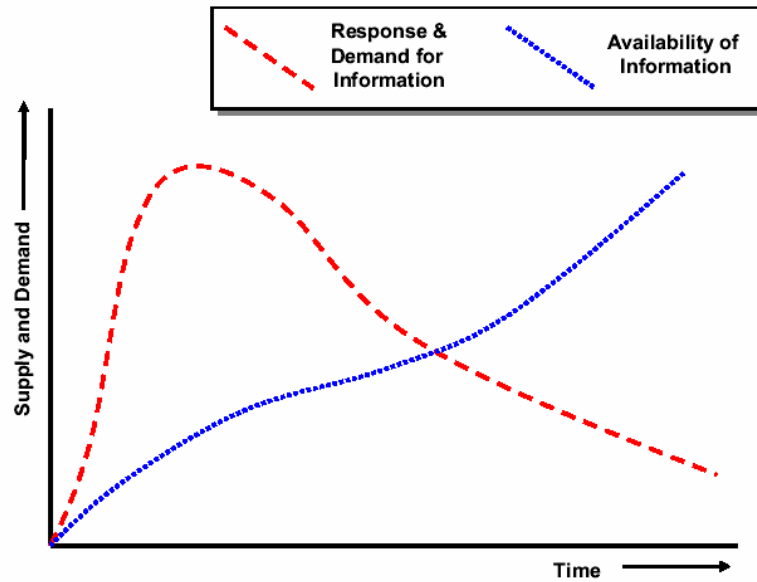


Figure 22. Information Demand-Provision Gap following an emergency event (based on work by Peter Power, Visor Consultants, 2004) (MacFarlane, 2005:8)

Whereas, Figure 23 depicts how an increase in the availability of information can narrow the gap between the need for information and what is available.

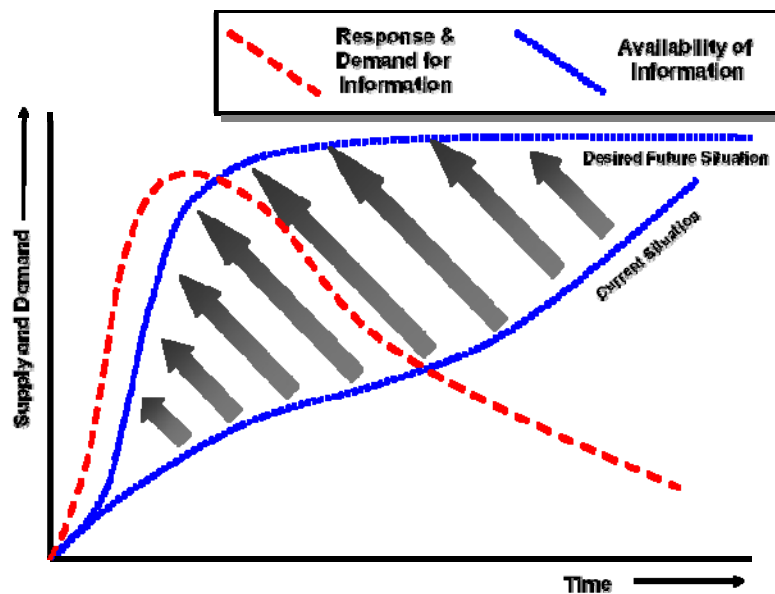


Figure 23. Accelerating information availability to keep closer pace with demand (based on work by Peter Power, Visor Consultants, 2004) (MacFarlane, 2005:26)

The shared geospatial information GeoBase provides help narrow this gap in the Air Force. Survival Recovery Centers (SRCs), Damage Control Groups (DCGs), Unit Control Centers (UCC), on-scene commanders through GIS and shared information networks, such as the Theater Battle Management Control System (TBMCS), a clearer situational picture is presented to a variety of decision makers. Now, instead of waiting hours for enough information for command and control to make a decision that it is safe to carry on the mission, is now completed with more precision, in much less time, and with a higher degree confidence.

PG6 What are the costs and benefits of either limiting or providing access to the data? Do they outweigh the risks?

As the concern over information security grows, the tendency seems to be that the sharing of information becomes limited, thus reducing the opportunities to synthesize information a helpful or a malicious way. There are costs involved to limit or manage the flow of information, both financial and non-monetary (mission) costs.

Financial Investments

Some experts have tried to calculate the financial costs of putting a classification on information. A 2005 cost report on government security classification done by the Information Security Oversight Office (ISSO) reported, “the total security classification cost estimates within Government for FY 2005 is \$7.7 billion. This figure represents estimates provided by 41 executive branch agencies, including the Department of Defense. It does not include, however, the cost estimates of the Central Intelligence Agency (CIA), which that agency has classified” (Information Security Oversight Office,

2006). Costs were divided into the following security constructs: physical security, such as the separate network, locks, safes, secure rooms, etc. that support that system; information security, which includes classification management, declassification, and information systems security for classified information; professional education, training and awareness; security management and planning; and unique miscellaneous items. (Information Security Oversight Office, 2006). Figure 24 breaks out the costs for each category, whereas Figure 25 compares the total government costs to that of industry for a ten-year period to provide further perspective.

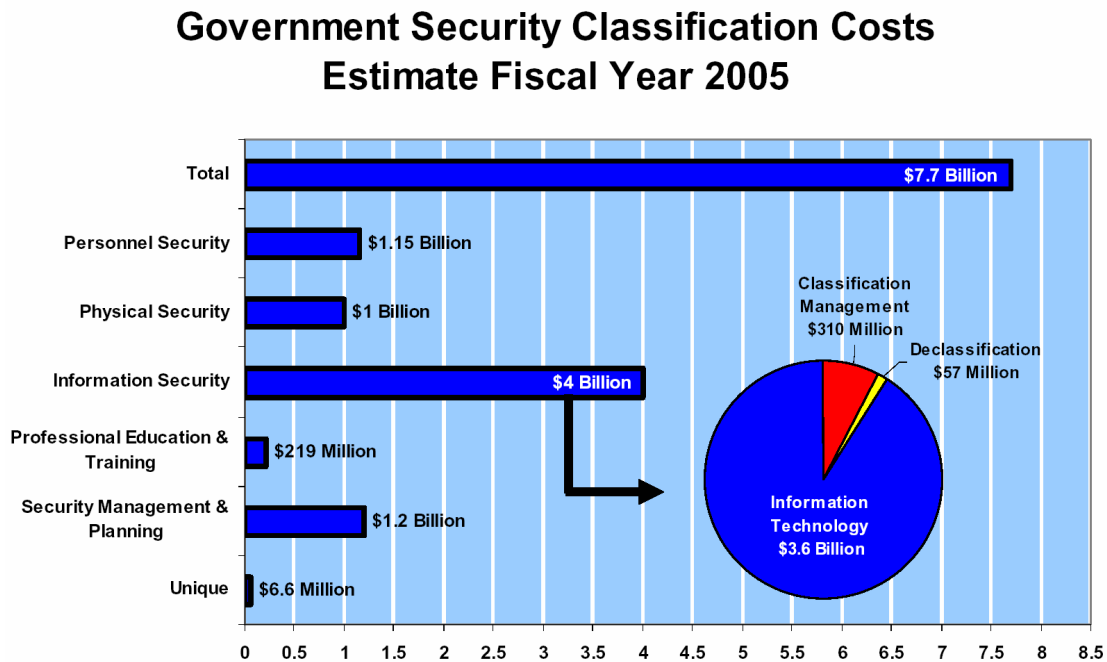


Figure 24. Government Security Classification Costs Estimate Fiscal Year 2005
(Information Security Oversight Office, 2006)

**GRAPH COMPARING TOTAL COSTS FOR GOVERNMENT AND
INDUSTRY FOR FY 1995 - 2005**

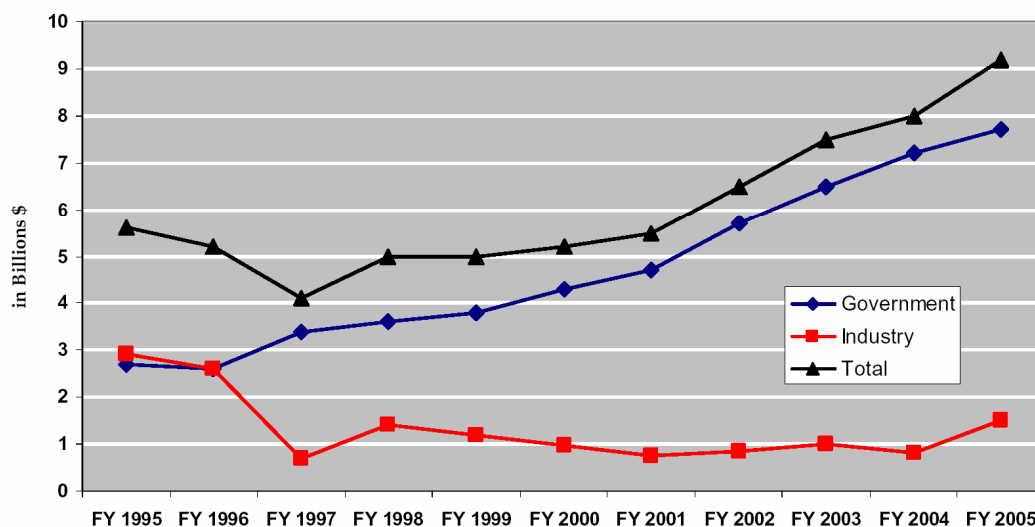


Figure 25. Graph Comparing Total Costs for Government and Industry for FY 1995-2005 (Information Security Oversight Office, 2006)

“In the past, the costs for the implementation of the programs to classify, safeguard and declassify national security information were deemed non-quantifiable, intertwined with other overhead expenses. While portions of the program’s costs remain ambiguous, ISOO continues to collect cost estimate data and to monitor the methodology used for its collection. Requiring agencies to provide exact responses to the cost collection efforts would be cost prohibitive. Consequently, ISOO relies on the agencies to estimate the costs of the security classification system. The collection methodology has remained stable over the past 11 years, providing a good indication of the trends in total cost. Nonetheless, it is important to note that absent any security classification activity, many of the expenditures reported herein would continue to be made in order to address other, overlapping security requirements” (Information Security Oversight Office, 2006).

Agencies, such as the Air Force, who invest in the GIS hardware, software, data and training understand the potential gains on their return on investment. Sure, there are high upfront costs, but “the level of benefit will be maintained over time as effectiveness and efficiency gains are realized” (see Figure 26) (MacFarlane, 2005:82).

