Low Risk, High Threat, Open Access Security in a Post 9-11 World: A study of the Smithsonian Institution's Office of Protection Services

Sonny Smith

A dissertation submitted
to the faculty of Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
In
Public Administration

Anne Khademian (Chair)
James Wolf
Patrick Roberts
Randall Murch

May 27, 2009
Alexandria, VA

Keywords: low risk, high threat, open access, terrorism, protection services, security screening, public institutions, The Smithsonian Institution

Low Risk, High Threat, Open Access Security in a Post 9-11 World: A study of the Smithsonian Institution's Office of Protection Services

Sonny Smith

ABSTRACT

The events of 9-11 resulted in a slew of policy, procedural, and organizational changes within many government departments as the U.S. government took many steps to enhance security to prevent future terrorist attacks. The emphasis on high threat targets by the Department of Homeland Security (DHS) and other government agencies, such as the White House, the Capitol and Congressional office buildings, major infrastructure and facilities within US cities, airline travel, ports and economic supply chains has generated a great deal of debate and attention. There are however, targets that are considered low risk situated in high threat areas that also provide open access to the public for which security professionals are responsible that should not be overlooked during the War on Terror. The question is how low risk targets in high threat areas should be protected? What resource distribution makes sense? What practices should be applied to achieve security?

The purpose of this research is to look at one of these targets, the Smithsonian Institution and how the Smithsonian Institution's Office of Protection Services (SI OPS) responded to the terror attacks of 9-11 and the ongoing threat. Four factors will be examined: (1) the screening process, (2) the budget, (3) the security policy formulation process, and (4) training.

The study focus is based on data derived from semi-structured interviews and a review of SI documents. Examining post 9-11 security changes allows one to see how SI OPS has evolved in its attempt to meet both internal security demands and expectations

against an external security concern. The findings reveal SI OPS initially underwent significant changes within the four factors in the three years following the attacks of 9-11. However, limited resources and manpower strains have played major roles in the subsequent decline in some of the factors after their initial increases.

Although a return to the security levels immediately following 9-11 may not be imminent, it is recommended that OPS management make stronger efforts to communicate with non-security managers and return to more stringent visitor screening procedures.

To Kim, Izzy, and Sophie,
for your love, support, and ability to make me smile –
I would be lost without you.

ACKNOWLEDGEMENTS

My heartfelt thanks go to Dr. Anne Khademian, my Advisor, Mentor, and Committee Chair, who guided me with intelligence and expertise which, with each meeting, shed more light on my dissertation path. With persistence and a lot of patience, she challenged me to learn, question, think, experiment, and critically analyze. She made this a wonderful learning experience for me.

My sincere thanks to Dr.'s Jim Wolf, Randy Murch, and Patrick Roberts, each of whom contributed important and unique perspectives throughout this research process. Their advice and feedback has been more helpful than they may realize. As a collective, the committee members added value to the dissertation and I would not have made it to this point without them.

I want to thank Dr.'s John Rohr and Gary Wamsley for encouraging me to pursue my Ph.D. and for all of their sage advice during my MPA and early Ph.D. studies.

I am very grateful to Bob Maier, Tom Heath, and David Duh for helping to make my life tolerable during my formative years at Christian Brothers Academy. They worked tirelessly to instill in me (sometimes beat into me!) a love and appreciation of learning, and who imparted in me the importance of courage and the drive to go after my dreams through the good and bad times.

Special Thanks to JJ, Doug, and James at the Smithsonian Office of Protection Services, who patiently worked with me to gather all the data and schedule the interviews that have made this dissertation possible.

For Gil and Polly Bartlett, who provided me so much support during some really lean years when I was struggling to find out who I really was. I'm still searching by the way…

And to Kim, Izzy and Sophie – boy has my life changed with you three in it!!!

TABLE OF CONTENTS

TABLES

FIGURES

CHAPTER 1

Introduction

How does an organization that is a low risk target for a terrorist attack located in a high threat setting that provides open access to the public adjust to the increased threat of terrorist attacks, and what can we learn from studying such an organization in order to inform the ongoing debate and efforts to improve security? This research addresses this question by examining how the Smithsonian Institution's (SI) Office of Protection Services (OPS) Uniformed Security Division responded as an organization to the terror attacks of 9-11 and the ongoing threat. Punctuated Equilibrium Theory (PET) will be the lens used to look at the response by SI OPS. This research is not intended to provide a major theoretical advancement of PET; rather PET provides a means to understand the post 9-11 changes implemented by SI OPS. The findings drawn from an examination of the policy, budgetary, and security enforcement changes within SI OPS will be the basis for recommendations for improving security in similarly situated organizations. It will also provide a perspective of where OPS is heading, and ways its managers might improve security given their constraints and the mission and culture of the SI, the view of the Congress, and the changing perspectives of the broader community of security professionals.

Change and Crisis

Policy and organizational change is typical in the wake of a crisis that hits a government agency or impacts an entire government. The events of 9-11 resulted in a slew of policy, procedural, and organizational changes within many governmental

departments as the U.S. government took many steps to enhance security to prevent future terrorist attacks. The emphasis on high risk targets by the Department of Homeland Security (DHS) and other government agencies, such as the White House, the Capitol and Congressional office buildings, major infrastructure and facilities within US cities, airline travel, ports and economic supply chains has generated a great deal of debate and attention: What constitutes a high risk target? What steps should be taken to reduce the risk for these targets? How much money should be spent on high-risk targets?

There has not been, however, much discussion within the academic literature about low risk targets; more specifically, the protection of low risk targets in high threat areas that provide open access to the public, such as the Smithsonian Institution, the National Zoo, and the Museum of Modern Art in New York City to name a few. The primary issues not being addressed revolve around topics such as: how should they prepare or train their security forces to detect or deter potential terror threats; which aspects of security should be emphasized in lieu of others; and how much should be spent to address these issues. This failure to disaggregate between institutions of varying degrees of risks and where they are located presents an opportunity to study one of the aforementioned institutions, SI OPS, in an effort to explore its reaction to the events of 9-11. An investigation of SI OPS provides an opportunity to explore whether and how well low risk targets respond to the threat of terrorism, as well as to study the types of hurdles such organizations have to overcome in their quest to enhance post 9-11 security structure. The punctuated equilibrium framework provides a means to examine the change practices and the extent/implications of those practices. The specifics of this exploration will focus on changes to the budget, screening policies, training, and the

managerial policy and planning processes of SI OPS and on the manner these areas changed.

The literature shows that there have been budgetary changes aimed at high risk targets (Capitol, FBI HQ, US Secret Service HQ, etc), but there has been little discussion about the potential low risk targets that reside in high threat areas. They do not appear to have received enough Congressional, professional security community or academic discussion. These sites still have security and anti terror interests that must be addressed in the post 9-11 era.

Window of Opportunity

According to Birkland, the 9-11 attacks opened a short "window of opportunity"[1] (Birkland, 2004) for policy and organizational learning within federal agencies in the United States. Birkland notes the opportunity for these changes is short, however, due to two key factors: first, the initial enthusiasm within the media and policy makers is likely to be short-lived, even for important events such as September 11. Second, "easy solutions" are generally adopted in an effort to do something after the event and more controversial ideas become more difficult to implement because the urgency within the policy environment wanes as opponents to new policies argue that the initial solutions need time to work (342).

The U.S. government took advantage of this short window described by Birkland, and used the year immediately following the events of 9-11 to introduce sweeping policy, organizational, and fiscal changes across many areas. Other studies and works (Bush,

[1] This term was first introduced by John Kingdon in his book *Agendas, Alternatives, and Public Policies* (1984). Kingdon, however, used the term "policy windows." Birkland's and Kingdon's definitions could be used interchangeably, as they were both used to express the short opportunity for policy change following an event.

2002; Delattre, 2002) also point out the drastic shift of the country and the sense of urgency and hurry to change the federal regulations and mandates to protect the country against terrorism. The primary entities impacted by this rash of new laws were the many federal, state, and local law enforcement agencies throughout the United States. From September 11, 2001 to January 2005, a number of public laws were enacted by the federal government to address various issues related to domestic terrorism. These can be found in Appendix I.

Policy Changes in High Threat Areas

As previously noted, the primary purpose of this dissertation is a focus on issues and policies affecting low risk facilities especially those residing in high threat areas. The purpose of this section is to provide a backdrop on those policies representing changes in areas targeting high risk entities. Some of these policies are not germane to this study; however they are used to show the scope of policy changes that took place following 9-11.

In November 2001, there were ten bills introduced in The Maritime Transportation Security Act of 2002 that directly focused on port and maritime security issues to address transportation system attacks. Among the proposals were bills that would require the following:

- Inspection of all cargo entering the United States;
- Establishment of a new government agency to coordinate domestic transportation modes during national emergencies; and
- Passage of a new, permanent 96-hour notice of arrival requirements for vessel operations.

In addition to the Maritime Transportation Security Act of 2002, Senate Bill S 1214, which was being considered prior to the 9-11 attack and originally focused primarily on cargo theft issues and included development of port security plans, grants and loan guarantees for port security projects was also introduced (*Report of Committee on Commerce, Science, and Transportation on S. 1214*, 2001). It also related to the purchase of screening and detection equipment for the U.S. Customs Service. After 9-11, however, the bill was substantially revised. In the aftermath, the bill, passed in December 2001, now focused on broader port security issues (Emersen & Nadeau, 2003). These included requirements for new cargo documentation and passenger and crew manifest information. Of the greatest importance was the bill's requirement that mandated employers (e.g., port authority, marine terminal operation, ocean shipping intermediary, an ocean carrier, etc.) be prohibited from hiring individuals that failed to meet certain criteria for security-sensitive positions. This could include (but was not limited to) criminal background checks. Not only were maritime employers now required to run such employee checks, but they were also required to pay fees for any investigative efforts in this respect as well.

Aviation security was also drastically changed as a result of 9-11, which was a result of the passage of the Aviation and Transportation Security Act. This law, which began as S 1447 was passed on November 16, 2001 and signed into law on November 19, 2001. Before the attacks, this type of security was the responsibility of the Federal Aviation Administration within the Department of Transportation (DOT). But glaring inadequacies were identified with this type of security management structure after the attacks. For example, there were inadequate screening procedures relating to airline

passengers and their carry-on bags, inadequate controls for limiting access to the more secure airport areas, and poor security measures in place for air traffic control computer systems and facilities (GAO, 2003).

The primary purpose of this new law was to secure the aviation industry through the federalization of its employees and by placing greater emphasis on the screening of baggage and passengers by promoting training and performance standards for the new federal security screeners. Section 108 of the new law required all areas of aviation security be under federal supervision, while section 110 required all check baggage be screened using x-ray technologies, as well as explosive detection devices.

As security management procedures and legislative initiatives specifically focused on aviation attacks, other issues and concerns have also assumed significantly greater urgency. A number of important security management procedures and legislation have been enacted as a result. Some of the federal agencies that are responsible for transportation security were transferred to the new Department of Homeland Security (DHS), for example. DHS merged 22 federal agencies together and was dedicated to homeland security enforcement issues, as well as science and technology, infrastructure protection, preparedness, prevention, response, and recovery (DHS Strategic Plan, 2004). The new Department's strategic goals called for:

1. Awareness: identify and understand threats, assess vulnerabilities, determine potential impacts and disseminate timely information to our homeland security partners and the American public.
2. Prevention: Detect, deter and mitigate threats to our homeland.
3. Protection: Safeguard our people and their freedoms, critical infrastructure, property and the economy of our nation from acts of terrorism, natural disasters, or other emergencies.
4. Response: Lead, manage and coordinate the national response to acts of terrorism, natural disasters, or other emergencies.