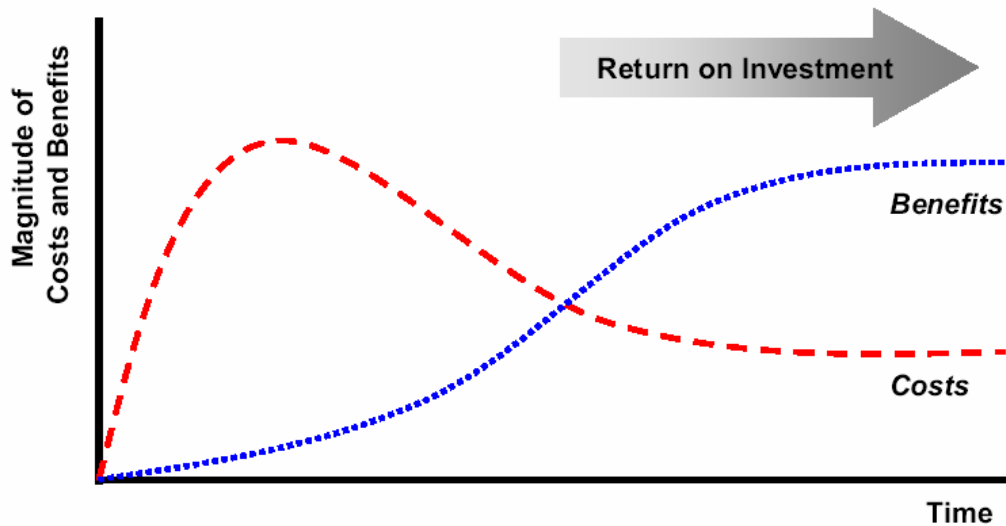


Figure 26. Timescale of Costs and Benefits of GIS Investments (MacFarlane, 2005:82)

In this section, we have explored a few aspects of different assumed financial costs. The next section will delve into the difficulty of putting a price on the demand for answers from information, particularly when the stakes of the questions are high.

Non-Monetary and Mission Benefits

Although it is unknown just how much it takes to secure the geospatial information of the GeoBase program, one can see that there are plenty of fiscal costs associated with the elements of security. Nonetheless, of greater value to the program is the understanding of the non-monetary costs of restricting access to customers that cost in

incalculable. The potential of restricted information having far bigger costs than just dollar costs are great. Not only are financial costs involved of things that we can see and count, but also there are the “would have” or “could have” costs of what would or could have happened if the information were not available when a particular decision was to be made. By keeping information out of the hands that need it could cost millions of dollars for an improperly sited building, millions in legal fees for an environmental disaster litigation process, or worse the potential of loss of aircraft and human life. For example, if explosive safety Q-D arcs are not shared and a contract is let to construct a building inside a Q-D arc, a lot of money is spent in change orders and redesign fees or the base inherits a risk to the facilities being inside a safety zone. On the other hand, knowing where the Q-D arcs are and their size, one could figure out what may be stored in that area that we do not necessarily want them to know. It becomes a fine balancing act. Another example of restricting information is confining it to the SIPRnet. SIPRnet is much more difficult to use than the NIPRnet and very difficult to deploy with. The Air Force Contingency Response Groups (CRGs) are an example of users of geospatial information who face the challenges of how to deal with sensitive information they collect for GeoReach. The GeoReach package relies on deploying forward, collecting data, and sending it back to the rear using NMARAT, a satellite communications system that can provide secure communications up to SECRET level. There are many reasons to keep things unclassified. Keeping information at a level so that it is readily available for use is important to maintain.

In the end, the cost is to the mission degradation and or mission effectiveness. If people cannot get quick access to the information they need, then they are bound to go

out and spend money or time to recollect. This can severely delay mission accomplishment (see Figure 27).

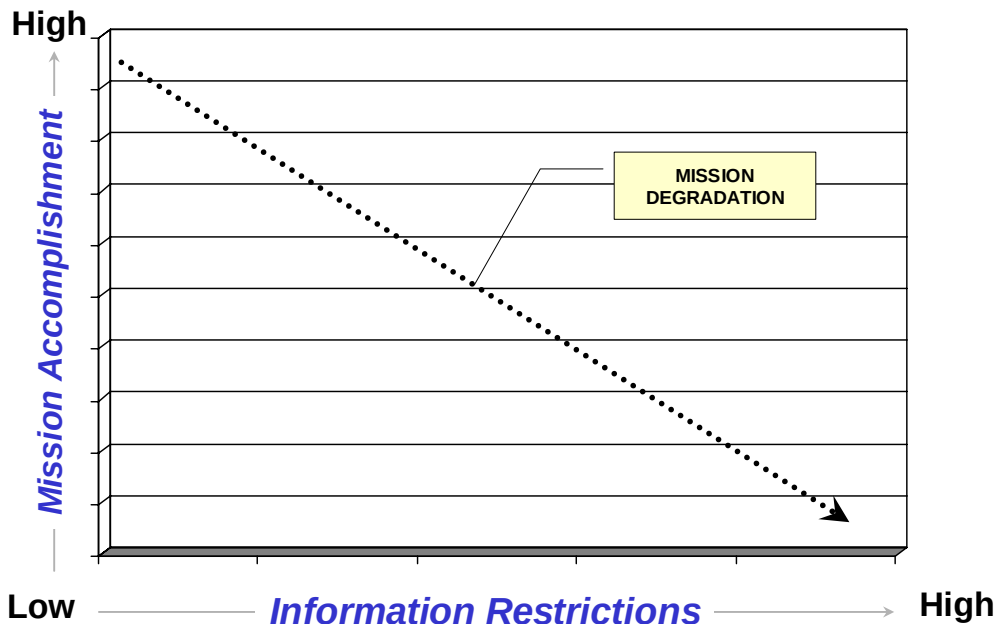


Figure 27. Information Restriction and Mission Accomplishment Relationship

Conversely, if people can be exposed to the information and know where to go to find it, time, money, and manpower can be decreased while increasing mission accomplishment.

Another example, at one base, someone dealing with the Freedom of Information Act (FOIA) maintained the understanding that the identity of base wells were not to be released or represented on the map and became concerned when a GeoBase map showed a building that housed a water well, a discussion ensued to have it removed. The historic document that was the basis of their understanding did not specify oil wells, water wells, drinking wells, etc. The GeoBase map had not annotated the facility identifying the facility as a well site. The problem comes in that if there was ever an emergency (fire, etc) and the fire department had to respond to that building, how are they going to

respond to it, if it is not on the map? Eventually, senior leadership took responsibility for it and allowed the information to be published. In this case, they were able to come to an understanding, but this example brings up two good points. One we have people out there that are appropriately concerned for the welfare of the base and have different perspectives of how information should be classified. The second is that it is important for communities with different perspectives to come together, while understanding that locking down information and not making it available to people is not the best answer, but look holistically at physical, logical, and administrative controls that can be enacted to overcome a complex and common goal..

A key finding in this research is that knowledge management is an important element in information security and information sharing. It is not always about giving and sharing the data, it is about sharing the awareness that the data exists. It is all about DATA DISCOVERABILITY. It is about information awareness and knowing where to get it. It may be available through a website, or speaking to a subject matter expert (SME), or the library. You can certainly restrict data to control better help alleviate some of these security concerns, but the problem is that you limit the intent of what the whole program is for of disseminate the information take advantage of the data being created. From the ESRI perspective, they want to be able to map the world and provide the data to everybody. That is good, but we must be careful where it may begin to interfere with our national security. There are many places to find information, it may be good to restrict access, but the key is not to restrict data discoverability.

V. Conclusions and Recommendations

In this chapter, we discuss the conclusions, recommendations, and suggestions for future research. This exploratory case study only begins to scratch the surface of GIS operational security issues. By no means is this study able to include the magic answer on securing geospatial information or the key to opening the door to the challenges of information sharing. It can however, continue, and in some cases begin, the needed discussion on these important issues challenging the Air Force community. Without purposeful discussion and awareness of the challenges, we cannot expect to adapt our business processes and policies to address to keep up with the constant changes in vulnerabilities and threats brought about by time and technology.

Conclusions and Recommendations

Increased use of electronic data sharing denotes a greater chance of information misuse, both inside and outside the Air Force. As the repository of critical information builds, GeoBase information will face a heightened risk of being targeted through cyber terror attacks. The security implications of the USAF GeoBase program are but a subset of a growing national dilemma that plagues academics and practitioners.

We have seen the inevitable swinging of the pendulum from all access and no control to the desire for tightly regulated and restricted information security laws, policies, and procedures. It is imperative that common and explicit guidelines are developed and implemented throughout the USAF and the DoD. There is a need in the Air Force to establish a tacit understanding that security of information is important and that the costs involved with not maintaining security standards are intolerable based on

the understanding of the risk. If this type of mindset does not exist, then the entire organization will continue to remain at risk and experience mission degradation, reduced productivity, lost data, revealed military secrets or compromised integrity. Motivating airmen and civilian partners to realize these risks and prepare them to treat geospatial data they handle as if it is their own banking information will go a long way in protecting the missions they serve. Without common standards to dictate minimum-security requirements and practices, bases will be left to develop and implement their own security standards. As a whole, the organization is only as strong as the weakest link.

Not only is it imperative to develop policies and procedures for sharing data, but it is incumbent upon this community to educate itself on the information that exists today.

Information security cannot limit data discovery; rather, it should encourage one's self to illuminate new data/information while providing the necessary security blanket that the discoveries will remain in the hands of a safe user community.

There are significant costs; not only financial, but serious mission degradation and effectiveness are at stake. The first step to moving beyond the problem is establishing and investing in the appropriate business processes to identify the sensitivity of information both on its own and combined with other information. Today's solution of referring to historical documents, policies, and processes and specific requests by the data steward or data layer owner has been a good start, but as the information grows in value and becomes more easily accessible through new technologies, these old decisions must be rethought as they do not completely address the issues of today's information situation. Just as the GeoBase service has helped to overcome the stove-piped mentality on the map between functional areas through the common vision of "One Base, One

Map”, similar hurdles must still be overcome in other areas of the organization. No one particular knowledge set will be able to solve this interwoven problem on its own. We need the expertise of many essential communities such as Information security (Infosec), Operational security (Opsec), Communications security (Commsec), the GeoBase Integration Office (GIO), and the data owners to come together to weave a balanced approach. There is a lot of work ahead, as the environment continuously changes, we must be willing to adapt. People will continue to find the information they need. If they do not have quick access to the information, then they are bound to either make a uninformed decision or spend money or time to recollect. We must keep in mind is that these efforts are not just about sharing the data itself, but building the awareness that the information exists. The quest for information security must not limit data discoverability and the ability to if not share the information, share that it exists and where it may be found. By actively managing geospatial information and the knowledge it brings we can more effectively identify and build the processes and have the best of all three worlds: accuracy, accountability, and access.

Much research is still needed to understand how to find balance between information security and the need to share data. A greater understanding of the technical side of computer security and the growing threats in cyberspace combined with the knowledge of what data providers know about what they provide in their functional area will help more efficiently and securely align the GeoBase workflows with Air Force Business processes needed for progress. As we become more connected across functional areas and between services the more important it become to coordinate our actions and collectively fight to protect the valuable information that protects us.

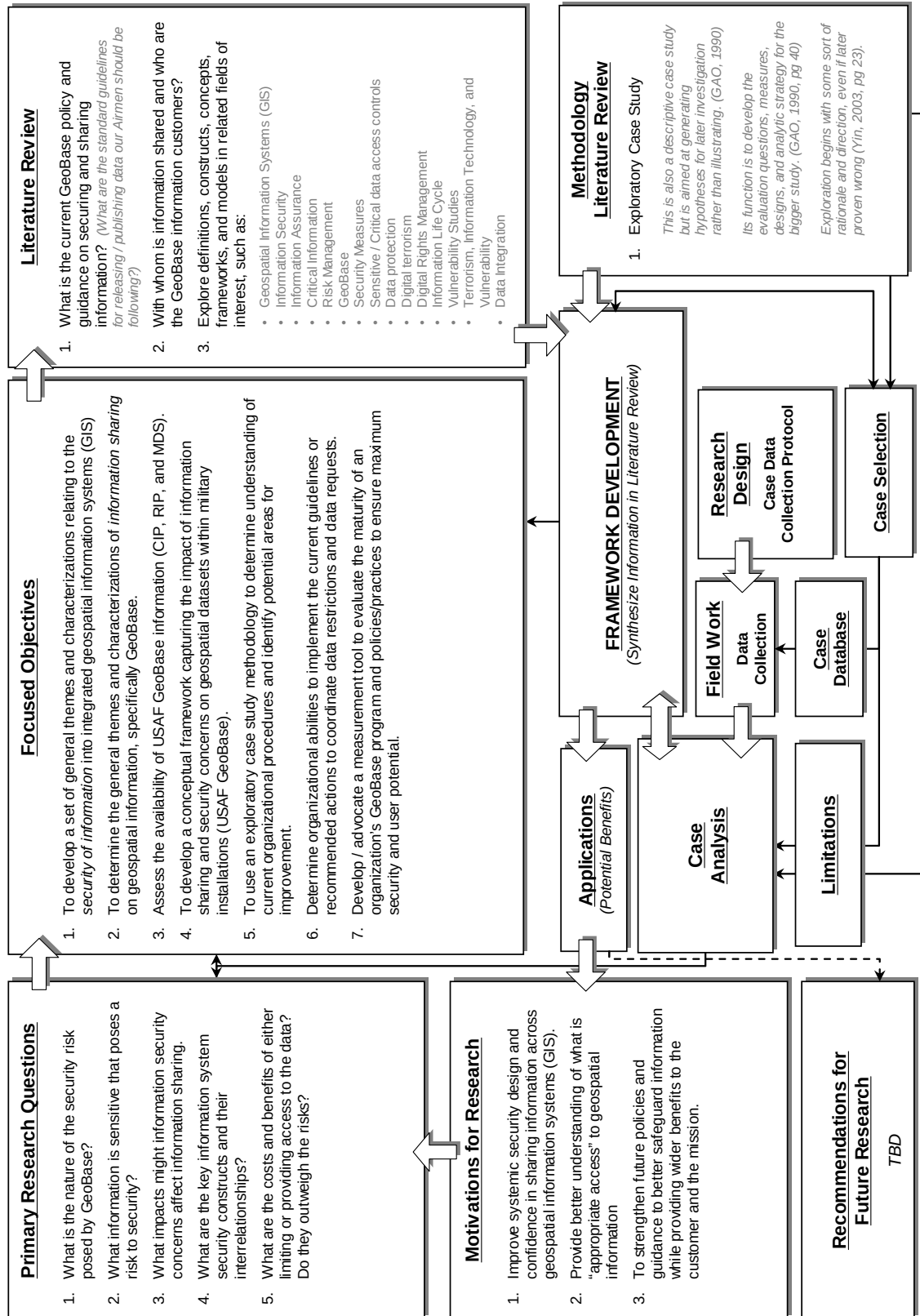
Table 15. Suggestions for Further Study

Proposition	Key Implications for Practice	Avenues for Future Research
1	Geospatial Information Sharing	Pinpointing barriers to information sharing within the culture of the Air Force and how they might be overcome.
2	GeoBase Metrics	A look at how well we have/are operationalizing GeoBase. HAF has been collecting an Air Force wide inventory from the different units at different levels. What we do not have is any type of inspection criteria or analysis of “best practices”. Identification of common themes which units and subsequently major commands and IG teams to look for that continue to enable the advancement of the technology that we’ve invested so heavily.
3	GeoBase Returns on Investment: Is GeoBase Paying Off?	Examine the investments made for GeoBase and determine a way to identify and quantify the returns on investment. Are our up-front costs paying off the way we anticipated them doing?
4	GeoBase Central Management and Funding	A look at the implementation and management of the GeoBase program's funding chain. As standards differ from one MAJCOM to another, some standards may not be on another's scope. Managing an Air Force Program without standards and sideboards? How do you transition from "as is" to "to-be" without a requirement? It is easier from a MAJCOM perspective, if the units are funded from that entity. What

		is the best way to fund units from one source entity or leaving it up to the units to fund their own programs; regardless, how do you set standards and evaluate the different set requirements?
5	Expanding GeoBase Centers of Gravity	An examination of the expansion of GeoBase beyond the parent organization (CE and other established centers of gravity). Bred within the Civil Engineering organization, GeoBase spreads beyond the scope of just CE. Are we organizationally postured to take advantage of all the possibilities that GIS (Information Technology) has to offer? Organizationally, how do we begin to expand that beyond CE into other career fields...much like our Field Operating Agencies (FOAs), such as Comm, Security Forces, AFCEE, AFCESA, etc
6	Information Security of Information Released to Contractors	How does giving geodatabase information to a contractor compare with previously releasing AutoCAD files?

Approach to Research Overview

Overall: Improve the general understanding of importance of
Research Goal: balance between **securing** and **sharing** information.



Appendix B: Investigation Protocol

Exploratory Case Study

Geospatial Informational Security risks and concerns of the U.S. Air Force GeoBase Program

Scott A. Bryant
Air Force Institute of Technology (AFIT), Wright-Patterson AFB, OH, USA
scott.bryant@afit.edu

Abstract	iv
Acknowledgements	vi
List of Figures	vii
List of Tables	ix
I. Introduction	1
Overview	1
Motivations for Research	2
Targeted Research Area	3
Research Goals	4
Overall Approach to Research	4
Benefits / Implications of Research	4
Thesis Overview	5
II. Background	7
Introduction	7
What is Information Security?	7
What is Geospatial Information?	8
GeoBase History	8
Emerging Geospatial Technologies	11
A New Paradigm	11
New Paradigms, New Problems	12
New Problems, New Policies	17
Identifying Security Risks	24
Top Challenges	27

III. Methodology	36
Purpose and Organization	36
Developing the Research Strategy	36
Case Study Research	38
Why an Exploratory Case Study?	39
Case Study Design	39
Step 1: Define and Design	40
Step 2: Prepare, Collect, and Analyze	50
Step 3: Analyze and Conclude	53
Potential Pitfalls	55
Summary of Methodology	57
IV. Analysis	58
PG1 What is the nature of the security risk posed by GeoBase?	58
PG2 What information is sensitive that poses a risk to security?	67
PG3 What impacts might information security concerns affect information sharing.	76
PG4 What are the key information system security constructs and their interrelationships?	82
PG5 What are the impacts of information security on information sharing within the GeoBase community?	91
PG6 What are the costs and benefits of either limiting or providing access to the data? Do they outweigh the risks?	104
V. Conclusions and Recommendations	111
Conclusions and Recommendations	111
Appendix A: Approach to Research Overview	116
Appendix B: Investigation Protocol	117
Background	119
Key Documents	119
Research Enablers	120
Field Procedures	120
A Guide for the Study Report	123

Appendix C: Thesis Research Overview (Sent to Interviewees).....	124
Appendix D: Interview Outline	130
Appendix E: Relative Laws & Executive Orders (1950 to Present).....	133
Appendix F: Relative Policies and Guidance	141
Bibliography	142

Background

Technological advancements such as Geospatial Information Systems (GIS) and the Internet have made it easier and affordable to share information, thus making complex and time sensitive decisions with higher levels of confidence. However, the sharing of information also increases the likelihood that an adversary can gain illicit access to the information. Today's military leaders face challenging decisions on how to make geospatial information collected on military installations and organizations available to authorized communities of interest while simultaneously restricting access to protect operational security. Often, these decisions are made without understanding how the sharing of certain combinations of data may pose a significant risk to protecting critical information, infrastructure or resources. Information security has been an area of growing concern in the GeoBase community since, by definition, it is required to strike a balance between competing interests, each supported by federal policy: (1) the availability of data paid for by tax dollars and (2) the protection of data as required to mitigate risks. This research sets out to explore the security implications of the US Air Force GeoBase (the US Air Force's applied Geospatial Information System) program. We examine the rapid expansion of the use of geospatial information in the military; examine the intrinsic and extrinsic security risks of the unconstrained sharing of geospatial information; and explore difficulties encountered when attempting to facilitate sharing geospatial information sharing while minimizing the associated operational risks.

Key Documents

- RAND Report, “[Mapping the Risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Information](#)”. (Baker, 2004)
- AFIT IMGT 669, “Vulnerability Investigation” (2004)
- “Evolving Federal Protocols for Safeguarding Geospatial Information” (Cullis)
- DoD Directive 8500.1, “Information Assurance (IA)”, 24 Oct 2002
- DoD Directive 8100.1, “Global Information Grid (GIG) Overarching Policy”, 19 Sept 2002
- GAO Report, “Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information”, Mar 06

- GAO Report, “Homeland Security: Efforts to Improve Information Sharing Needs to be Strengthened”, Aug 2003

Research Enablers

This research is being sponsored by the following organizations:

AF/A7CI (Pentagon)
Information Resources Management Division, DCS/Installations,
Logistics & Mission Support

USAF GIS Support Center (USAFA)
US Air Force Academy, Colorado Springs

Field Procedures

Setting up the interview

Begin by an initial phone call or introduction email (basic format below) to establish contact and explain the purpose of the interview. Follow up with a phone call and additional email with additional information.

[Rank] [Name],

My name is Capt Scott Bryant. I am a student at the Air Force Institute of Technology conducting thesis research regarding geospatial information security and information sharing. Specifically, the goal of this research is to identify security and sharing issues regarding geospatial information of the USAF GeoBase program and to improve the general understanding of importance of balance between securing and sharing information in order to maximize USAF mission processes and minimize customer inefficiencies.

I understand you are involved with this process and I would like to conduct an interview to gather data for my research. Please contact me at scott.bryant@afit.edu if you are able to participate and we can set up a time convenient for you.

If you have any questions, please do not hesitate to contact me. I have also included my thesis advisor's contact information below:

Thesis Advisor: Dr. Michael Grimaila – Phone 937-255-3636 (DSN 785) x. 4800; Email - michael.grimaila@afit.edu.