5. Recovery: Lead national, state, local and private sector efforts to restore services and rebuild communities after acts of terrorism, natural disasters, or other emergencies.
6. Service: Serve the public effectively by facilitating lawful trade, travel and immigration.
7. Organizational Excellence: Value our most important resource, our people. Create a culture that promotes a common identity, innovation, mutual respect, accountability and teamwork to achieve efficiency, effectiveness and operational synergies (Securing Our Homeland, 2004:9).

As part of the Department the Transportation Security Administration (TSA) was now responsible for all transportation security management, it too, was required to address a number of new major challenges. The United States General Accounting Office (GAO, 2003) details these changes:

> By the end of December 2002, the agency had hired and deployed a workforce of over 60,000, including passenger and baggage screeners and federal air marshals, and was screening about 90 percent of all checked baggage for explosives…local mass transit agencies have assessed vulnerabilities, increased training for emergency preparedness, and conducted emergency drills... The Coast Guard has also performed initial risk assessments of ports, established new security guidelines, and initiated a comprehensive assessment of security conditions at 55 U.S. ports (1).

The USA PATRIOT Act was also passed to enhance the capacity of law enforcement agencies, in particular, to fight terrorism by removing barriers in data collection used for espionage and law enforcement, among other things (U.S. PATRIOT Act, HR 3162 RDS, 2001). The formal name of the Act is "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act." Its purpose is to restrain and punish terrorist acts in the United States and to enhance law enforcement investigatory tools. This legislation gave the Attorney General significantly more power to find, detain and prosecute foreigners that he suspected of having ties to terrorism. According to the PATRIOT Act, the Attorney General can now

authorize the arrest a foreigner if he has a "reasonable ground to believe that a non-citizen is either engaged in terrorist activity or other activity that endangers the national security (Bartley, 2001, A19)."

Thus the Act essentially seeks to close American borders to foreign terrorists and detain and remove terrorists within the country. In addition, the Act gives federal officials greater authority to track and intercept communications for both law enforcement and foreign intelligence gathering. Also, the new bill has provided the Treasury Department with regulatory powers against American financial institutions with respect to foreign money laundering by specifically defining procedures, crimes, and penalties for use of such funds against both domestic and international terrorists (Doyle, 2002).

The scope of the U.S. PATRIOT Act included (but was not limited) to the following: Enhancing domestic surveillance and security; deterring international money laundering, currency crimes, border control, enhancing immigration protection, strengthening laws against terrorism in general, and addressing the bank secrecy act. Of interest is the fact that the PATRIOT Act was passed six weeks after it was introduced, making it one of the most significant pieces of congressional legislation passed in such a short period of time. Such emergency measures soon became the norm in the federal government's attempts to address what was perceived to be extraordinary circumstances that threaten national security (Doyle, 2002). Finally, the post of Director of National Intelligence was established to enhance the sharing of information and collaboration across the intelligence community (Intelligence Reform and Terrorism Prevention Act of 2004). These changes mark only a few of the many that have been implemented since the events of 9-11.

Congressional Budget Office figures outline the new role and efforts of the government since 9-11 in terms of billions of dollars that have been and continue to be spent by the United States government on efforts to overcome the new, diverse and changing terrorist challenges. Table 1 on the following page illustrates the federal funding information for homeland security and combating terrorism for the years 2001-2006, respectively. Figures are presented in terms of billions of dollars.

As indicated in the table listing, authorized funding in all areas (i.e., annual appropriates, emergency supplemental appropriations, and discretionary spending) have significantly increased over the time period. Specifically, annual appropriations for security management efforts have more than doubled since 2001 (In 2001, the amount was $20.7 billion versus $49.7 billion in the fiscal year 2006). Spending more than doubled for emergency supplemental appropriations between the fiscal years of 2001 and 2002.

Table 1 - Federal Funding for Homeland Security and Combating Terrorism by Year (Budget Authority in Billions of Dollars*)

	2001	2002	2003	2004	Estimated 2005 [a]	Requested 2006[a]
Discretionary Budget Authority						
Regular appropriations	15.0	17.1	32.2	36.5	43.0	42.2
Supplemental appropriations	3.6	12.3	5.9	0.1	0.6	0
Fee-funded activities	0.7	2.0	2.6	3.2	3.3	5.4
Mandatory Spending	1.5	1.7	1.8	1.9	2.2	2.2
Gross Budget Authority [b]	20.7	33.0	42.5	41.7	49.1	49.7

Sources: Congressional Budget Office; Office of Management and Budget.

Note: Components may not sum to totals because of rounding. All years referred to are fiscal years.

a. The figures in this brief differ slightly from those published by the Office of Management and Budget as part of the Administration's 2006 budget request because CBO used different estimates of spending for mandatory and fee-funded activities.

b. Excludes offsetting collections and receipts, which are recorded as negative budget authority. (For 2004, those totaled $5.0 billion. For 2005, according to CBO's estimates, they will total $5.3 billion.)

*Source: Economic and Budget Issue Brief (2005), Congressional Budget Office Total Federal Resources Allocated for Homeland Security, 2001-2006.

Other security management efforts of the government have also been documented in financial terms. According to Childress (2002), the Homeland Security Budget for 2003 proposed $11 billion for a variety of programs focused on tracking the entry and exits of non-American citizens to and from the United State. Four specific policy initiatives were included in this cost. The most important of these in the context of this study was securing America's borders.

What does this mean?

The broader government response, as has been outlined, resulted in substantial changes in organizations, budgets, and policy after 9-11, particularly among those organizations on the front lines of security and those deemed at high threat for attack.

Despite these changes, what became evident was the government was not able to ensure high security for every aspect and facility of the government throughout the entire country due to budget and manpower requirements. Therefore, there was a need to prioritize sites based on potential risks. Delattre (2002) addressed this dilemma and noted, "We need as a people to face hard questions: Which hazards of terrorism must we learn to live with? What civic responsibility do we have in light of 9-11? Since we cannot prevent the execution of every terrorist plot, but we are determined to go on with our lives, what forms of vigilance most befit us? What are the realistic expectations and reasonable hopes with respect to terrorist attack? (4)."

Because of this inability to address all of these nationwide facilities, risk assessments must be performed and security efforts must be focused towards those high threat facilities such as the Pentagon, the Capitol Building, and FBI Headquarters, to name just a few. The resulting question is: what kind of response do we see from low risk targets in high threat settings and what can we learn about those responses in order to better allocate homeland security resources and management initiatives?

An Introduction to Punctuated Equilibrium Theory

What the above sections outline is the U.S. government's efforts to implement a series of laws, financial outlays and manpower increases within a relatively short period of time to address the fallout from and prevent another 9-11. A number of these dynamic changes can be examined through the lens of PET as it applies to organizations and policy areas. The three basic elements of PET that are studied regarding this research are deep structures, equilibrium periods, and revolutionary periods. Deep structure is the "set of fundamental choices a system has made of (1) the basic parts into which its units will

be organized and (2) the basic activity patterns that will maintain its existence (Gersick, 1991:14). In equilibrium periods, organizational structures and activity patterns are maintained. Small incremental adjustments are made to adjust for environmental changes without affecting the deep structure. Revolutionary periods occur in response to crises that undo an organization's deep structure until the revolutionary period ends and choices are made about forming a new structure (Gersick, 1991). This is because organizations change and adapt to their environment incrementally, but punctuation can prompt the organization to realign more dramatically with changes in the environment --or mesh the organization within its environmental context.

PET provides a framework for analyzing the changes associated with an organizational shock. Specifically, a shock will produce nonincremental changes (in quantity and quality, in other words, training for example, is extended and the types of training activities are new, etc) and then the changes will track again toward incrementalism. The analysis of SI OPS will show that changes did take place after 9-11 and then settled back into an incremental mode, and it will also show that the re-tracking is not the result of complacency, as the literature suggests, but the result of institutional, resource, and political dynamics—the security personnel have wanted to sustain or increase the focus in the four areas, but other dynamics prevailed, which will be outlined in the following chapters.

Why OPS?

SI OPS[2] is being used for this study for two primary reasons. First, SI is located in a high threat area, The National Mall in Washington, DC. This is coupled with the fact

[2] A distinction should be made between SI and SI OPS. SI is the organization, while SI OPS is an office within SI that is responsible for SI's overall security efforts. This focus of this research is on SI OPS.

that there has been no evidence found to suggest it to be a high risk site. Secondly, SI must balance its role as a public institution which thrives on allowing virtually unfettered public access, with maintenance of a security force that is placed under greater demands to provide a safe environment for all employees, visitors, and the cultural objects housed within its buildings. This dichotomy presents an opportunity to examine how security agencies or other agencies with a mission to protect national assets as well as the public were particularly challenged by 9-11. This study provides an opportunity to address the complacency debate surrounding acts of terror and government responses. This is important to the overall study because some literature has shown (Harowitz, 2001; Cook, 2005; Green, 2008) that complacency following an attack often times leads to vulnerabilities going unaddressed.

It is also important to begin a dialogue on institutions under similar security and geographic environmental conditions as SI, such as the Museum of Modern Art (MOMA), the National Gallery of Art in Washington, DC, and the Bronx Zoo, which are present in virtually all major metropolitan areas. They are all low risk sites that are located in high threat environments. They are also unique in that they allow almost unfettered public access into their facilities, as well. It could also be argued that the United States is a zero risk tolerant nation in which the outcome of an attack on SI, MOMA, or any other public institution could be just as important and traumatic, as an attack on, say an icon such as the U.S. Capitol Building. An attack on SI would be very likely unexpected, it would be a "soft" target and lots of innocent lives – families, scholars, children, and visitors from other countries--would be affected. Also historical and cultural treasures would be lost. In the end, the results of an attack would lead to a

lack of confidence in the security efforts of our government and the departments entrusted to protecting the citizenry and its treasures.

Overview of Chapters

The remaining chapters in this dissertation are arranged as follows. Chapter Two provides a comprehensive literature review of security management and homeland security issues. Chapter Three provides a history of the Smithsonian Institution's Office of Protection Services (SI OPS) to include an emphasis on the Uniformed Guard Force following the events of 9-11. Chapter Four outlines the study methodology, which includes a review of the interview questions and the four factors reviewed for the study. Chapter Five presents the variables and results of the study. Chapter Six provides a summary and discussion of the findings presented in chapter five. Lastly, Chapter Seven provides conclusions, the studies implications, as well as identifies possible future research.

Table 2 - Definition of Terms

Deep Structure – the set of fundamental 'choices' a system has made of (1) the basic parts into which its units will be organized and (2) the basic activity patterns that will maintain existence (Gersick, 1991:14).
Emergency Management – the organization and management of resources and responsibilities for dealing with all aspects of emergencies, in particularly preparedness, response and rehabilitation (International Strategy for Disaster Reduction, 2004).
Equilibrium Periods – characterized by the maintenance of organizational structures and activity patterns, where small incremental adjustments are made to adjust for environmental changes without affecting the deep structure (Gersick, 1991).
Knock-on effect - A secondary, often unintended effect.

Manager – SI OPS has a security manager for each SI facility. That manager is responsible for all security personnel and the implementation of all security policies for that particular facility.

Protect - shield from danger, injury, destruction, or damage (WordNet Search: Version 3.0, 2008).