Thanks,

*Scott A. Bryant, Capt, USAF
Student, Air Force Institute of Technology (AFIT)
School of Engineering and Management (ENV)
scott.bryant@afit.edu*

Immediately prior to the interview:

1. Review pertinent information
2. Ensure to have the following information readily available:
 - a. Reference Folder
 - b. Any correspondence previously made with the interviewee
 - c. List of Questions / Question Answer Sheet
 - d. Laptop and notepad for recording answers

At the start of the interview:

1. Researcher Introduction: “My name is Capt Scott Bryant. I am a student at the Air Force Institute of Technology conducting thesis research regarding geospatial information security and information sharing within the US Air Force GeoBase program.”
2. Ensure attendees are familiar with the intent and concepts of the research. Read the purpose statement: “the goal of this research is to identify security and sharing issues regarding geospatial information of the USAF GeoBase program and to improve the general understanding of importance of balance between securing and sharing information in order to maximize USAF mission processes and minimize customer inefficiencies.”
3. Describe the interview process: “This will be a semi-structured interview. I have a short list of questions, which may lead to additional questions for further research or clarification purposes. Please feel free to interject any information you feel may be useful to the research.”
4. Assure anonymity: “I want to remind you that no identifying information obtained through this or subsequent interviews will be retained or reported in the final thesis. In order to complete the research effort, data collected on individual subjects may include duty title and description of/duration in current position, which will facilitate analysis and follow up for the duration of this study only. Data gathering will be focused on information specific to the USAF GeoBase policies and procedures.”
5. Obtain permission for vocal recording (if applicable): “Vocal recording is a useful tool to my research so that I may accurately capture the conversation, reducing the chance for misinterpretation. Do I have your expressed permission to record this interview?”
6. Record Interviewee information and interview start time on record sheet

7. Ask the appropriate questions, depending on the interviewee
8. Provide interviewees ample time to fully articulate all comments. Wait for appropriate pauses to seek clarification and for follow-up questions. Capitalizing on the nature of the discussion, allow brainstorming of ideas. Tangential ideas can be flushed out as the comments lull. (Oliver, 2004; Swanson et al, 2005.).

Following the interview:

1. Record interview stop time on record sheet
2. Consolidate all information into Case Study Database (see below)
3. Follow up with an email which should contain the following elements (see template below):
 - a. Short message thanking the participant for their time
 - b. Request for any outstanding information necessary for completing the report
 - c. Full contact information of researcher and thesis advisor
 - d. Assurance they will receive a copy of draft report when complete.
 - e. Reiteration of any information promised to the interviewee during the interview

[Rank] [Name],

Thank you for participating in the [telephone] interview conducted on [date]. The information you provided will certainly contribute to my research efforts.

*As discussed, I would appreciate your assistance in obtaining the following documents:
[As applicable]*

Also, as discussed, I owe you the following information/deliverables: [As applicable]

In addition, you will receive a copy of the draft thesis for your review prior to publishing.

If you have any questions, please do not hesitate to contact me.

Thanks again,

*Scott A. Bryant, Capt, USAF
Student, Air Force Institute of Technology (AFIT)
School of Engineering and Management (ENV)
scott.bryant@afit.edu*

4. Once the instrument has been completed and all necessary clarification and follow-up has been accomplished, type up the interview notes. Send each

participant a copy of the notes and request a review. For the review, each participant should add any additional comments and correct any errors in content or context. Use of Track Changes in MS Word facilitates the investigators review and allows copies to be saved for the “chain of evidence”. When the investigator receives each reviewed copy, he should note any changes or additions. Edits should be discussed, which may spur more discussion. A final opportunity to add comments should also be given. (Oliver, 2004).

A Guide for the Study Report

The final case study report will be written in the approved Air Force Institute of Technology thesis format.

Appendix C: Thesis Research Overview (Sent to Interviewees)



AFIT

Air Force Institute of Technology



Geospatial Informational Security risks and concerns of the U.S. Air Force GeoBase Program

Capt Scott A. Bryant
AFIT/GEM

U.S. AIR FORCE

14-Dec-06

2



U.S. AIR FORCE

THESIS PROPOSAL PRESENTATION
Capt Scott A. Bryant, AFIT/ENV



Geospatial Informational Security risks and concerns of the U.S. Air Force GeoBase Program



Research Enablers:

AF/A7CI (Pentagon)

Information Resources Management Division,
DCS/Installations, Logistics and Mission Support

USAF GIS Support Center (USAFSA)

US Air Force Academy, Colorado Springs

Thesis Committee:

Dr. Michael R. Grimaila (Advisor)

Ass't Prof of Info Mgmt, CISM, CISSP, GSEC Gold
Dept of Systems and Engineering Management

Dr Alfred Thal (GEM)

Assistant Professor
Dept of Systems and Engineering Management

Maj Chris West (GEM)

Assistant Professor
Dept of Systems and Engineering Management

105

One Installation...One Map



U.S. AIR FORCE

Abstract

Security Risks in USAF Geospatial Information Sharing

Scott A. Bryant,
Michael R. Grimaila (Advisor)
Air Force Institute of Technology (AFIT), Wright-Patterson AFB, OH
scott.bryant@afit.edu
michael.grimaila@afit.edu (937)255-3636 (DSN 785-3636) ext 4800

Technological advancements such as Geospatial Information Systems (GIS) and the Internet have made it easier and affordable to share information, which enables complex and time sensitive decisions to be made with higher confidence. Further, advancements in information technology have dramatically increased the ability to store, manage, integrate, and correlate larger amounts of data to improve operational efficiency. However, the same technologies that enable increased productivity also provide increased capabilities to those wishing to do harm.

Today's military leaders are faced with the challenge of deciding how to make geospatial information collected on military installations and organizations available to authorized communities of interest while simultaneously restricting access to protect operational security. Often, these decisions are made without understanding how the sharing of certain combinations of data may pose a significant risk to protecting critical information, infrastructure or resources. Information security has been an area of growing concern in the GeoBase community since, by definition, it is required to strike a balance between competing interests, each supported by federal policy: (1) the availability of data paid for by tax dollars and (2) the protection of data as required to mitigate risks.

In this paper, we explore the security implications of the US Air Force GeoBase (the US Air Force's applied Geospatial Information System) program. We examine the rapid expansion of the use of GeoBase to communities outside of the civil engineering field; examine the intrinsic and extrinsic security risks of the unconstrained sharing of geospatial information; explore difficulties encountered when attempting to rate the sensitivity of information, discuss new policies and procedures that have been implemented undertaken to protect the information, and propose technical and managerial control measures to facilitate sharing geospatial information sharing while minimizing the associated operational risks.

Keywords: Geospatial Information Security, USAF GeoBase, Terrorism, Targeting, Information Sharing

14-Dec-06

One Installation... One Map

3



U.S. AIR FORCE

Primary Research Goal



Improve the general understanding of importance of balance between **securing** and **sharing** information in order to maximize USAF **mission** processes and minimize **customer** inefficiencies.

SECURITY



BENEFITS
(Sharing)

14-Dec-06

One Installation... One Map

4



U.S. AIR FORCE

Secondary Research Goals



1. Improve systemic security design and confidence in sharing information across geospatial information systems (GIS).
2. Provide better understanding of what is “appropriate access” to geospatial information
3. To strengthen future policies and guidance to better safeguard information while providing wider benefits to the customer and the mission.

14-Dec-06

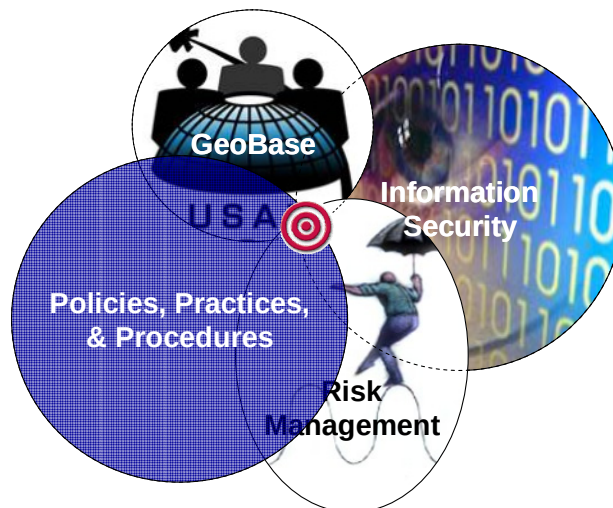
One Installation...One Map

5



U.S. AIR FORCE

Targeted Research



14-Dec-06

One Installation...One Map

6



U.S. AIR FORCE

Type of Research Case Study (Exploratory)

Table 3.2: Exploratory Case Studies

Aspect examined	Characteristic
Evaluation questions	Usually cause and effect
Functions	Where considerable uncertainty exists about program operations, goals, and results, exploratory case studies help identify questions, select important measurement constructs, develop actual measures for these, which can be used later in larger-scale tests; formulate expectations; safeguard investment in larger studies (for problems or programs that are not well-developed)
Design features	Site selected; needs at least one site that represents each important variation to make a convenience sample acceptable; number of cases sufficient to cover diversity; data focus on program operations and on-site observation, are not longitudinal but need enough time to find out what is going on; analysis is closely concurrent with field work but does not require strong chain of evidence or audit trail; reports are usually internal or parts of larger, longer reports
Pitfalls	Temptation to prolong the exploratory phase; site selection only for convenience; inadequate coverage of diversity; prematurity —exploratory findings released as conclusions; over-involvement in evaluator's own hunches so that initial findings are confirmed rather than tested

Exploratory Aspect

- When discussing “security”, so many uncertainties exist. This research will also explore questions and, where possible, develop measurement constructs for further research in this field.
- Aimed at defining the questions and hypotheses of a subsequent study or determining the feasibility of the desired research procedures (Yin, 2003, pg 5)
- Goal may justifiably be to discover theory by directly observing social phenomenon in its raw form (Yin, 2003, pg 6)
- Should be taken at face value (Yin, 2003, pg 7)
- Problems may arise if investigator wrongly uses data collected as part of an ensuing case study (Yin, 2003, pg 7)

14-Dec-06

One Installation...One Map

1



U.S. AIR FORCE

Key Concepts (for Literature Review)

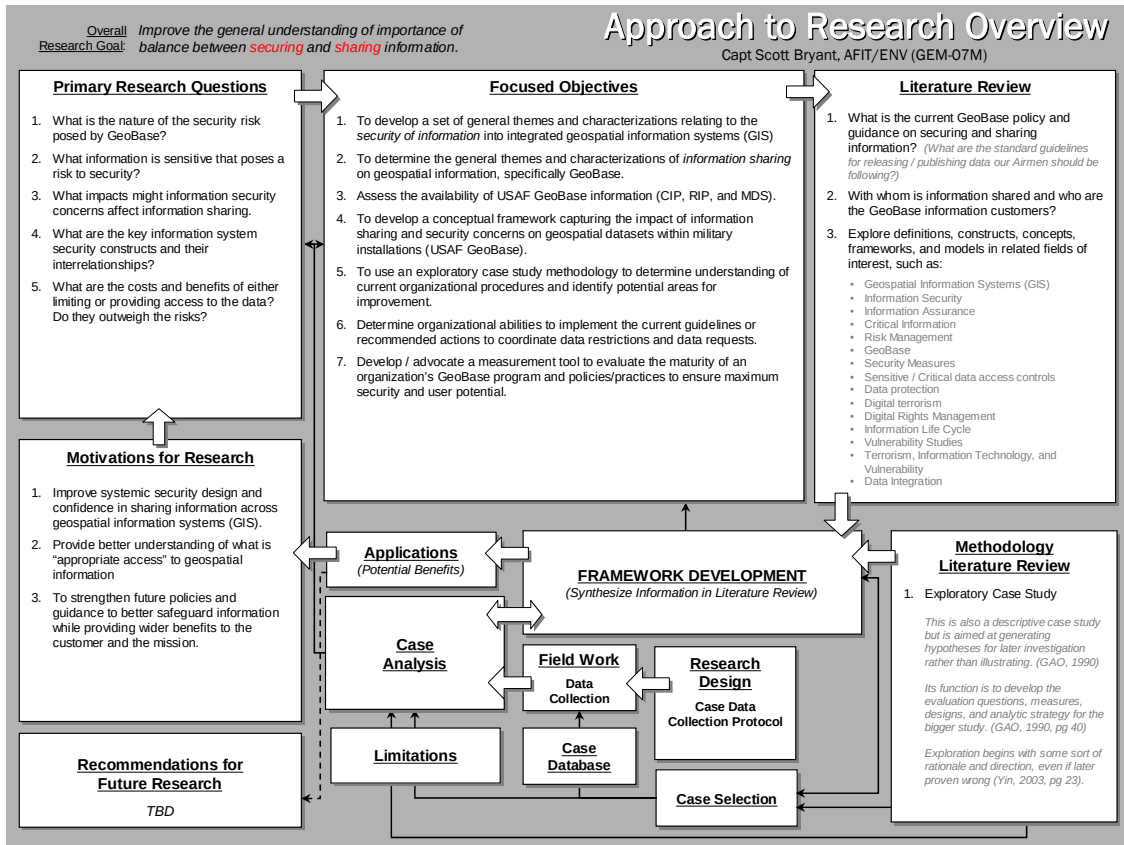
USAF GeoBase
Geospatial Information Systems (GIS)
Information Security
Information Assurance
Information Sharing
Critical Information
Data-sharing policies
Data Stewardship
Risk Management
Security Measures
Sensitive / Critical data access controls
Data protection
Digital terrorism
Digital Rights Management
Information Life Cycle
Vulnerability Studies
Terrorism, Information Technology, and Vulnerability
Knowledge Management
National Map Efforts
Global Information Grid (GIG)
Freedom of Information Act
User Rights and Privileges
Internet Map Servers (IMS)
Data Integration (Security)
DoD Information Policies
Information Resource Management (IRM)



14-Dec-06

One Installation...One Map

9





U.S. AIR FORCE

The Road Ahead



- Continue reviewing policies
- Nail down framework
- Evaluate support structure
 - DoD
 - MAJCOMs (1 or all)
 - Unit Level
- Establish Scope
- Determine Key Questions for Interviews
- **Conduct Interviews**
 - Phone
 - VTC
 - Site Visit
- Populate Case Database
- Synthesize and Analyze Data
- Explore the community's needs & opportunities (*Exploratory Case Study*)



14-Dec-06

One Installation...One Map

10

RESEARCHER CONTACT INFORMATION

Capt Scott A. Bryant, AFIT/ENV

Air Force Institute of Technology (AFIT),
Engineering Management (GEM)
Wright-Patterson AFB, OH
scott.bryant@afit.edu

GRADUATION DATE: MAR 07

Dr Michael R. Grimala

michael.grimala@afit.edu (937)255-3636 (DSN
785-3636) ext 4800



11

One Installation...One Map

Appendix D: Interview Outline

Disclaimer: The research associated with the interviews conducted during the site visits is wholly academic in nature and not connected with any GeoBase reviews, initiatives, or staff visits.

Research Background: The researcher is a captain in the AF and a graduate student in the Information Resource Management (IRM) program at the AF Institute of Technology. As part of the graduation requirements, the researcher must complete a thesis research project. The topic chosen, in collaboration with the Headquarters Air Force Geo Integration Office (HAF-GIO), concerns the relationship of IRM and GeoBase. The primary objective of this research is to:

Improve the general understanding of importance of balance between securing and sharing information in order to maximize USAF mission processes and minimize customer inefficiencies.

This objective can be explored by identifying information security and sharing issues by those with experience in the GeoBase program and relating them to recommended information security and sharing practices found in the literature review.

Answers to the following questions should help provide greater insight that will enhance the understanding of GeoBase and the securing and sharing of geospatial information.

Interview Questions:

SECTION 1: INTERVIEW INFO

1. Name:
2. Duty Title:
3. Are you involved with operating GeoBase servers?

SECTION 2: COMMAND BACKGROUND

1. What is your status on the completion of the Common Installation Picture (CIP)?
2. What Mission Data Sets (MDS) are you currently collecting / managing?
3. How far outside the installation boundary do you maintain as the extent of the Regional Information Picture (RIP)?
 - a. What data is included in your version of the RIP?
 - b. What data is important and would like to include? (wish list)
 - c. What is the source(s) of your RIP data?

SECTION 3: SECURITY

1. In your own words, what does “information security” mean to you in regards to the GeoBase program?
2. How do you currently control access to your current GeoBase data/applications?
3. Do you consider “need to know” before granting access to GeoBase information?
 - a. How do you make that determination?
4. In your own experience, what is the biggest information security issue with regards to GeoBase data and applications?
 - a. What steps are you currently taking to address this?
5. Do you or your office work with classified information?
 - a. How is classified information and unclassified information separated?
 - b. What are the expected security benefits of restricting access to the information?
6. What are the expected costs of restricting access to the information to either you or your customers?
7. What factors are considered for deciding the sensitivity of information?

ADMINISTRATIVE CONTROLS

1. Do you have a copy of your local security policy?
2. Are all AF GIS databases documented e.g. command has a central listing)?
3. What contractor hiring practices are employed to ensure security?
4. What type of security awareness training do users receive relating to geospatial information?
 - a. May I have a copy?
5. Who are your customers and how often do they use the GIS web server?
6. How do you identify the responsibilities of organizations that receive or add value to data, or of intermediaries such as contractors or host nations?
7. How are data restrictions enforced on these "downstream" users?
8. Is there a systematic review of policies (e.g. inspections)?
 - a. If so, how often is the program reviewed and by who?

LOGICAL / TECHNICAL CONTROLS

1. What methods are used to identify users who request access to restricted information?
2. How do you permit authorized users to access restricted information?
3. How do users access non-restricted information?
4. Do you log all accesses to the database?
 - a. Do you review the logs for any purposes?
5. How is change management handled (e.g. modifications to the database)?

PHYSICAL CONTROLS

1. Where do your servers reside?
 - a. Who maintains your servers?
2. Do you have a copy of your disaster recovery plan?
3. How do you recover from a catastrophic system failure? (Physical security - backup plans)
4. How do you recover from a partial system failure? (Physical security - backup plans)
5. Are there any screening measures in place to detect questionable data in the database?

SECTION 4: INFORMATION SHARING

1. Who do you share your information with? (Who depends on your information?)
2. Who do you depend on information from?
3. Have you encountered problems relating to information sharing?
 - a. If yes, what kind of problems?
 - b. How are you overcoming these problems?
4. How do you determine what information is acceptable for sharing?
5. When you share information, is anything expected in return?
6. What type (how many) designations of sensitive information can be applied to GeoBase information?

Is there anything else that you would like to add, which you feel is important to this subject?

Appendix E: Relative Laws & Executive Orders (1950 to Present)

LAW	PURPOSE - DESCRIPTION	YEAR
The Federal Records Act	"The Federal Records Act of 1950, as amended, establishes the framework for records management programs in Federal Agencies. As the primary agency for records management oversight, the National Archives and Records Administration (NARA) is responsible for assisting Federal agencies in maintaining adequate and proper documentation of policies and transactions of the Federal Government. This is done by appraising records (determining record value and final disposition of temporary or permanent records), regulating and approving the disposition of Federal records, operating Federal Records Centers and preserving permanent records. Federal records may not be destroyed-except in accordance with the procedures described in <u>Chapter 33 of Title 44</u>, United States Code. These procedures allow for records destruction only under the authority of a records disposition schedule approved by the Archivist of the United States. NARA issues a General Records Schedule (GRS) that gives record descriptions of records that are common to most Federal agencies and authorizes record disposals for temporary records. The Department is responsible for developing agency record schedules-with the approval of the Archivist of the United States-that are tailored to our own agency-specific records that are not provided for in the GRS. Record schedules are mandatory instructions of what to do with records (and nonrecord materials) no longer needed for current Government business. The records schedules indicate how long a document must be kept before it is transferred to a Federal Records Center, destroyed or transferred to NARA for permanent preservation. The Department's Records Management Program is responsible for ensuring that the legal, financial, evidentiary and historical transactions are recorded accurately and completely. We must document and preserve the historical and nationally important events that have taken place as a result of the Department's educational leadership and support. As the Department transitions from paper to e-government, we must capture and protect all forms of documentation in accordance with Federal laws and regulations relating to records management. We must provide and implement safeguards against the unlawful removal or loss of the Department's information. This is accomplished by using the GRS and the agency's NARA-approved records disposition schedules for records unique to this agency. Such a schedule ensure the systematic disposal of inactive records and the transfer of permanent records to the National Archives for permanent retention." (http://www.ed.gov/policy/gen/leg/fra.html)	1950
The Privacy Act	"The Privacy Act of 1974, 5 U.S.C. § 552a (2000), which has been in effect since September 27, 1975, can generally be characterized as an omnibus "code of fair information practices" that attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal executive branch agencies. However, the Act's imprecise language, limited legislative history, and somewhat outdated regulatory guidelines have rendered it a difficult statute to decipher and apply. Moreover, even after more than twenty-five years of administrative and judicial analysis, numerous Privacy Act issues remain unresolved or unexplored. Adding to these interpretational difficulties is the fact that many Privacy Act cases are unpublished district court decisions. A particular effort is made in this "Overview" to clarify the existing state of Privacy Act law while at the same time highlighting those controversial, unsettled areas where further litigation and case law development can be expected." http://www.usdoj.gov/foia/04_7_1.html http://www.usdoj.gov/foia/privstat.htm	1974