Punctuated Equilibrium Theory – patterns of change in groups and organizations where periods of "stasis" are punctuated by brief and intense periods of "radical" change (Gersick, 1991).

Risk – the possibility of loss resulting from a threat, security incident, or event (General Security Risk Assessment Guideline, 2003).

Revolutionary Periods – occur due to significant changes in the environment that lead to wholesale upheaval where a system's deep structure comes apart, leaving it in disarray until the period ends and choices are made around which a new structure forms (Gersick, 1991).

Risk Assessment – the process of assessing security-related risks from internal and external threats to an entity, its assets, or personnel (General Security Risk Assessment Guideline, 2003).

Security - the protection of a person, property or organization from an attack (Kurtus, 2002).

Terrorism - violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or any state, or that would be a criminal violation if committed within the jurisdiction of the United States or any state. These acts appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by assassination or kidnapping (FBI).

Weapons of Mass Destruction (WMD) – weapons that are capable of a high order of destruction and/or of being used in such a manner as to destroy large numbers of people. Weapons of mass destruction can be high explosives or nuclear, biological, chemical, and radiological weapons, but exclude the means of transporting or propelling the weapon where such means is a separable and divisible part of the weapon (Department of Defense Dictionary of Military and Associated Terms, 2001).

CHAPTER 2

Literature Review

Introduction and overview

The primary focus of this chapter is to review the literature relevant for examining the security challenges of publicly accessible organizations that are low risk targets in high threat areas. Specifically, the chapter examines pre and post 9-11 security issues of management, threats, role of government, and budgetary issues.

The Pre 9-11 Security Environment

In order to compare the security environment in the U.S. before and after September 11, 2001, this section and the subsequent one focus on five key themes, which are identified on the basis of the literature in this area: 1) the nature of security threats; 2) the nature and role of risk management; 3) the role of government; 4) specific security measures and 5) issues and challenges. The pre 9-11 security literature focused mainly on disaster management and emergency management, with prominent themes including the government's role in response efforts, and consideration of what mitigation measures might be taken to prevent or lessen the effects of manmade disasters. Many of the issues addressed cut across both main categories of literature, since the primary aim of emergency and security management personnel, as well as that of disaster planning personnel is to deter the loss of life and property from manmade disasters.

Nature of Threats

The perceived nature of threats in the pre 9-11 security environment can be inferred from the nature of policies, legislation and operational practice at this time. The main focus of these by far was on emergency and disaster management in the context of

natural hazards such as earthquakes and floods. Since the mid-1990s, however, there was, at least on the part of the federal government, a growing recognition of the threat of terrorist attacks on the U.S., as reflected in its efforts to prepare the country for various types of terrorist activity (Falkenrath, 2001), especially those involving biological and chemical weapons. As this researcher explained:

> Collectively known as the "U.S. domestic preparedness program," this effort involves multiple federal agencies and a variety of initiatives. The budget of the federal weapons of mass destruction (WMD) preparedness program grew from effectively zero in fiscal year 1995 to approximately $1.5 billion in FY 2000, making this one of the fastest growing federal programs of the late 1990s (Falkenrath, 2001: 147).

Nature of Security Management

Much of the pre 2001 literature on security management was grounded in classical organizational behavior theory and had a strong emphasis on the scientific management paradigms espoused by theorists such as Frederick Taylor (1911), Frank and Lillian Gilbreth (Price, 1990), and Henri Fayol (1911). These viewed organizations as having vertical or hierarchical structures, with Corporate Management on the top, followed by Senior Management, Operational Management, and then Staff (2002: 4). These paradigms generally reflected the traditional structure of security management functions, which were operated from the top-down with relatively little interaction or integration with external bodies such as the emergency services (or on advice, expertise and experience from the bottom up).

This type of traditional organizational structure in security management, which failed to promote communication and co-ordination with external agencies, may have

contributed to the observed tendency for traditional security management to evolve only in response to the experience of dealing with incidents in practice (and after the fact), rather than being a forward-looking specialization. As Waugh (2000) observed, even the U.S. emergency management system evolved mainly in response to specific major disasters, and policies and programs in this area were generally "instituted and implemented in the aftermath of a disaster, based almost solely on that disaster experience, and with little investment in capacity building to deal with the next disaster." Rosenthal (1988) also observed that virtually all disaster policies are oriented to the past instead of focused on the future, and are therefore erroneously grounded in facts which may actually be irrelevant to future situations: "Disaster scenarios usually do not reach beyond extrapolations of the most recent calamity, thus imposing incremental solutions upon a typically non-incremental context (1988: 294)."

The need for forethought as espoused by Rosenthal is also expressed in some security management literature. According to Faye (2002), disaster mitigation challenges are contingent upon management's ability to predict, quantify, and control threats or potential threats, and the ability to adapt to these threat risks is the security leader's highest mark of excellence. Regarding this Faye notes, "To predict, which is restricted by the limitations of human understanding and available technology, is to identify the nature of the threat; to quantify is to measure uncertainty through the application of science and experience; and to control risk is to manage resources logically and flexibly (2002: 16)." Despite Faye's proclamation, the security and budgetary demands (which are outlined in previous and future chapters) have made if difficult for OPS executives to be as flexible with their resources as they would like.

The Role of Government

As noted by Rubin (2004), government has traditionally used both direct and indirect means of encouraging states and local areas to take steps to prepare for emergencies and disasters. However the actual influence of federal government on the development of such plans in the pre 9-11 era was relatively limited and its role in the whole process was a fairly passive one, as illustrated by the examples given in the following section. Although states were required to take certain steps by law or under particular program requirements to develop disaster mitigation plans, very little guidance was provided to the states government on how to go about preparing these plans and risk assessments, so the national situation with regard to disaster management was relatively decentralized and uncoordinated.

Specific Measures

As Rubin (2004) points out, states have been required to prepare Hazard Mitigation Plans since 1974 (Public Law 93-288) and under the 1988 Stafford Act (Public Law 100-707), and since 2000, there has been a requirement for these plans to include a risk assessment component, under the provision of the Disaster Mitigation Act of 2000 (Public Law 106-390). The federal government has also used indirect means to encourage state and local governments to take mitigative actions, for example in the form of requirements which underpin federal funding of initiatives such as The National Dam Safety Program, the National Flood Insurance Program, and the National Earthquake Hazards Reduction Program. From the mid-1990s, when the threat of terrorism became more apparent, federal funds and grants were made available to states in order to assist them to obtain equipment and facilities in order to prepare them to be better equipped to

deal with disasters, including terrorist attacks, or to deal with their impact (Rubin, 2004), but the take-up of these was voluntary.

Difficulties and Challenges

The main challenges facing security and emergency managers in the pre 9-11 era were primarily related to the difficulties prioritizing risks in order to secure or allocate adequate funding. It was noted by Waugh (2000) that, "The biggest problems for emergency managers are less technical than they are the obvious difficulties of gaining and maintaining political and economic support for mitigation efforts (2000: 156)." These issues gave rise to the need for management to perform cost-benefit analyses in order to determine which specified risks should therefore receive support. McCrie (2001) suggested that a range of options should be evaluated for their pertinence to a given situation, so that "at one end, controls are absent and risks for loss are high. At the other end, the reverse is true (2001: 304)." In this context, McCrie noted the "Risk of losses and the cost of security measures have a reciprocal relationship. Low protection has low cost, but invites higher risk of loss. In response, the cost of security can increase (2001: 305)." The challenge facing security and safety organizations in resolving the dilemma presented by this reciprocal relationship was noted by Comfort (1988): "A major task of design in the emergency management process is to specify assessment criteria that recognize variation in degree of risk but commonality in meanings of risk across organizations and jurisdictions (1988: 13)."

The Post 9-11 Security Environment

Nature of Threats

The events of 9-11 showed to American citizens, the government as a whole, and to security management personnel the vulnerability of open societies to attacks on infrastructure, health, food and water supplies, information networks, and other facilities. As it relates to the focus of this research, the aftermath of 9-11 left SI in a similar state of being a low risk target, but now it was considered to be in a much higher risk attack area, the National Mall. Not only did SI OPS have to contend with its regular security function it also had to address and adjust to the new realities facing SI and its environment. Not only did SI OPS have to address the new environment by changing its infrastructure, but the role of the federal government and the obstacles to effective emergency and security management also changed dramatically as a result. It became clear to all that the threat from terrorism was indeed real, immediate, and evolving.

To defeat counterterrorism measures, terrorists were becoming more operationally adept and technically sophisticated. As security increased around government and military facilities after the attack, terrorists began seeking out "softer" targets such as transportation systems that provided opportunities for mass casualties. In a Washington Post article dated May 7, 2006, Clark Kent Ervin noted, “the hardening of these targets has increased the appeal of shopping malls, sports arenas, hotels, restaurants, bars, nightclubs, movie theaters, housing complexes and other "soft" targets that remain relatively unprotected against terrorist attacks.” As terrorists employ increasingly advanced devices and used strategies such as simultaneous attacks (i.e. Mumbai 2009),

the number of people killed or injured in international terrorist attacks has also risen dramatically.

A particularly new threat was the risk of suicide attacks or the targeted use of self-destructing humans against noncombatant populations to effect political change (Atran, 2003: 1534). This type of terrorism is potentially much more lethal than most other kinds of attacks due to the high casualty rates. As Pape (2003) observed, suicide attacks accounted for just 3% of all terrorist attacks internationally between 1980 and 2001 but accounted for 48% of all terrorism-related deaths (excluding the September 11 attacks). Nunn (2004) considered the implications of the threat of suicide attacks on United States territory and the difficulties of developing effective preventative policies to deal with this new risk. According to this author, these difficulties are related to the fact that the attacks are perpetrated by people who "believe in a cause outside themselves, which in turn can be operationalized with attacks on an overwhelmingly large number of possible targets (2004: 11)."

Nature of Security Management

As the field of security management expanded to deal with the changing nature of threats, new organizational paradigms were developed in the literature to explain its role and the nature of the challenges it faces. There has been a movement away from the classic models of organizations and management to a model in which the traditional "practices of control and supervision that are part and parcel of the vertical organization diminish or disappear in the network organization (Faye, 2002: 51)." Security managers must now achieve the same type of results that the classic model intended, but they must now go about them differently, as they are forced to adapt to the ever changing demands

and changes within organizations and the security industry especially in the aftermath of the tragic 9-11 terrorist attacks.

According to Faye, there are other external pressures on security managers, who now operate in a rapidly changing business world, in which the fast-paced, highly competitive nature of business forces them to find new ways to be effective at lower cost. This often results in new security risks. Faye also notes that every important decision made by a security leader depends on technical knowledge. These security decisions are never risk-free, and technical knowledge is often critical in arriving at the best possible decision. Overall, Faye notes, security risks take new forms and are shrouded in complexities that call for technical knowledge (Faye, 2002: 11).

The significance of these points can be illustrated by Nunn's (2004) discussion of what would be required in order to develop risk reduction policies against suicide attacks and the difficulties of developing such policies in the U.S. context. He observed that in order to be effective, these preventative policies would need to include (1) consideration of the basic information needed to prevent suicide bombing attacks; (2) modifications to protocols and procedures used currently in bombing situations; (3) use of deadly force policies; (4) profiling strategies; (5) the use of advanced technologies; and (5) target hardening practices (2004: 2). Nunn's observations in relation to these points demonstrate the radical changes in the security environment in recent years. For example, he notes the need to change current protocols and procedures, citing the example of Israel, a country which has experienced many such attacks, in which "aggression and retaliation are used to increase costs to those using suicide bombing tactics," and which include the use of armored bulldozers or targeted 'precision' military strikes as methods of flattening

suspected, arrest or assassination of bomb-makers and engineers identified by the intelligence services, efforts to disrupt recruitment networks to reduce the number of potential shaheeds (martyrs) using political and economic sanctions, and the prosecution of supporters of suicide attacks (2004: 13).