Executive Order 12356 (National Security Information)	"This Order prescribes a uniform system for classifying, declassifying, and safeguarding national security information. It recognizes that it is essential that the public be informed concerning the activities of its Government, but that the interests of the United States and its citizens require that certain information concerning the national defense and foreign relations be protected against unauthorized disclosure. Information may not be classified under this Order unless its disclosure reasonably could be expected to cause damage to the national security." (http://www.archives.gov/federal-register/codification/executive-order/12356.html)	1982
Computer Security Act of 1987	"Following OMB A-130, The Computer Security Act of 1987 developed standards and guidelines to assure [40 USC 0759]: • Cost-effective security • Privacy of sensitive information • Standards and guidelines are followed • Security plans are developed • Mandatory periodic training is conducted The Computer Security Act also provided a provision to allow agencies to waive mandatory FIPS. This waiver provision, in effect, significantly dampened the effectiveness of FIPS." (DIACAP, 2005) (http://www.cio.gov/archive/computer_security_act_jan_1998.html)	1987
The Stafford Act	"The Stafford Disaster Relief and Emergency Assistance Act (Stafford Act) (Public Law 100-707) is a United States federal law designed to bring an orderly and systemic means of federal natural disaster assistance for state and local governments in carrying out their responsibilities to aid citizens. The Stafford Act is a 1988 amended version of the Disaster Relief Act of 1974 (Public Law 93-288). It created the system in place today by which a Presidential Disaster Declaration of an emergency triggers financial and physical assistance through the Federal Emergency Management Agency (FEMA). The Act gives FEMA the responsibility for coordinating government wide relief efforts. The Federal Response Plan it implements includes the contributions of 28 federal agencies and non governmental organizations, such as the American Red Cross. In October 2000, Congress amended it again by passing the Disaster Mitigation Act of 2000 (Public Law 106-390)." (http://en.wikipedia.org/wiki/Stafford_Disaster_Relief_and_Emergency_Assistance_Act)	1988
The Government Performance and Results Act of 1993	"To provide for the establishment of strategic planning and performance measurement in the Federal Government, and for other purposes. Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, Purposes.-The purposes of this Act are to- (1) improve the confidence of the American people in the capability of the Federal Government, by systematically holding Federal agencies accountable for achieving program results; (2) initiate program performance reform with a series of pilot projects in setting program goals, measuring program performance against those goals, and reporting publicly on their progress; (3) improve Federal program effectiveness and public accountability by promoting a new focus on results, service quality, and customer satisfaction; (4) help Federal managers improve service delivery, by requiring that they	1993

	plan for meeting program objectives and by providing them with information about program results and service quality; (5) improve congressional decisionmaking by providing more objective information on achieving statutory objectives, and on the relative effectiveness and efficiency of Federal programs and spending; and (6) improve internal management of the Federal Government.” (http://www.whitehouse.gov/omb/mgmt-gpra/gplaw2m.html#h2)	
Executive Order 12829	“Ex. Ord. No. 12829, Jan. 6, 1993, 58 F.R. 3479, as amended by Ex. Ord. No. 12885, Dec. 14, 1993, 58 F.R. 65863, provided: This order establishes a National Industrial Security Program to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the United States Government. To promote our national interests, the United States Government issues contracts, licenses, and grants to nongovernment organizations. When these arrangements require access to classified information, the national security requires that this information be safeguarded in a manner equivalent to its protection within the executive branch of Government. The national security also requires that our industrial security program promote the economic and technological interests of the United States. Redundant, overlapping, or unnecessary requirements impede those interests. Therefore, the National Industrial Security Program shall serve as a single, integrated, cohesive industrial security program to protect classified information and to preserve our Nation's economic and technological interests.” (DIACAP, 2005) (http://www.archives.gov/isoo/policy-documents/eo-12829.html)	1993
Executive Order 12906 (Coordinating Geographic Data Acquisition and Access: The National Spatial Data Infrastructure)	“Geographic information is critical to promote economic development, improve our stewardship of natural resources, and protect the environment. Modern technology now permits improved acquisition, distribution, and utilization of geographic (or geospatial) data and mapping. The National Performance Review has recommended that the executive branch develop, in cooperation with State, local, and tribal governments, and the private sector, a coordinated National Spatial Data Infrastructure to support public and private sector applications of geospatial data in such areas as transportation, community development, agriculture, emergency response, environmental management, and information technology.” (http://www.fas.org/irp/offdocs/eo12906.htm)	1994
The Paperwork Reduction Act	“The purposes of this subchapter are to— (1) minimize the paperwork burden for individuals, small businesses, educational and nonprofit institutions, Federal contractors, State, local and tribal governments, and other persons resulting from the collection of information by or for the Federal Government; (2) ensure the greatest possible public benefit from and maximize the utility of information created, collected, maintained, used, shared and disseminated by or for the Federal Government; (3) coordinate, integrate, and to the extent practicable and appropriate, make uniform Federal information resources management policies and practices as a means to improve the productivity, efficiency, and effectiveness of Government programs, including the reduction of information collection burdens on the public and the improvement of service delivery to the public; (4) improve the quality and use of Federal information to strengthen decisionmaking, accountability, and openness in Government and society; (5) minimize the cost to the Federal Government of the creation, collection,	1995

	maintenance, use, dissemination, and disposition of information; (6) strengthen the partnership between the Federal Government and State, local, and tribal governments by minimizing the burden and maximizing the utility of information created, collected, maintained, used, disseminated, and retained by or for the Federal Government; (7) provide for the dissemination of public information on a timely basis, on equitable terms, and in a manner that promotes the utility of the information to the public and makes effective use of information technology; (8) ensure that the creation, collection, maintenance, use, dissemination, and disposition of information by or for the Federal Government is consistent with applicable laws, including laws relating to— (A) privacy and confidentiality, including section 552a of title 5; (B) security of information, including the Computer Security Act of 1987 (Public Law 100-235); and (C) access to information, including section 552 of title 5; (9) ensure the integrity, quality, and utility of the Federal statistical system; (10) ensure that information technology is acquired, used, and managed to improve performance of agency missions, including the reduction of information collection burdens on the public; and (11) improve the responsibility and accountability of the Office of Management and Budget and all other Federal agencies to Congress and to the public for implementing the information collection review process, information resources management, and related policies and guidelines established under this subchapter." http://www.archives.gov/federal-register/laws/paperwork-reduction/	
Executive Order 12951 (Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems)	This order prescribes a comprehensive and exclusive system for the public release of imagery acquired by space-based national intelligence reconnaissance systems. This order is the exclusive Executive order governing the public release of imagery for purposes of section 52(b)(1) of the Freedom of Information Act. Provides release for certain scientifically or environmentally useful imagery acquired by space-based national intelligence reconnaissance systems, consistent with the national security, it is hereby ordered as follows: Section 1. Public Release of Historical Intelligence Imagery. Imagery acquired by the space-based national intelligence reconnaissance systems known as the Corona, Argon, and Lanyard missions shall, within 18 months of the date of this order, be declassified and transferred to the National Archives and Records Administration with a copy sent to the United States Geological Survey of the Department of the Interior consistent with procedures approved by the Director of Central Intelligence and the Archivist of the United States. Upon transfer, such imagery shall be deemed declassified and shall be made available to the public. Section 2. Review for Future Public Release of Intelligence Imagery. (a) All information that meets the criteria in section 2(b) of this order shall be kept secret in the interests of national defense and foreign policy until deemed otherwise by the Director of Central Intelligence. In consultation with the Secretaries of State and Defense, the Director of Central Intelligence shall establish a comprehensive program for the periodic review of imagery from systems other than the Corona, Argon, and Lanyard missions, with the objective of making available to the public as much imagery as possible consistent with the interests of national defense and foreign policy. For imagery from obsolete broad-area film-return systems other than Corona, Argon, and Lanyard missions, this review shall be completed within 5 years of the date of this order. Review of imagery from any other system that the Director of Central	1995

	Intelligence deems to be obsolete shall be accomplished according to a timetable established by the Director of Central Intelligence. The Director of Central Intelligence shall report annually to the President on the implementation of this order. (http://www.fas.org/irp/offdocs/eo12951.htm)	
The National Technology Transfer and Advancement Act of 1995	"United States Public Law 104-113, was signed into law March 7, 1995. The Act amended several existing acts and mandated new directions for federal agencies with the purpose of: • bringing technology and industrial innovation to market more quickly • encouraging cooperative research and development between business and the Federal government by providing access to federal laboratories • making it easier for businesses to obtain exclusive licenses to technology and inventions that result from cooperative research with the Federal government The Act made a direct impact on the development of new industrial and technology standards by requiring that all Federal agencies use privately developed standards, particularly those developed by standards developing organizations." (http://en.wikipedia.org/wiki/National_Technology_Transfer_and_Advancement_Act)	1995
The Clinger-Cohen Act of 1996	Clinger-Cohen Act (CCA) of 1996 provides that the government information technology shop be operated exactly as an efficient and profitable business would be operated. Acquisition, planning and management of technology must be treated as a "capital investment." While the law is complex, all consumers of hardware and software in the Department should be aware of the Chief Information Officer's leadership in implementing this statute. CCA emphasizes an integrated framework of technology aimed at efficiently performing the business of the Department. Just as few businesses can turn a profit by allowing their employees to purchase anything they want to do any project they want, the Department also cannot operate efficiently with hardware and software systems purchased on an "impulse purchase" basis and installed without an overall plan. All facets of capital planning are taken into consideration just as they would be in private industry: • cost/benefit ratio • expected life of the technology • flexibility and possibilities for multiple uses (http://www.ed.gov/policy/gen/leg/cca.html)	1996
The Freedom of Information Act and the Electronic Freedom of Information Act Amendments of 1996	The Freedom of Information Act-⁽¹⁾ generally provides that any person has a right, enforceable in court, to obtain access to federal agency records, except to the extent that such records (or portions of them) are protected from public disclosure by one of nine exemptions or by one of three special law enforcement record exclusions. Enacted in 1966, and taking effect on July 4, 1967, the FOIA firmly established an effective statutory right of public access to executive branch information in the federal government. The principles of government openness and accountability underlying the FOIA, however, are inherent in the democratic ideal: "The basic purpose of [the] FOIA is to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed."⁽²⁾ The United States Supreme Court has emphasized that only "[o]fficial information that sheds light on an agency's performance of its statutory duties falls squarely within that statutory purpose." (http://www.usdoj.gov/oip/introduc.htm) http://www.usdoj.gov/04foia/04_7.html	1996