In her article, *Rethinking Security: Organizational Fragility in Extreme Events* (2001), Louise Comfort highlighted how the changing external environment requires government agencies to adapt to changing conditions or risk failing in their Constitutional mission to be the guarantor of rights and the protector of the citizenry. Comfort outlined five conditions that affect the performance, or fragility of public security systems in the post 9-11 world: 1) a shared goal among the participating units; 2) an accurate assessment of the threats to the system; 3) a technical infrastructure that effectively supports system operations; 4) organizational policies and procedures that enable flexible adaptation to dynamic events by the participating units; and 5) a culture that accepts inquiry and information sharing (2002: 100). Comfort explained further that the importance of meeting these conditions is related to the unique characteristics of the new threats to the U.S.: "terrorism, unlike most hazards, is committed by intelligent agents. That is, terrorist agents learn, adapt, and adjust their performance to hide their intentions and evade efforts to counter their activities (100)."

According to Comfort, the way forward in responding to these threats lies in the concept of "shared risk" for society and government. She notes that "the condition of shared risk offers an important alternative perspective on governmental response to terrorism. As the risk is shared, so is the responsibility for assessing, mitigating, and responding to that threat…Individuals, households, and private and nonprofit

organizations become resources for disrupting terrorist acts, as well as potential targets (100).” Similarly, Atlas (2003) advocated the advantages of a more participatory national method of security management: “no system can prevent all breaches, but a comprehensive and consistent approach will empower the security systems ability to catch potential criminals and terrorists with much greater certainty (Atlas, 2003: 2).”

One of the outcomes of the 9-11 attacks is reported to have been an increased acceptance on the part of the general public to take security more seriously. This entails an acceptance in the measures put in place to protect them, and to be more aware of their own responsibility for their safety (Corporate Security, 2002). These outcomes may become factors that change the nature of the environment in which security professionals operate, and may go some way towards helping to ease some of the pressures brought about by the new threats to security, as there are now more eyes available to assist with threat identification.

In organizational terms, the development of a more coordinated, participatory approach has indeed been one of the main characteristics of security management in the post 9-11 era, including a movement towards more integrated working relationships between the public sector and corporate security organizations. One security export has noted that “Homeland defense integrates all respondents … In a corporate structure, you now have facilities designed and maintained that might be likened to public works. You have fire protection which would parallel [to safety], and medical service which is often done by corporate security, because they are generally the first to respond on the scene. The overarching core role in emergency management is where you take all those and wrap them up into a proper project that has a broader base (Corporate Security, 2002).”

Another expert interviewed by a leading security journal concurred with this view, explaining that “Since the events of September 11, it has become corporate security's responsibility to cooperate, as much as possible, with the new Office of Homeland Security. This can be accomplished through cooperation with the newly formed state homeland security operations. These units are charged with the responsibility to evaluate the infrastructures within their state, and devise the necessary plans to protect that infrastructure. Once the plans are developed, they will need to be tested, evaluated and kept current … Security managers will need to form a liaison with the state homeland security team to accomplish these goals. Neither side alone can accomplish a task this large, considering the immediacy of the project (Corporate Security, 2002).”

Although there is still some way to go before there is full integration of public and private sector security services, an example of how this is starting to happen in practice was provided in 2003 by the director of a private security firm, who noted that since 9-11 his company stays in closer contact with local police and fire agencies to share information and even lets the emergency services use their buildings for training (Corporate Security, 2003).

There has also been a more integrated approach within the federal government to dealing with the threat of terrorism since September 11, 2001, as demonstrated for example by closer co-operation and the establishment of many joint working groups and policy committees between the Office of Homeland Security and the Federal Bureau of Investigation (FBI) (Federal Bureau of Investigation, 2001). The latter organization has a mandate to protect the U.S. from foreign intelligence and terrorist activities (Theoharis,

Poveda, Rosenfeld, & Powers, 2000). The ways in which the role of government in security has changed in the post 9-11 era are discussed further in the following section.

Role of Government

As the pre 9-11 literature focused on issues relating to the government's role in preventing an attack or in establishing a government role in disaster planning and mitigation efforts, the post 9-11 literature seemed to shift towards a notion of "now that we have been attacked what's the government role in preventing another attack and ensuring for the safety of its citizens?" The government had to address issues ranging from disaster and security preparedness, emphasis on new security risks, and ways to address the escalating costs that these areas required.

The federal government has responded to such questions by playing a much more central and proactive role in national security in the post 9-11 period, passing a wide range of laws and regulations and developing strategy and policy documents in this area and establishing the Department of Homeland Security within a month of the September 11 attacks. As Rubin (2004), writing in 2003, noted: "An unprecedented number of public policy outcomes have occurred in the 18 months since 9-11. Far more legislation and other outcomes have occurred in those 18 months since 9-11 than in the prior decade (2004: 2)." Rubin observes, however, that these developments were influenced not only by the September 11 terrorist attacks, but by wider changes in the nature and number of risks faced by the United States, including familiar threats such as earthquake and floods as well as new concerns about "chem- and bio-terrorism, critical infrastructure, and cyber-terrorism threats (2004: 1)."

Another change in the nature of development which occurred during the aftermath of the 9-11 attacks was the implementation by the federal government of detailed regulations and guidance to state and local governments on the development of all-hazards planning. The guidance was issued in February 2002, with a requirement on all states to complete their plans by September 30, 2004. To assist states in the process of assessing risks, the Federal Emergency Management Agency (FEMA/DHS) developed an analysis tool for use in calculating loss, HAZUS-MH (Rubin, 2004).

Despite these developments, however, it has been argued that – at least at the federal level, the role of government in relation to security management has remained mainly retrospective consisting of threat or hazard analysis, rather than being forward looking with an emphasis on risk assessment and prevention. Although uncertain, this approach may be the result of budget concerns or a cost benefit analysis that has shown this method of mitigation to be the most advantageous. As a result, federal government responses to emergency incidents have continued to be reactive rather than preventative (Rubin, 2004). At the same time, increased focus on risk analysis and mitigation planning at state and local level have largely been directed at planning for natural disasters and emergencies rather than man-made events such as terrorism (Rubin, 2004). It has been argued (Rubin, 2004) that motivation on the part of federal government to encourage states to conduct risk assessments and take mitigation measures has been in large part driven by budgetary considerations and the desire to reduce payouts in the event of a disaster. The focus on reducing the cost of emergencies and disasters is also reflected in the central role which the General Accounting Office (GAO) plays in analyzing the costs

of emergency management and disaster policies and programs, and its promotion of a risk-based approach to expenditure.

On the other hand, Corbin (2003) cites evidence of the expanded role and efforts of the government since the 9-11 in terms of security in the increased budget allocations, amounting to billions of dollars that have been and continue to be spent by the United States government on the efforts to overcome the new diverse terrorist challenges. Table 3 illustrates the federal funding information for homeland security and combating terrorism for the years 2001, 2002, and 2003, respectively. Figures are presented in terms of billions of dollars. When the source of this information was published, the figures for emergency supplemental appropriations were not available the fiscal year, 2003. Nevertheless, it is clear to see that the figure of spending more than doubled for emergency supplemental appropriations between the fiscal years of 2001 and 2002.

Table 3 - Federal Funding for Homeland Security and Combating Terrorism by Year (Budget Authority in Billions of Dollars*)

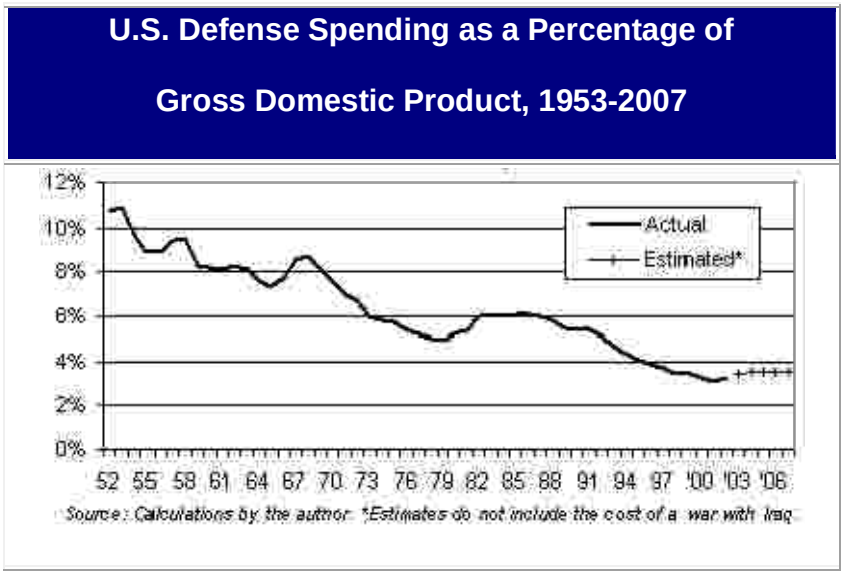
	FY 2001	FY 2002	FY 2003*
Annual Appropriations			
OMB Estimate of Federal Funding	20.0	24.2	44.8
Other DoD Funding (not including in OMB estimate)**	0.0	0.0	8.2
Subtotal	**20.0**	**24.2**	**53.0**
Emergency Supplemental Appropriations			
September 2001	20.0	0.0	0.0
January 2002	0.0	20.0	0.0
August 2002	0.0	24.0	0.0
Subtotal	**20.0**	**44.0**	**0.0**
Total Discretionary	**40.0**	**68.2**	**53.0**
Direct Spending* **	**5.2**	**3.0**	**2.7**
Total Spending	**45.2**	**71.2**	**55.7**

* Level of funding requested for FY 2003.
** This is the $20.1 billion request for the Defense Emergency Response Fund, excluding funding for combat air patrols (which is included in the OMB estimate), funding related to the Nuclear Posture Review and the $10 billion requested for a war reserve fund.
*** Primarily funding for the Air Transportation Safety and System Stability Act.

*source: S. Kosiak (2003), *Security after 9-11, p. 9*

Other security management efforts of the government have also been documented in financial terms. According to Childress (2002), the Homeland Security Budget for 2003 proposed $11 billion for a variety of programs focused on tracking the entry and exit of non-American citizens to and from the United State, in order to meet the four specific policy objectives the most important of which was seen as securing America's borders. However, Childress (2002) also points out that, in comparison to the Gross National Product, defense spending has actually decreased in recent years, and is considerably lower per capita than other areas of federal spending, such as education. To support his argument, Childless (2002) compared the cost of homeland security ($340 and $480 for every American) with educational expenses for each American ($1,780). Table 3 provides a graph of defense spending by the government of the United States as a percentage of the country's Gross National Product from 1953 to 2007 (with estimated amounts after 2003). As indicated at the bottom of the graph, the estimates do not include the cost of a war with Iraq.

Table 4 - U.S. Defense Spending as Percentage of GDP: 1953-2007



Specific Measures

A major development which demonstrated the new role of the government in the aftermath of 9-11 occurred on October 8, 2001, when President Bush signed an Executive Order creating the Office of Homeland Security "to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks (David, 2002)." The Office of Homeland Security (OHS) was created on October 8, 2001 via Executive Order 13228 in a concerted effort by the United States government to provide indications of progress in countering terrorism. This was, perhaps, the most ambitious and direct security management response to 9-11 by the United States government. The office was created less than one month after the tragic event. OHS was charged with six primary functions: to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States. The Office was established within the Executive Office of the President and was headed

by the Assistant to the President for Homeland Security (Executive Order 13228, October 8, 2001).