Rehabilitation Act, Sec. 508, Electronic and Information Technology	"Congress amended the Rehabilitation Act to require Federal agencies to make their electronic and information technology accessible to people with disabilities. Inaccessible technology interferes with an individual's ability to obtain and use information quickly and easily. Section 508 was enacted to eliminate barriers in information technology, to make available new opportunities for people with disabilities, and to encourage development of technologies that will help achieve these goals. The law applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology. Under Section 508 (29 U.S.C. ' 794d), agencies must give disabled employees and members of the public access to information that is comparable to the access available to others." http://www.section508.gov/index.cfm?FuseAction=Content&ID=3	1998
The Government Paperwork Elimination Act of 1999	"The Government Paperwork Elimination Act (GPEA, Pub. L. 105-277) requires that, when practicable, Federal agencies use electronic forms, electronic filing, and electronic signatures to conduct official business with the public by 2003. In doing this, agencies will create records with business, legal and, in some cases, historical value. This guidance focuses on records management issues involving records that have been created using electronic signature technology. It supplements the Office of Management and Budget (OMB) guidance for agencies implementing the GPEA, as well as other National Archives and Records Administration (NARA) guidance. This guidance discusses the records management principles that apply to electronic signature technology generally. Electronic signatures may be accomplished by several different technologies, such as Personal Identification Number (PIN), digital signatures, smart cards and biometrics. If additional technology-specific records management guidance is necessary, NARA will work with agencies to develop it." http://www.archives.gov/records-mgmt/policy/electronic-signature-technology.html	1999
USA PATRIOT Act	"H.R.3162: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (Enrolled as Agreed to or Passed by Both House and Senate) "An Act to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes." http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3162.ENR:	2001
Government Act of 2002	"Today I have signed into law H.R. 2458, the "E-Government Act of 2002." This legislation builds upon my Administration's expanding E-Government initiative by ensuring strong leadership of the information technology activities of Federal agencies, a comprehensive framework for information security standards and programs, and uniform safeguards to protect the confidentiality of information provided by the public for statistical purposes. The Act will also assist in expanding the use of the Internet and computer resources in order to deliver Government services, consistent with the reform principles I outlined on July 10, 2002, for a citizen-centered, results-oriented, and market-based Government. Title II of this Act authorizes agencies to award "share-in-savings" contracts under which contractors share in the savings achieved by agencies through the provision of technologies that improve or accelerate their work. The executive branch shall ensure, consistent with applicable law, that these contracts are operated according to sound fiscal policy and limit authorized waivers for funding of potential termination costs to appropriate circumstances, so as to minimize the financial risk to the Government. Title III of this Act is the Federal Information Security Management Act of 2002. It is very similar to title X of the Homeland Security Act of 2002, which also bears the name Federal Information Security Management Act of 2002 and which I signed into law on November 25, 2002. I am signing into law the E-Government Act after the enactment of the Homeland Security Act, and	2002

	there is no indication that the Congress intended the E-Government Act to provide interim provisions that would apply only until the Homeland Security Act took effect. Thus, notwithstanding the delayed effective dates applicable to the Homeland Security Act, the executive branch will construe the E-Government Act as permanently superseding the Homeland Security Act in those instances where both Acts prescribe different amendments to the same provisions of the United States Code. Finally, the executive branch shall construe and implement the Act in a manner consistent with the President's constitutional authorities to supervise the unitary executive branch and to protect sensitive national security, law enforcement, and foreign relations information. In particular, consistent with my constitutional authorities and section 301(c) of this Act, the executive branch shall construe the Act in a manner that preserves the authorities of the Secretary of Defense, the Director of Central Intelligence, and other agency heads with regard to the operation, control, and management of national security systems. GEORGE W. BUSH THE WHITE HOUSE, December 17, 2002" (http://www.whitehouse.gov/news/releases/2002/12/20021217-5.html) (http://www.whitehouse.gov/omb/egov/index.html)	
Federal Information Security Management Act of 2002 (Sec 3541 of title 44, US Code)	"The Federal Information Security Management Act of 2002 ("FISMA", 44 <u>U.S.C. § 3541</u>, <i>et seq.</i>) is a <u>United States federal law</u> enacted in 2002 as Title III of the <u>E-Government Act of 2002</u> (Pub.L. <u>107-347</u>, 116 <u>Stat.</u> 2899). The Act was meant to bolster computer and network security within the Federal Government and affiliated parties (such as <u>government contractors</u>) by mandating yearly <u>audits</u>. FISMA has brought attention to cybersecurity within the Federal Government, which had previously been much neglected. As of <u>February 2005</u>, many government agencies received extremely poor marks on the official report card, with an average of 67.3% for 2004, an improvement of only 2.3 percentage points over 2003.^[1] This shows a marginal increase in how federal agencies prioritize cybersecurity, but experts warn that this average must increase for the Government to truly protect itself." (http://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002)	2002
OMB Circular A-130 (on Management of Federal Information Resources)	"This Circular establishes policy for the management of Federal information resources. OMB includes procedural and analytic guidelines for implementing specific aspects of these policies as appendices." (http://www.whitehouse.gov/omb/circulars/a016/a016_rev.html)	2002
Homeland Security Act (HSA)	"This section establishes the Department of Homeland Security in the executive branch of the United States government and defines its primary missions and responsibilities. The primary missions of the department include preventing terrorist attacks within the United States, reducing the vulnerability of the United States to terrorism at home, and minimizing the damage and assisting in the recovery from any attacks that may occur. The Department's primary responsibilities correspond to the five major functions established by the bill within the Department: information analysis and infrastructure protection; chemical, biological, radiological, nuclear, and related countermeasures; border and transportation security; emergency preparedness and response; and coordination with other parts of the federal government, with state and local governments, and with the private sector. These primary missions and responsibilities are not exhaustive, and the Department will continue to carry out other functions of the agencies it will absorb." (http://www.whitehouse.gov/deptofhomeland/bill/)	2002
Executive Order 13356 (Strengthening the Sharing of Terrorism Information to	"in order to further strengthen the effective conduct of United States intelligence activities and protect the territory, people, and interests of the United States of America, including against terrorist attacks, it is hereby	2004

Protect Americans)	ordered as follows: Section 1. Policy. To the maximum extent consistent with applicable law, agencies shall, in the design and use of information systems and in the dissemination of information among agencies: (a) give the highest priority to (i) the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America, (ii) the interchange of terrorism information among agencies, (iii) the interchange of terrorism information between agencies and appropriate authorities of States and local governments, and (iv) the protection of the ability of agencies to acquire additional such information; and (b) protect the freedom, information privacy, and other legal rights of Americans in the conduct of activities implementing subsection (a)." (http://www.whitehouse.gov/news/releases/2004/08/20040827-4.html)	
Executive Order 13388 (Strengthening the Sharing of Terrorism Information to Protect Americans)	Revokes Executive Order 13356 and Section 1. Policy. (same as 13356) Sec. 2. Duties of Heads of Agencies Possessing or Acquiring Terrorism Information. Sec. 3. Preparing Terrorism Information for Maximum Distribution. Sec. 4. Requirements for Collection of Terrorism Information Inside the United States. Sec. 5. Establishment and Functions of Information Sharing Council. (http://www.fas.org/irp/offdocs/eo/eo-13388.htm) (http://www.whitehouse.gov/news/releases/2005/10/20051025-5.html)	2005
USA PATRIOT Improvement And Reauthorization Act Of 2005	This new legislation "allows intelligence and law enforcement officials to continue sharing information and using the same tools against terrorists already employed against drug dealers and other criminals. While safeguarding Americans' civil liberties, this legislation also strengthens the U.S. Department of Justice (DOJ) so that it can better detect and disrupt terrorist threats, and it also gives law enforcement new tools to combat threats. America still faces dangerous enemies, and no priority is more important to the President than protecting the American people without delay." (http://www.whitehouse.gov/news/releases/2006/03/20060309-4.html)	2006
Executive Order 13407 (Public Alert and Warning System)	"By the authority vested in me as President by the Constitution and the laws of the United States of America, including the Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended (42 U.S.C. 5121 et seq.), and the Homeland Security Act of 2002, as amended (6 U.S.C. 101 et seq.), it is hereby ordered as follows: Section 1. Policy. It is the policy of the United States to have an effective, reliable, integrated, flexible, and comprehensive system to alert and warn the American people in situations of war, terrorist attack, natural disaster, or other hazards to public safety and well-being (public alert and warning system), taking appropriate account of the functions, capabilities, and needs of the private sector and of all levels of government in our Federal system, and to ensure that under all conditions the President can communicate with the American people." (http://www.whitehouse.gov/news/releases/2006/06/20060626.html)	2006 (June)

Appendix F: Relative Policies and Guidance

Interim Department of Defense (DoD) Information Assurance (IA) Certification and Accreditation (C&A) Process Guidance (DIACAP)	6 Jul 2006
Guidance for Implementing Net-Centric Data Sharing (DoD 8320.02-G)	12 Apr 2006
Interim AMC GeoBase Information Security Policy	15 Sep 2005
USAF Installation Geospatial Information Security Policy	DRAFT
Installations and Logistics (IL) Data Access Policy	7 Feb 2005
AMC GeoBase Data Replication Policy	Oct 2004
Air Force Information and Data Management Strategy Policy	3 Mar 2004
DoD Directive 8500.1: Information Assurance (IA)	24 Oct 2002
USAF GeoBase Policy Memo	7 Oct 2002
DoD Directive 8100.1: Global Information Grid (GIG) Overarching Policy	19 Sep 2002
FGDC Policy on Access to Public Information and the Protection of Personal Information Privacy in Federal Geospatial Databases	Apr 1998
DoD Instruction 5200.40: DoD Information Technology Security Certification and Accreditation Process (DITSCAP) – <i>CANCELED, See DIACAP</i>	30 Dec 1997

Bibliography

- Australian Institute of Criminology 2006. Australian Crime: Facts and Figures 2005.
<http://www.aic.gov.au/stats/crime/cybercrime.html> ed. Canberra: Australian Institute
of Criminology, 2006. 15 Nov 06
<<http://www.aic.gov.au/stats/crime/cybercrime.html>>.
- Baker, John C., et al. Mapping the Risks: Assessing the Homeland Security Implications
of Publicly Available Geospatial Information. RAND National Defense Research
Institute, 2004.
- Barker, William C. Volume I: Guide for Mapping Types of Information and Information
Systems to Security Categories. Ed. Computer Security Division Information
Technology Laboratory National Institute of Standards and Technology. Vol. NIST
Special Publication 800-60. Gaithersburg, MD: Technology Administration U.S.
Department of Commerce, Jun 2004. <<http://csrc.nist.gov/publications/>>.
- Cullis, Brian J., Col., and Hal Tinsley Col. "One Installation, One Map." GeoIntelligence
(2004)
- Cullis, Brian J. "Geospatial Mandates Pave Way for DISDI." Military Geospatial
Technology Jul 26, 2005.
- Datta, Lois-ellin. Case Study Evaluations. Vol. GAO/PEMD-91-10.1.9. United States
General Accounting Office, Program Evaluation and Methodology Division, Nov
1990.
- Decker, Raymond J., and Brian J. Lepore. Homeland Security: Efforts to Improve
Information Sharing Need to be Strengthened. Trans. U.S. Government
Accountability Office. Washington D.C., Aug 2003.
- Defense Information Systems Agency (DISA). "Defense Information System Network
(DISN) Data Services." . 3 Nov 2006.
<<http://www.disa.mil/main/prodsol/data.html>>.
- Department of Defense. "DoD Common Access Card (CAC): Security Features." .
<<http://www.cac.mil/CardInfoSecurity.do>>.
- Dunn, Grover L. Installations and Logistics (IL) Data Access Policy. Vol.
Memorandum. Pentagon, Washington D.C.: HQ USAF/IL-CIO, 7 Feb 2005.

ESRI. "ArcIMS: Publish Maps, Data, and Metadata on the Web." ESRI. 21 Dec 2006. 11 Feb 2007 <<http://www.esri.com/software/arcgis/arcims/index.html>>.

Evans, Donald, Phillip J. Bond, and Bement, Arden L., Jr. Standards for Security Categorization of Federal Information and Information Systems. Ed. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology. Vol. FIPS PUB 199. Gaithersburg, MD: Department of Commerce, Feb 2004.

Federal Geographic Data Committee. Federal Geographic Data Committee 2005 Annual Report. Federal Geographic Data Committee (FGDC), 11 Aug 2006a.

---. Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns. National Spatial Data Infrastructure (NSDI), Jun 2005b.

Fuhr, Jordan. "Spatial Manager: Interview with Colonel Brian Cullis." Military Geospatial Technology Dec 21, 2004.

Geo InSight International, Inc. 3rd Civil Engineer Squadron Geospatial Information Strategic Plan. Vol. FEDSIM Contract No. DACW65-97-D-0063. PACAF, 1999.

Grance, Tim, et al. Security Guide for Interconnecting Information Technology Systems: Recommendations of the National Institute of Standards and Technology. Ed. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology. Vol. NIST Special Publication 800-47. Gaithersburg, MD: Department of Commerce, Aug 2002. <<http://csrc.nist.gov/publications/>>.

Hammer, Michael, and James Champy. Reengineering the Corporation: A Manifesto for Business Revolution. New York, NY: HarperBusiness Essentials, 2003.

Headquarters Air Force Geo Integration Office. Installation Mapping and Visualization Common Installation Picture Control Document. Pentagon: Headquarters Air Force Geo Integration Office (AF/A7CI)., March 2006a.

---. United States Air Force GeoBase Common Installation Picture Data Quality Assurance Plan Draft Version 1.0. Pentagon: Headquarters Air Force Geo Integration Office (AF/A7CI)., April 2006b.

Information Security Oversight Office. "2005 Report to the President." (2006a) . 19 Dec 2006 <<http://www.archives.gov/isoo/index.html>>.

- . "Classified National Security Information Directive no. 1 (32 CFR Parts 2001 and 2004 RIN 3095-AB18)." National Archives and Records Administration (NARA). 22 Sept 2003b. 7 Feb 2007 <<http://www.archives.gov/isoo/policy-documents/eo-12958-implementing-directive.html#2001.10>>.
- ISO/IEC 17799. Information Technology - Code of Practice for Information Security Management. First ed. Vol. ISO/IEC 17799:2000(E). Switzerland: SANS Institute, 2000.
- Lachman, Beth. Assessing the Impacts of Sharing Geospatial Data Assets Across the Department of Defense (DoD). 2006 Geospatial Technologies Symposium: RAND National Defense Research Institute, 2006.
- MacFarlane, Robert. A Guide to GIS Applications in Integrated Emergency Management. United Kingdom: Emergency Planning College, Cabinet Office, 30 Nov 2005.
- Matthews, William. "OMB Weighs Info Classification: Efforts to Protect some Public Data from Misuse are Generating a Mix of Reactions." Federal Computer Week 16 Sep 2002 2002: 14-15.
- Moseley, T. Michael, and Michael W. Wayne. SECAF/CSAF Letter to Airmen: Mission Statement. Washington D.C.: SECAF/CSAF, 7 Dec 2005. <<http://www.af.mil/pressreleases/release.asp?storyID=123013463>>.
- National Archives and Records Administration. "Records Management Guidance for Agencies Implementing Electronic Signature Technologies." Office of Records Services - Washington, DC, Modern Records Programs. Oct 18, 2000. The National Archives. <<http://www.archives.gov/records-mgmt/policy/electronic-signature-technology.html#1^0>>.
- Oliver, Mario. Investigation of GeoBase Implementation Issues: Case Study of Information Resource Management. AFIT:, Mar 2004.
- Onley, Dawn S. "DISA Official: Users should be Accountable for Security." Government Computer News 1.1 (25 April 2004) <www.gcn.com>.
- Powner, David, and Eileen Larence. Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information. Vol. GAO-06-385. Washington D.C.: U.S. Government Accountability Office, Mar 2006.

- Ross, Ron, et al. Recommended Security Controls for Federal Information Systems. Ed. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology. Vol. NIST Special Publication 800-53 (Revision 1). Gaithersburg, MD: Technology Administration U.S. Department of Commerce, Dec 2006. 24 Jan 07 <<http://csrc.nist.gov/publications/>>.
- Schomper, Charles R., and et al. Realizing the Potential of Information Resources: Information, Technology, and Services. Track 2: Policies and Standards. Vol. ED392336. Boulder, CO: CAUSE Exchange Library, 1996.
- Solomon, Michael G., Chapple, Mike. Information Security Illuminated. Sudbury, MA: Jones and Bertlett Publishers, 2005.
- Speed, Timothy, Juanita Ellis, and Steffano Korper. the Personal Internet Security Guidebook: Keeping Hackers and Crackers Out of Your Home. Academic Press, 2002.
- Stenbit, John P. Department of Defense Critical Infrastructure Protection (CIP) Security Classification Guide. Assistant Secretary of Defense, Command, Control, Communications and Intelligence (ASD(C3I), 2003.
- Swanson, Marianne, Joan Hash, and Pauline Bowen. Guide for Developing Security Plans for Federal Information Systems. Ed. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology. Vol. NIST Special Publication 800-18 Rev 1. Gaithersburg, MD: Technology Administration U.S. Department of Commerce, Feb 2006. <<http://csrc.nist.gov/publications/>>.
- Swanson, Marianne, et al. Guide for Information Security Program Assessments and System Reporting Form. Ed. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology. Vol. NIST Special Publication 800-26Rev 1. Gaithersburg, MD: Technology Administration U.S. Department of Commerce, Aug 2005. <<http://csrc.nist.gov/publications/>>.
- Thiagarajan, Val. Information Security Management Audit Check List for SANS. Ed. Algis Kibirkstis. 2003rd ed. Vol. BS 7799,2:2002 Audit Checklist. SANS Institute, 2003a. <http://www.sans.org/reading_room/?ref=3701>.
- . Information Security Management Audit Check List for SANS. Ed. Algis Kibirkstis. 2005th ed. Vol. BS 7799,2:2005 Audit Checklist. SANS Institute, 2005b. <http://www.sans.org/score/ISO_17799checklist2.php>.

Tombs, Bradley R. "Policy Review: Blocking Public Geospatial Data Access is Not Only a Homeland Security Risk." Urban and Regional Information Systems Association Journal 16.No. 2 (2005)

United States Air Force, Air Mobility Command. Interim AMC GeoBase Information Security Policy., 15 Sep 2005.

United States Department of Education. "Clinger-Cohen Act." Office of Information and Privacy and Office of Management and Budget (OMB). 15 Sept 2004. United States Department of Education. <<http://www.ed.gov/policy/gen/leg/cca.html>>.

United States Department of Justice. "Overview of the Privacy Act of 1974, 2004 Edition." Office of Information and Privacy and Office of Management and Budget (OMB). May 2004. United States Department of Justice. <<http://www.usdoj.gov/oip/1974intro.htm>>.

West, Christopher J. Development of a Theoretical Framework of Distributed Cognition Phenomena in Control Centers during Crisis Conditions. Doctor of Philosophy Old Dominion University, 2006.

Yin, Robert K. Case Study Research Design and Methods. Third Edition ed. Vol. 5. California: Sage, 2003.

Zettler, Michael E. USAF Geobase Policy Memo. Washington D.C.: HQ USAF/IL, 7 Oct 2002a.

---. USAF Installation Geospatial Information Security Policy [Draft Policy Memorandum]. Washington D.C.:, 2002b.

Vita

Major Scott A. Bryant graduated from Jersey Village High School in Houston, Texas. He entered undergraduate studies at Texas A&M University in College Station, Texas where he graduated with a Bachelor of Landscape Architecture (BLA) degree in May 1997 and was commissioned through Texas A&M's Corps of Cadets, AFROTC, Detachment 805.

His first assignment was at Davis-Monthan AFB, Arizona as a base level civil engineer working throughout the Engineering Flight of the 355th Civil Engineers Squadron, starting in June 1997. In June 2000, he was assigned to the 3rd Civil Engineers Squadron, Elmendorf AFB, Alaska where he served as the GeoBase Integration Officer, Deputy of Base Development, Chief of Maintenance Engineering, and Readiness Flight Commander. In June 2003, he was assigned to 7th Air Force Headquarters Civil Engineer Directorate (A7), Osan AB, Republic of Korea where he served two years as the Chief of Resources, Environment, and GeoBase. Following his overseas assignment, he entered the Graduate School of Engineering and Management, Air Force Institute of Technology, Wright-Patterson AFB, Ohio. Upon graduation in March 2007, he will be assigned the Air Force Material Command (AFMC) Headquarters.

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 074-0188	
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 02-23-2007		2. REPORT TYPE Master's Thesis		3. DATES COVERED (From – To) Aug 2005 – Mar 2007	
4. TITLE AND SUBTITLE Geospatial Informational Security risks and concerns of the U.S. Air Force GeoBase Program				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Bryant, Scott A., Major, USAF				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S) Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) 2950 Hobson Way, Building 640 WPAFB OH 45433-7765				8. PERFORMING ORGANIZATION REPORT NUMBER AFIT/GEM/ENV/07-M1	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) USAF GIS Support Center (USAF) Institute for Information Technology Applications 2354 Fairchild Dr, Suite 4K31 US Air Force Academy, CO 80840 POC: SMSgt Mark Barner email: mark.barner@usafa.af.mil Phone: (719) 333-0653 (DSN: 333-0653)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT Technological advancements such as Geospatial Information Systems (GIS) and the Internet have made it easier and affordable to share information, which enables complex and time sensitive decisions to be made with higher confidence. Further, advancements in information technology have dramatically increased the ability to store, manage, integrate, and correlate larger amounts of data to improve operational efficiency. However, the same technologies that enable increased productivity also provide increased capabilities to those wishing to do harm. Today's military leaders are faced with the challenge of deciding how to make geospatial information collected on military installations and organizations available to authorized communities of interest while simultaneously restricting access to protect operational security. Often, these decisions are made without understanding how the sharing of certain combinations of data may pose a significant risk to protecting critical information, infrastructure or resources. Information security has been an area of growing concern in the GeoBase community since, by definition, it is required to strike a balance between competing interests, each supported by federal policy: (1) the availability of data paid for by tax dollars and (2) the protection of data as required to mitigate risks. In this research we will explore the security implications of the US Air Force GeoBase (the US Air Force's applied Geospatial Information System) program. We examine the rapid expansion of the use of GeoBase to communities outside of the civil engineering field; examine the intrinsic and extrinsic security risks of the unconstrained sharing of geospatial information; explore difficulties encountered when attempting to rate the sensitivity of information, discuss new policies and procedures that have been implemented undertaken to protect the information, and propose technical and managerial control measures to facilitate sharing geospatial information sharing while minimizing the associated operational risks.					
15. SUBJECT TERMS US Air Force (USAF) GeoBase, Geospatial Information Systems (GIS) Information Security, Sharing, GIS OPSEC, INFOSEC, Risk Management, Critical Infrastructure, Knowledge Management, Data Discoverability					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 148	19a. NAME OF RESPONSIBLE PERSON MICHAEL R. GRIMAILA, Ph.D.
REPORT U	ABSTRACT U	c. THIS PAGE U			19b. TELEPHONE NUMBER (Include area code) (937) 255-6565, ext 4800