Difficulties and Challenges

The expanded range of governmental functions brings about new challenges and difficulties in the post 9-11 era, due to the sheer scale of funding, coordinating and implementing the various responsibilities involved. For example, a 2003 report on the Department of Homeland Security's transportation policies and operations noted five major challenges: 1) developing a comprehensive transportation risk management approach – one that should involve the states; 2) ensuring that transportation security funding needs are identified and prioritized and that costs are controlled; 3) establishing effective coordination among the many public and private entities responsible for transportation security; 4) ensuring adequate workforce competence and staffing levels within all agencies and departments involved; and 5) implementing security standards for transportation facilities, workers, and security equipment.

In the context of new threats to national security, in which any virtually any location might be targeted for attack, the prioritization of risks becomes fraught with difficulty. The risks are arguably too high in terms of possible loss of human life to justify using traditional post-attack, retrospective methods of developing preventative strategies for the future, yet it is virtually impossible to conduct meaningful cost-benefit analyses. With regard to suicide attacks, for example, Nunn highlighted the immense potential costs of developing expertise in suicide bombing post-event responses in terms of widespread training of health, fire, emergency response, and police personnel, and noted the difficulty of answering the hypothetical question: "If you could invest $10

million in training that would reduce the probability of suicide bombing by 20%, would it be a bargain?, with no reliable information on the probability of attacks or likely numbers of casualties." It is even very difficult to decide which venues or locations to focus on in terms of preventative measures, because as Nunn notes "almost any place under the right circumstances can have the ingredients necessary for an effective, 'message-generating' suicide attack (Nunn, 2004: 17)."

The expanded uses of security measures, particularly using technology such as video surveillance and biometric systems in public places, have implications for personal freedom and privacy which also need to be considered by security policymakers and practitioners. Haque (2002) has noted the possibility that these developments might have an adverse effect on the public co-operation and participation which is so crucial to effective security management in the post 9-11 era. In his article *Government Responses to Terrorism: Critical Views of Their Impacts on People and Public Administration*, Haque outlines some of the dilemmas facing public administration, the role of government and the role of citizens, and suggests that the issue of legitimacy often depends on how public officials promote broadly based public participation (176). The primary problem he suggests is the effects of the dichotomous relationship between the new anti-terror laws that stress bureaucratic secrecy against the public's need for information. He further notes, "In this atmosphere, overwhelmed by concerns for security, surveillance, investigation, suspicion, and distrust, it is unrealistic to expect greater public participation in public administration (176)."

One of the early lessons for security managers in the aftermath of 9-11 was reportedly the importance of quality rather than quantity of security measures. One

security professional noted that his company learned that rather than recruit more guards or introduce advanced technology, it was much more effective to “lean” the force and properly train them so they understand their duties. To illustrate his point, this security manager added "It doesn't matter how good an access control system you have if an employee props a door open (Corporate Security, 2003).” The point of emphasis is that more security personnel does not necessarily equate to better security, nor does the addition of an infusion of technical security devices. Instead a security force that is well trained on the technical aspects of security, as well as the proper mitigation and response to events is best able to cope with post 9-11 security efforts.

Conclusion

The evidence has shown the pre 9-11 governmental security environment was responsive in nature to events. Actions and policy implementation, as well as major policy shifts were generally effected after an incident had occurred, with a focus on response and receiving assistance from federal agencies. This environment shifted to a mode of pre-emption in the aftermath of the events of 9-11, which focused on prevention and preemption with a more dominant centralized role for the federal government. The trends in the post 9-11 security and policy literature, as well as in the actions of the US government (formation of DHS, strengthening of the TSA, to name a few) for the most part, shows a policy shift from reacting to past known events to attempting to mitigate future unknown terrorist events. The literature also outlines a shift in expectations for security management from a hierarchical top-down model of management to a more networking top-down bottom-up type of system. As the trends in the post 9-11 literature

shows a policy world shift, evidence also shows that SI OPS, an organization which manages low risks for manmade threats in a high threat area also faces similar challenges.

Chapter 3

The Smithsonian Institute (SI) and the Office of Protection Services (OPS)

Smithsonian - Organization and History

The Smithsonian Institution (SI), an educational and research institution and associated museum complex which is administered and partly-funded by the government of the United States, has facilities located in Washington, D.C., New York City and Republic of Panama. SI consists of 19 museums, seven research centers and a zoological park. It has approximately 142 million items in its collections; it is now the world's largest museum complex and research institute, with "irreplaceable national collections in American and natural history, art, and other areas (GAO, 2007)." Two of its museums on the National Mall in Washington, D.C. receive more visitors than any other museum worldwide (GAO, 2007). SI currently employs approximately 6,300 Federal employees (SI Pamphlet).

The Smithsonian Institute was founded in 1846, "for the promotion and dissemination of knowledge" by a gift to the United States by the British scientist James Smithson (1765–1829). This gift was contingent upon his nephew, Henry James Hungerford, dying without any heirs of his own. In such a case, the Smithson estate would go to the United States of America for creating an "Establishment for the increase & diffusion of Knowledge among men (U.S. Congress, 1846)." After Hungerford's death, the U.S. Congress passed an act establishing the Smithsonian Institution as, "an American hybrid of a public/private partnership," which was then signed into law on August 10, 1846, by President James Polk. According to documents located in the Library of Congress, the Act establishing the Smithsonian was to provide for the

administration of the trust, by a group independent of Government influence, which consisted of a Secretary and a Board of Regents comprised of private citizens and members of all three branches of the Federal Government. This diverse body of individuals was chosen in an effort to ensure `the wise and faithful use' of the Institution's funds. The group was also given broad discretion in the use of these funds (Senate Report 109-275 - Department of the Interior, Environment, and Related Agencies Appropriations Bill, 2007).

Nowadays, funding for the operating and capital program costs of the Smithsonian are provided from its own private trust fund assets as well as federal appropriations, while its facilities are mostly federal-funded (GAO, 2007). Services for the protection and security of the Smithsonian are also federal funded and are administered by the Office of Protection Services (OPS).

SI OPS – Organization and History

SI OPS provides protection and security services and operates programs for security management and criminal investigations at SI facilities on and near the National Mall in Washington, D.C., in New York City and in Panama. SI OPS also provides technical assistance and advisory services to SI bureaus, offices, and facilities. It serves SI employees, volunteers and more than 25 million visitors each year (IWA, 2005).

The protection and security services for the SI began in 1846 when the first "night watchman" for the United States National Museum was hired. The position required the person to manage the public in the galleries and library of the Smithsonian Castle, keep up the building in adverse and cold weather, and perform additional duties such as the management of coal deliveries, water barrels for fighting

fire, and errands for the Secretary (IWA, 2005). The duty hours required the guard to work 12 hours a day, seven days a week, for a salary of $30.00 a month. After a fire in the East end of the Castle in January 1864, the Board of Regents justified the hiring of a second watchman (IWA, 2005).

By 1878, the “Watch Force,” as it was then referred to, was to consist of not less than twenty-four people duly appointed by the Secretary of the Smithsonian, or by his order. According to the Rules for Watchmen (1893) all new guards were required to possess the qualifications of a District of Columbia police officer. As such, the guards were to: (1) be able to read and write the English language; (2) be a citizen of the United States; (3) Never have been indicted and convicted of a crime; (4) be at least 5 feet 8 inches in height; (5) be between 22 and 35 years of age; (6) of physical health and vigor; (7) of good moral character; and (8) of unquestionable energy and courteous manners.

The first electric "alarm" was installed in 1876 when call-bells for alerting the building superintendent in case of emergencies were placed in the basement and in the main and anthropological halls. A large gong was placed outside the east entrance for calling employees outside. As new buildings and facilities were added, so were additional security personnel. By 1915, the security force numbered 51 employees, but that year 22 of them resigned due to low pay (IWA, 2005).

By 1943, the force had grown to 71, but a reduction in force caused by wartime recruitment soon lowered the number to 44. A 40-hour workweek was established for the security force, then consisting of 82 employees, in 1945. In 1960 the security force totaled 120, and by 1964 it was up to 210. The Smithsonian Institution staff numbered more than one thousand employees at the time. What is now known as the Office of

Protection Services was formed in 1973 to consolidate the administration of protection, security, safety, and health services for the SI (IWA, 2005). In early 1986, reorganization resulted in the reassignment of the safety functions to the newly created Office of Environmental Management and Safety. Health Services functions were also moved there in 1995, leaving the OPS to cover protection and security. OPS is currently part of SI's Office of Facility Engineering and Operations division and currently has over 600 guards and security personnel protecting its facilities, guests, and staff, as well as guarding and protecting the art from theft and/or vandalism. The Office of Protection Services receives the authority to police the buildings and grounds of the Smithsonian Institution from Title 40 of the United States Code 193 n-x (IWA, 2005).

SI OPS – Pre 9-11 Role and Challenges

It could be argued that in terms of the four main areas that are the focus of this study – screening, policy processes, budget and training - SI OPS was in equilibrium in the pre 9-11 period, undergoing only minor fluctuations such as routine shifts in yearly budgets. In a similar way to the federal government, as outlined in the previous chapter (Comfort, 1988; Cigler, 1988), SI OPS management worked in a top-down policy-directive mode and had a firmly established role for its guard force: to ensure the safety and security of its staff, visitors, buildings, and the artifacts housed within those buildings. Interviews conducted with security officers and managers revealed that that an overwhelming majority cited this as the primary mandate of SI OPS prior to 9-11.

Screening

PET predicts that an examination of SI OPS should reveal that screening activities were practiced in particular ways prior to 9-11, and then underwent a drastic change to address the new security environment post 9-11. It stayed at the new level (if one was established), became more stringent, or reverted back to pre 9-11 levels. Although there was a security presence at museums at this time, it was minimal and consisted primarily of one officer counting visitors as they entered a museum, with additional personnel scattered throughout that museum supervising errant youth on escalators and ensuring no theft or damage to the artifacts was occurring. In one museum, regular bag searches were conducted, but this was mainly in order to prevent vandalism rather than terrorism. Screening policies and practices would be considered to be in deep structure leading up to 9-11 due to the fact that the policies and practices had been relatively unchanging during those years.

Policy

Similar to the effects on screening PET predicts that an examination of SI OPS should reveal that prior to 9-11 OPS managers addressed day-to-day issues relating to security, personnel issues, and budgets. However, following 9-11 there should be an indication of major security policy shifts to address the growing security environment. Pre 9-11 security management policy was primarily concerned with how to most effectively meet SI OPS' primary mission of providing for the basic safety of all employees and visitors and the security of the artifacts housed in its buildings. As such, policy was largely directed at the development of strategies, such as internal patrols, to ensure that all staff was appropriately provided badges and in the proper places, and that

there was sufficient coverage of the buildings. Although interviews with some managers suggested that terrorism was something that was “thought about” as a risk to the museums, it was not actually addressed in the design of security policies and measures. Any perceived risk in terms of terrorism was primarily related to potential collateral damage that could be inflicted upon the museum or persons due to an event or attack on the Congress or another federal agency near SI on the National Mall.

Training

PET predicts that an examination of SI OPS’ training manual should reveal that prior to 9-11 training consisted of basic law enforcement concepts, such as rules of detention, arrest, search and seizure practices, Smithsonian policies, protection of artifacts, and firearms training. However, following 9-11, there should be an indication that training changed to address issues related to terrorism prevention, screening techniques, and emergency management procedures. Within this context, training and instructions to security officers were concerned with basic operational, safety and law enforcement issues. Each museum security office conducted formal briefings or formations for its officers prior to each shift, with topics covered including security directives issued from headquarters, a briefing of the days upcoming activities (for later shifts any relevant events that occurred during the prior shifts), and basic officer safety and awareness issues. The training for new officers consisted of a three week basic security course that provided firearms training, District of Columbia and Federal law statutes, arrest and detention techniques, as well as SI internal rules and guidelines training. Once completed, the officers were assigned to museums and assigned to shifts. They would then attend formation each day to hear the directives from OPS management.

Training is another area that would be considered in deep structure prior to 9-11. Again this is due to the fact that the training modules went relatively unchanged for many years leading up to 9-11.

Budget

PET predicts that an examination of SI OPS budget data should reveal that prior to 9-11 the OPS budget maintained a certain level or grew at a steady rate similar to other governmental agencies. Following 9-11, there should be an indication that the budget shifted to match new security concerns related to terrorism, and anti-terror technology, and manpower issues; stayed the same; or grew to address new terrorism concerns, then gradually reverted to a growth pattern similar to the years prior to 9-11. The OPS budgetary process is similar to that of other federal and state agencies. It consisted of each museum submitting its fiscal year needs to OPS management, who would then compile the data, make any line item adjustments they deemed necessary and submit it to the Smithsonian's budget office for OMB approval. OMB would perform its own line item adjustments and send it back to OPS for any additional comments or rebuttals. Once a compromise was reached, the budget proposals were submitted to the House Interior Appropriations Committee for final mark-up and approval (IWA, 2005).

CHAPTER 4

Methodology

Introduction

As previously noted the purpose of this research is to explore how the Smithsonian Institution's Office of Protection Services' (SI OPS) responded to the terror attacks of 9-11. This chapter presents the methods used to conduct the study. Specific sections within this chapter will outline the research design, role of the researcher, limitations and delimitations of the study, data collection, and data analysis.

This research was conducted as a qualitative exploratory case study that was predicated on research questions posed to various members of the Smithsonian Institution, as well as from data made available for review. According to Lecomte & Preissle (1993), "Qualitative research is a loosely defined category of research designs or models, all of which elicit verbal, visual, tactile, olfactory, and gustatory data in the form of descriptive narratives like field notes, recordings, or other transcriptions from audio- and videotapes and other written records and pictures or films." It can also be considered as: naturalistic research, interpretive research, phenomenological research (although this can mean a specific kind of qualitative research as used by some), or descriptive research. In essence, there is no standard definition that can be used to really encapsulate qualitative research. It is as much a perspective as it is method. Gall, Borg and Gall (1996) define qualitative research as:

> "Inquiry that is grounded in the assumption that individuals construct social reality in the form of meanings and interpretations and that these constructions tend to be transitory and situational. The dominant methodology is to discover these meanings and

> interpretations by studying cases intensively in natural settings and by subjecting the resulting data to analytic induction (767)."

Table 5 provides a brief perspective on the strengths and weaknesses of using qualitative research methodology.

Table 5

Strengths of Qualitative Research	**Weaknesses of Qualitative Research**
1. Depth and detail - may not get as much depth from a standardized questionnaire; 2. Openness - can generate new theories and recognize phenomena ignored by most or all previous researchers and literature, which is making it especially valuable tool; 3. Helps people see the world view of the individual or group studied with the hope of capturing, from their perspectives, what is happening without being judgmental.	1. Fewer people studied usually due to high resources (monetary and human) and time constraints; 2. It is difficult to generalize the results; aggregate data and make systematic comparisons; 3. Very much dependent upon researcher's personal attributes and skills; Different researchers may obtain different results entirely due to their knowledge, professionalism and practical skills; 4. Researcher participation within the setting can change the social situation (although not participating can always change the social situation as well). 5. Introduction of Bias

The logic for conducting qualitative research, as opposed to quantitative research, comes from the observation that it allows a researcher to better understand and interpret subtle data that are not necessarily evident in quantitative research. Qualitative research

methods are especially useful for this study because they are designed to help researchers understand people and the social and cultural contexts within which they live.

Assessing the qualities of a person's reality can be accomplished in many ways. This study aimed to use an exploratory case study format, where single-person interviews, review of documents, and observations were the primary means of assessing the changes, if any, that took place in OPS after 9-11 focusing on the policy processes, the budget, training practices, and screening. These methods were applied by means of triangulating data (Yin, 2002). Triangulating data provides the research a means of using different methods, data sources, researchers, or perspectives to explore a single program, problem, or issue.

Prior to the study, the Virginia Polytechnic Institute and State University Institutional Review Board (IRB) reviewed and approved the research protocol. Expedited status was received. The voluntary consent forms, as well as the interview questions were provided to participants by the researcher prior to conducting any interviews. The consent form contained general information about the study, along with the contact information of the researcher. Interviews were recorded except in instances where the interviewee declined. In those cases, notes were taken to record the interviewee comments.

Case Study

Case study research was used for this study because it focuses on understanding the dynamics in a particular setting (Yin, 2002). The term "case study" has multiple meanings. It can be used to describe a unit of analysis (e.g. a case study of a particular organization) or to describe a research method. The discussion here concerns the use of

the case study as a research method. Although there are numerous definitions, Yin (2002) defines the scope of a case study as follows: A case study is an empirical inquiry that investigates a contemporary phenomenon within its real-life context especially when the boundaries between phenomenon and context are not clearly evident (Yin, 2002).

According to Winegardner (2002), Yin outlines six specific skills researchers should possess before moving into the research area of the case study, "an inquiring mind and a willingness to ask questions before, during, and after data collection; an ability to challenge oneself as a researcher to determine what is happening; an ability to listen, observe and assimilate large amounts of data without bias; adequate flexibility to accommodate the unexplained; a working understanding of the issue at hand; and a lack of bias regarding interpretation (12)."

Yin (2002) further implies that a case study is a process of investigation of contemporary activities in real-life context and that it is a process of dealing with a diversity of evidence and articulating research questions. Yin (2002) continues that the case study research manager must back up the research with experience and evidence through documentation, management of archival records, interviews, direct observations and physical artifacts. Collected data should, in Yin's view, be more relevant to the case study and should converge to support a central fact, creating a "robust fact" where three or more sources support the same idea. The articulation of each research question is imperative to Yin as the questions seek to explain the "how's" and "why's" behind occurrences at the site being studied.

Kaplan and Maxwell (1994) suggest that the goal of understanding a phenomenon from the point of view of the participants and its particular social and institutional context

is largely lost when textual data are quantified. Through the use of multiple interviews, document review, and observation, the data can be collected and evaluated to examine the extent to which it is typical of the findings at the organization in question. For the purposes of this dissertation, the researcher will be utilizing three sources through interviews, observation, and documentation, where possible, to study the "how" question of SI OPS—specifically, how did the organization change after 9-11, with focus on key variables for your assessment. The point of view of the participants is very important in this case, as well as the security guards, managers, and SI curators to enact and impact the changes, if any, that have resulted.

Role of Researcher and Origin of the Study Topic Chosen

This research was developed, documented, and conducted by the author. This consisted of collecting, analyzing, conducting the interviews, and reporting all of the findings regarding the collected data. I initially became interested in museums as a high school student who was intrigued by Baroque art. Museum security became a part of this fascination as I began my career as a Virginia State Trooper after graduating college in 1993. I read books about art theft and art fraud and once I became a Special Agent in the United Stated Secret Service in 1997, I was able to travel to various countries around the world and visit museums and sites of famous art thefts.

I began my graduate studies shortly after resigning from the Secret Service in 2001, and in the summers of 2002 and 2003, I was a recipient of the Smithsonian Institution's James E. Webb Minority Scholarship. It was through this scholarship that I was able to work closely with members of SI's OPS. As a result of this interaction, I may

have accumulated biases concerning the work and functions of the SI OPS, individuals interviewed the data, and my interpretation of the data.

While this experience conditions my research, I have attempted to bring a robust and experience-based view to this research in several ways. First, interviews were conducted with some of the individuals that I have worked with, but the majority of the interviews were with individuals who have come to SI OPS after my work in the office. Second, the interview base reaches beyond the personnel in SI OPS to bring a fuller picture of the broader environment in which SI OPS functions in the SI. Third, I have relied on observation (social science field techniques) and secondary sources to assess the data, in addition to the interviews. Finally, in the text, I discuss areas of analysis where possible biases or insights might be most relevant. Although there may be individual biases held by the author, the previous interactions between those individuals and this author might prove to strengthen this study as I bring organizational knowledge and insights that someone unfamiliar with this organization may lack. In the text I discuss areas of analysis where these possible biases or insights might be most relevant.

Data Collection

The data collection process was comprised of a combination of techniques, which included open-ended interview questions, on site observations, SI archival research, and a document analysis of SI OPS Uniformed Security Policies. There were four factors used as measuring points for change: the budget, security screening policies, training, and the policy formulation process. Each variable was examined through reading of documents and through information gathered in interviews from 1998-2004. The data was also derived from interviews of museum security personnel, non-security employees,

Smithsonian curators, as well as from documents (relating to the four variables) made available for review. Uniformed security personnel were chosen because they are the group who practice security for the SI. Their actions manifest security. The security managers and Curators have influence over the ways in which security policies are defined and executed, with their own priorities.

Interviews

Interviewees were chosen based on their knowledge, expertise and experience in the areas of this study. Structured interview formats aim to capture "precise data of a codable nature in order to explain behavior within pre-established categories ... [the unstructured interview] is used in an attempt to understand the complex behavior of members of society without imposing any a priori categorization that may limit the field of inquiry (Fontana and Frey, 1994:366)." Unstructured interviews have the advantage of situating any prior conceptions held by the researcher in the background and giving priority to the participants' own conceptions of their experiences. The disadvantage of an unstructured interview format is that lack of a specific focus may tend to produce a great deal of material that may not be closely connected with the research. When time is at a premium the unstructured interview may not make the best use of this limited resource. Interviews are also a good means of developing a rapport with interviewees in contrast to survey's in which the respondents are likely to only answer the questions posed without going into much detail behind those answers.

In analyzing data for the open-ended/semi structured questions, it is necessary to code the data to establish themes in responses and to look for patterns (Ryan & Bernard, 2003). The analysis of the data varies depending on the goal of the study and the

researcher; an historian's analysis may differ from that of an anthropologist's (Gall et al., 2002). A researcher applying safeguards for bias, taking adequate notes and practicing interview skills will be less likely to make errors collecting data (Gall et al., 2002).

The questions were primarily open-ended or semi-structured to provide the participants ample opportunities to touch upon any related matters they felt were pertinent to this study. The open-ended or semi-structured interview format that I developed is situated between the two extremes of the structured and unstructured interview and although this approach may require a greater length of time than a structured interview, it has the advantage of allowing the participants to raise new issues and concerns that I, as a researcher, had not conceptualized as being pertinent. These types of interviews were chosen because the personnel are participants who have broad knowledge of the institutions and were able to provide in-depth information regarding the organizational, managerial, and structural issues and policies within the Smithsonian.

It was intended that the interviews would provide insight into the types of changes, if any, that have taken place since 9-11, how those changes were manifest, and which factors were driving those changes. Examination of budget, training, policy and planning documents were chosen because it was believed they would be able to provide additional insight on the question of change.

All subjects approached for interviews were considered volunteers and had the option to decline participation at any time before, during, and/or after the interview process. The interviewees were not identified on any of the documents; rather they were anonymized with assigned numbers with the corresponding names being available only to the researcher and his advisor. The current director of OPS determined access to all

personnel and documents. He also reviewed all proposed questions. He, however, did not offer or reject any interview questions, nor did he deny access to any members of his security staff or uniformed officers. The sample selection consisted of any uniformed security personnel and managers, as well as non-uniformed security managers who had been employed any time prior to the events of 9-11, and who were SI employees at the time of this study.

Questions for the interview framework for 1:1 interviews are as follows:

Officers

1. Prior to 9-11 what were you instructed regarding the primary security concerns for your position?
2. How did those instructions change after 9-11?
3. Has your training changed since 9-11? If so, how?
4. Has your screening policy changed since 9-11? If so, how?
5. What are the types of inspections and searches that your security force conducts?
6. To your knowledge has the OPS budget changed since 9-11? If so, how?

Managers

1. Prior to 9-11 what were your primary security concerns? What kinds of security programs did you have in place to address pre 9-11 concerns?
2. How did those concerns change after 9-11? How did your various security programs change post 9-11?
3. Has officer training changed since 9-11? If so, how?
4. Has the OPS budget changed since 9-11? If so, how?
5. Has your screening policy changed since 9-11? If so, how?
6. Has your approach to security changed since 9-11? If so, how?
7. How do you guide your subordinates regarding post 9-11 security?

Literature Review and Document Analysis

The documents reviewed in this study consisted of SI OPS' uniformed security officer's policy manual. The following chapters were analyzed for this study:

OPS-01 OPS Organization and Functions (07/03)

OPS-06 Enforcement Duty, Authority and Jurisdiction (09/97)

OPS-15 OPS Operations (07/03)

OPS-32 Training Division (11/01)
OPS-43 How to Request Training (05/00)
OPS-51 Mail and Package Screening Policy (07/03)

In addition to the security manual, archived historical documents related to the founding of SI, SI and the Civil War, SI and World War II, and any other historical documents relating to the function of OPS prior to its current incarnation. Archival documents were used for three primary reasons. First, the documents helped to clarify and formulate questions pertinent to understanding the nature of events that occurred at SI OPS during and following radical organizational changes in SI OPS with a focus on the four variables. Secondly, the documents provided organizational meaning, understanding, and insights into its history (Merriam, 2001). Finally, the documents served as records of activities and events that occurred at a time where I could not be a first hand observer (Stake, 1995).

Several methods were used to conduct a review of the literature for this study. The use of several online databases including Info Trac One file, ABI, Emerald, JSTOR, and the Expanded Academic Index ASAP were used to search for relevant articles, books, and dissertations. The searches were initiated using keywords such as punctuated equilibrium, organizational change, radical change, and incremental change. The references and endnotes of each document used in this review were themselves reviewed for leads to other articles and books that might further expand this study and provide additional sources.

The purpose of the literature review was to identify relevant material relating to security policy and practices, and budgeting in both the pre and post 9-11 settings. It was hoped that by combining the information gathered from the interviews, the review of

archival data, and the material derived from the literature review, a well- rounded analysis could be realized regarding organizational change within SI OPS. The security literature review focus also aimed at introducing low risk/high threat organizations.

As previously noted, four factors are studied for this dissertation as the points for which the author is looking for change in response to 9-11. PET posits that punctuations (significant events, for example) disrupt a linear, incremental path of policy making or organizational behavior. This study examines the terror attacks of 9-11 as punctuation. While the attacks had consequences for policy making trajectories and organizations across federal, state and local governments, this study examines the consequences for an organization in a high threat area, but with a low probability of direct attack. Change in SI OPS is examined by focusing on screening practices at the SI museums, the OPS budget, the policy process within SI, and training practices. These factors were chosen because of their measurability over time, through both document analysis and by gleaning the responses of those who created and implemented the responses.

The research will look not only at immediate changes in the budget amount, or specific changes in the training practices, but the more nuanced or longer-term changes, as well—for example, with policy making, the understanding of or utilization of risk analysis before and after 9-11, and the implications for how policies within SI OPS are made, but also how that approach to risk might impact training, as well as resources for training, etc. The policy process is not as easily measureable, however, due to the low turnover within the management positions in SI OPS, it is believed that the data derived from manager interviews measured against the SI OPS manual will constitute a fairly accurate portrayal of changes, if any, within the post 9-11 policy process.

Data Verification/Triangulation

The data was coded and categorized into tables where the reader will be able to discern similarities in responses. Data collected through the review of documents was used to confirm or disconfirm the responses from the interviews as a means of triangulating the collected data. Documents from the site were paraphrased, represented in depth or provided as full narratives, depending on how they were used or referred to during the interview process.

CHAPTER 5

Factors and Results

Introduction

The purpose of this study is to explore how SI OPS responded to the terror attacks of 9-11 and the ongoing threat. This chapter provides more detailed background into the four factors of this study and outlines how one particular factor (the budget) affects the implementation and sustainability of the other factors. In addition to the general discussion regarding pre and post 9-11 security changes at the Smithsonian, an interwoven theme throughout this chapter involves the difficulties (obtaining adequate budget, manpower issues, policy consensus, etc) that a unique federal agency (the Smithsonian)--considered a low threat target, but located in a high threat area has undergone since the events of 9-11.

The structural and practical elements of each variable will be explored. The structural elements are primary topics that each variable addresses, while the practical elements are the implementation processes undertaken by SI OPS for each variable. The results from each question are grouped according to the variables and will be divided between security managers and officers. There were also two introductory questions that were used to set the stage for this study. The introductory questions are discussed as part of the overall pre and post 9-11 questions and are intended to provide the researcher with a broad picture of pre and post 9-11 SI OPS. The introductory questions are helpful in providing context for more specific questions as well. A separate section is devoted to non-security personnel responses to questions. Finally, the results of the qualitative review and assessment of are provided, and the chapter ends with a summary.

Introductory background information and questions

Security Managers

Seven security managers in SI OPS volunteered to be interviewed for this dissertation. All seven were working for SI OPS prior to 9-11; it is believed that those employed prior to 9-11 can provide a better hands-on explanation of the security changes, if any that took place after 9-11. On my behalf, SI OPS sought to identify all security managers who were employed prior to 9-11. In this section I summarize the data related to the introductory questions. Appendix I summarizes the responses of these seven supervisors to each of the survey questions.

The first question on the interview guide consisted of two parts. First Question, Part 1: *Prior to 9-11 what were your primary security concerns?* Five of the managers indicated that protection of the galleries, artifacts, and other property were of primary concern (noting that theft or vandalism were potential problems). One manager noted that they had to be on guard against "people bringing stuff that could damage the art you know like paints and stuff like that." Four of the seven managers mentioned that the safety of both staff members and visitors was a primary security concern. Only one manager mentioned terrorism at all, but indicated that this was not as big of a focus as it became after 9-11 "because there were (sic) not so much [terrorism] in the United States." Continuing on that theme the same manager noted,

> "We knew it [terrorism] was there and we did have concerns… we tried to build up our manpower, which we were gradually doing up to 9-11. We tried to increase training of the officers trying to make them aware of what could happen and tried to keep them up on what's going on around the country (IWA, 2005)."

That sentiment was echoed by another manager who noted, "It [terrorism] was something we were aware of and a bit concerned with, but it wasn't our primary concern. Our primary concern was mitigating theft and vandalism."

First Question, Part 2: *What kinds of security programs did you have in place to address pre-9-11 concerns?* Two of the seven managers mentioned random and infrequent bag checks for members of the public entering galleries, with one noting "We checked bags randomly looking for spray paint and things like that." No other security program was mentioned by more than one manager, with single managers mentioning disaster/emergency programs, bomb detection, traffic flow, making arrests, and cameras/security equipment.

Second Question, Part 1: *How did those concerns change after 9-11?* Six of the seven managers agreed that there was an increase in security (visitor, parcel, and bag searches; perimeter roving patrols; raised security awareness) and a focus on possible terrorist acts, although the seventh respondent stated "The existing security programs remained in place. The risks to terrorism didn't change they just weren't addressed prior to 9-11." Four specifically noted that their security programs became more geared toward terrorism through more personnel on duty and more of an interest in the outside (perimeter) of the buildings than prior to 9-11. Concerns were also mentioned for both items that could be detected only electronically and for items that could be brought in to the facility by either staff or visitors. One manager noted that there was a considerable move towards increasing manpower following 9-11. He offered the following statement:

> "Of course you know they [concerns] changed dramatically after 9-11. Where we had been trying to get additional people we were able to get additional staffing after 9-11 and we were able to go to electronic screening something that we had never done prior to 9-11 (IWA, 2005)."

Another manager spoke of the growing realization that terrorism was now an issue and noted, "Things became a lot more geared towards terrorism. What's this person carrying in their bag and what are their motives or whatever? I think it's more or less the concerns turned towards the prevention or the detection of terrorist acts or anything related to that."

Second Question, Part 2: *How did your various security programs change post-9-11?* Five of the seven managers mentioned more of an emphasis on electronic monitoring devices such as x-ray machines and magnetometers. Two managers emphasized enhanced security procedures for the exterior of the building, with one noting "we set up external barriers…and blast mitigation devices." Individual respondents also mentioned more manpower, more personnel training, and new assessment procedures to determine if current security programs were functioning properly. Regarding the overall post 9-11 changes in SI OPS one manager noted,

> "And again we were able to get more manpower, we started the electronic screening, we started what is called a bag check because here at natural history we were unable to because of space configuration we were unable to get the x-rays posted at the doors so we just ended up with just the mags [magnetometers] the actual people coming through magnetometers and the wand and we did bag check and again we had more human resources to work with. And also we got more electronic security protection as well for instance cameras on each own all four corners of the roof. We had never had that prior to until after 9-11. So now we are able to see events, record events that's taken place outside of the museum that we weren't able to do before."

Security Officers

Seventeen non-managerial security officers were interviewed. All seventeen were working for SI OPS prior to 9-11 and were currently still employed at the time of the interviews. It is believed that those employed prior to 9-11 can provide better hands-on observations of the security changes, if any that took place after 9-11. A search was

conducted by SI OPS to identify all security officers who were employed prior to 9-11 to pose the pre and post SI OPS questions. The search was conducted by imputing the security officer federal position number and employee orientation date (EOD) that was set at January 1, 2001 into the SI OPS officer database. A list of officers falling into these categories was produced. A subsequent list of questions, the consent form, and a call for volunteers to participate in a non-SI research project was then sent to those on the list. Volunteers then came forward.

Appendix I shows a summary of the responses to the six interview questions on the security officer interview guide. This section contains a review of the results from the non-managerial security officer interviews related to the introductory questions.

The first question: *Prior to 9-11 what were you instructed regarding the primary security concerns for your position?* The most common response, provided by 14 of the 17 security officers, was the safety of visitors and staff. Thirteen security officers also noted the protection of artifacts and other museum property. One noted that ensuring employees carried the proper SI identification cards, which were verified at identity checkpoints, was also an important security concern.

The second interview question: *How did those instructions change after 9-11?* While five officers indicated that the procedures and instructions did not change or did not change much, six noted that identification checks (especially for outside vendors) increased, and five noted that they were instructed to increase the use of x-ray and other technologies. One of these five that discussed the x-ray machines noted that packages and other items were "not going to come in the main door, they had to go through the x-ray procedure now." Four security officers noted that they were instructed to be more

wary and suspicious of anything out of the ordinary (e.g., one noted that they "had to be more aware of unusual/suspicious people and objects left around") and three noted that bag searches were increased. One officer noted that patrols outside the building were increased and noted,

> "The change I noticed was primarily 24 hours a day; around the clock we had exterior patrol. We had an orientation on the other [non-Smithsonian] organizations around most of buildings and the 24 hour watch was [in effect] no matter what the weather was we were still out there."

The answers to the introductory questions reveal that prior to 9-11 the majority of managers and security officers agreed that the primary mission of SI OPS was to provide protection and safety to staff, visitors, the galleries, and the artifacts stored within those galleries. They similarly agreed that the aftermath of 9-11 led to many changes in the way security was conducted in the museums. The managers and security officers pointed to an increase in visitor, parcel, and bag searches; an increase in the use of x-ray machines, magnetometers, and wands[2]; as well as raised level of security awareness.

Primary Factors

SI OPS post 9-11

As detailed in Appendix I, responses to the interviews conducted with SI OPS security officers and managers, as well as a review of various published and unpublished sources, reveals that post SI OPS underwent dramatic organizational changes in an effort to upgrade their security efforts after September 11, 2001. There were four primary areas of interest for the security manager interviews: budget, screening, training, and security policy formulation process.

[2] A wand is a hand held magnetometer.

The interviews and document review also shed light on the relationships between some of the variables, primarily the prominent role budgeting plays in screening policies, officer retention, and overall security policy decisions. As such, and although not always apparent in the initial review of the findings, is the strong role budgeting plays regarding most of OPS' successes and failures. The underlying message that does appear evident is the sense of marginalization of the importance of OPS' role in the overall activities of the Smithsonian. Its role or lack thereof is questioned until an act of vandalism or other non-terrorism related incident occurs, then OPS shortfalls become apparent.

Information derived from the interviews only represents the experiences of a small fraction of security and non-security personnel who agreed to take part in this research. The small sample of security officers interviewed should be acknowledged when assessing these findings.

Screening

Structural Elements:

- **New visitor screening procedures**
- **New screening equipment**

One of the biggest changes, which had a major impact on SI OPS, was the introduction of visitor screening to Smithsonian buildings. Prior to 9-11 visitors could freely walk into the Smithsonian buildings. An interview with an SI OPS manager revealed the museums' security presence was mostly concerned with cultural property protection (theft and vandalism), visitor safety, petty crime, and other related issues. Bags were not searched except in the Portrait Gallery, and that was due to the perceived risk of vandalism, not terrorism (IWA, 2005).

In an attempt to reduce vulnerabilities after 9-11, SI OPS management implemented a new screening policy that required hand inspections of all bags carried by staff and visitors. The staff inspections continued until January 2002, while the visitor searches are still ongoing. OPS also received additional funding in FY03 and FY04 to hire additional officers and install magnetometers and x-ray machines at museum entrances (Visitor Opinions, 2002:1). Prior to conducting major installations at all Smithsonian museums, a pilot test was used at a major museum on The Mall and the Office of Policy and Analysis (OP&A) conducted a survey to gauge visitor reactions and opinions to the implementation of the new electronic screening measures and to anticipated waiting times prior to entering museums.

The survey revealed the following regarding SI OPS procedures:

- Visitors felt that inspections of visitor bags increased their feelings of safety.
- Visitors preferred electronic inspections to hand inspections of their bags.
- Visitor enjoyment of Smithsonian museums and visit satisfaction were not substantially reduced by electronic and hand searches.
- National Air and Space Museum (NASM) visitors, after installation of electronic security measures, experienced longer average waiting times to enter the museum than visitors at other museums.
- The length of waiting time at a museum entrance strongly impacted visit enjoyment especially when the time period exceeded 15 minutes.
- A small percentage of Smithsonian visitors waited more than 15 minutes and, therefore, security (hand or electronic) appeared to have had a minimal impact on visitors' agendas.
- Security measures did not discourage visitors from visiting other Smithsonian museums.
- Visitors felt that the electronic security procedures at NASM and hand inspections at other museums could be managed better. Some suggested that electronic measures should replace hand searches at other Smithsonian museums.
- The challenge associated with negative visitor reactions to the electronic security measures at NASM is principally a logistics challenge about how to handle large numbers of visitors on peak visitation dates.
- Based on the survey responses, either stopping security inspections or continuing security inspections would have approximately the same, small

> effect on Smithsonian visitation; that is, very few visitors said they would not come in both of those cases (2).

The findings of this survey were in line with the comments of many security officers and managers who were interviewed. The common theme among both groups was "visitors will feel safer if they see us doing security." With those results in hand SI OPS executives went about looking at the viability of installing visitor and bag screening equipment within the museums.

To that end, a full scale risk assessment was conducted by SI OPS and an independent contractor Applied Research Associates (ARA) in 2002. One of the areas investigated during the risk assessment dealt with the viability of visitor screening at Smithsonian museums. According to the *Final Security Recommendations Report for Secretary Lawrence Small* (2002), "The most contentious, and operationally upsetting, of all the OPS recommendations is the potential implementation of public electronic screening with x-ray machines and magnetometers at some of our public facilities (4)." This statement was based on a compilation of results of surveys and pilot programs conducted and discussed by SI OPS and the SI Security Initiative Committee (SIC).

The SI SIC was initiated by the office of the Smithsonian Secretary at the time, Lawrence Small, immediately following the events of 9-11. It consisted of upper management personnel from each museum and the Director, Deputy Director and Associate Director of Technical Security from OPS, who were the only three on the committee who had security backgrounds. The Committee met every two weeks, then monthly after a few months and continued this meeting pace until the committee disbanded in 2002. The Committee made several suggestions and recommendations regarding security issues related to the Smithsonian, many of which were incorporated

into present day SI OPS policy (IWA, 2008). The Committee found three primary reasons for screening difficulties:

1. Many facilities have insufficient space at their public entrances to support the equipment. The equipment would have to be installed so far into the building that it would greatly reduce, if not completely eliminate, the value the equipment provides in preventing the introduction of hand-delivered explosives or firearms into the building;
2. Most facility entrances also serve as emergency egress points. Installation of electronic screening equipment would interfere with, or completely eliminate, appropriate emergency egress;
3. A wait time to enter facilities greater than fifteen minutes is unacceptable according to the public survey. In those facilities that can support some equipment, it would be impossible to install sufficient equipment, ensure appropriate emergency egress and keep the public's wait below the fifteen-minute threshold (4).

These results revealed the addition of electronic screening equipment would be costly due to construction costs (for renovating lobbies), as well as the addition of more security personnel to man the equipment adequately. One of the primary issues that was interweaving throughout these committee discussions revolved around a cost-benefit analysis of implementing these security upgrades and spending the money at a site that, by all previous estimates, was considered a low threat target.

To address these perceived major problems, the Smithsonian Security Initiative Committee recommended one long-term option and the choice of one of two short-term options to address screening. The long-term recommendation called for the construction of one or more Visitor Centers where electronic screening would take place. It was noted that the addition of Visitor Centers would:

- Reduce the amount of screening equipment and support staff
- Eliminate the need for construction/renovation at each facility and move it to one single construction project
- Reduce the risk substantially and mitigate the impact of an attack because the screening process is removed from the facilities (4).

This option is still available; however, there is some uncertainty about the ability to successfully build a Mall Visitor Center as well as procure the funding for such an effort (7).

Short-term Option One recommended constructing temporary electronic screening structures, such as high-end canopies or tents, outside of those museums unable to currently support the equipment. The Committee based this determination "upon initial surveys…that unless some facilities closed select public entrances, approximately thirteen structures of various sizes would be needed to support the access control screening process (6)." This option was not considered due to the number of years it would need to be in use, lack of adequate funding, and because of difficulties with an implementation schedule (6).

Short-term Option Two, on the other hand, was much more positively received by the members of the Committee, as it was determined that OPS had the resources available to fund the measures in all existing museums (6). Option Two called for a deployment of security personnel towards the public entrances and open public spaces within each museum. This option allowed SI OPS to use additional anti-terror funding to train the staff in anti-terrorism measures that would assist them in identifying and responding to potential threats. Their increased presence in these areas, coupled with an increase in a variety functions would provide:

- A greater deterrence to potential attackers
- Increased visual screening of visitors
- Increased efficiency in bag searches
- Magnetometer screening based upon identified potential threats
- Random magnetometer screening
- Increased capability to respond and defend against a potential threat or attack
- Increased capability to evacuate staff and visitors from a

facility (6).

The Committee agreed that the methods of screening visitors (electronic vs. manual) would vary between buildings, and include manual bag checks and the use of magnetometers at some of the larger museums. Currently screening is done on a random basis, while decisions about whether to use manual or electronic methods in individual buildings are largely related to the size of the building, numbers of visitors, and the space available.

Practical Elements implemented to address Structural Elements:

- **Post 9-11 visitor screening procedures**
- **Introduction of new screening equipment**
- **Introduction of exterior and canine patrols**

Manager Interviews

Question-by-Question Review and Assessment

As SI OPS moved to implement the directives proposed by the Committee, it is beneficial to the operation of SI OPS if it were determined that security managers were on the "same sheet of music (IWA, 2005)" as the SI OPS executives and the Committee regarding the changes in screening. To that end, the fifth question asked of managers was: *Has your screening policy changed since 9-11? If so, how?* All seven managers stated that the screening policies had changed. Six of the seven noted that all visitor bags were now checked, with one noting that "we've…not always done [bag checks] before 9-11…but I guess we've become even more intrusive." Four managers indicated that random visitor searches were now being conducted, and two indicated that electronic

monitoring (x-rays, wands) were now in use. One manager stated that risk assessments at museums were now being conducted.

All seven managers stated that screening policies had changed since 9-11. The most prominent area of change was that all visitor bags and packages are now checked electronically (through the use of x-rays and/or magnetometers), as noted by 6 of the 7 managers. Random visitor searches as a means of screening have also increased as was noted by 4 of the 7 managers. Electronic monitoring of visitors and staff and risk assessments has also increased. Responses to other survey questions also reflect an increased reliance on screening technologies (e.g., in response to Question 2b on changes in security programs and Question 3 regarding officer training).

An analysis of the directives outlined by the Committee reveals that the responses provided by the security managers were in line with the agreed upon screening changes as proposed. Interviews with security managers revealed that manpower was shifted from interior patrol areas to the entrances at many museums to assist with x-ray and magnetometer searches; and magnetometer searches were put in place at some museums based on the findings of the risk assessments. Visual observation of screening practices was also performed me during my employment in SI OPS following the events of 9-11. The screening methods observed do concur with those statements outlined by security managers for this research. The visitor screening methods are not referenced in the SI OPS Training Manual; however, there are sections identifying parcel and vehicle screening policies. Interviews with SI OPS executives revealed that although the visitor screening policies were not written in the policy manual they were taught to the officers during the five week new officers Basic Entry Level Training (BELT) magnetometer and

wand training sessions on Day 12 of training. An outline of the training can be found in Appendix II.

Security Officer Interviews

Question-by-Question Review and Assessment

Just as it is important to know that OPS security managers and executives were on the "same sheet of music," it is equally important to this research to discern whether OPS security managers effectively communicated screening directives to those who are responsible for its implementation. The fourth question for security officers addressed this issue in asking: *Has your screening policy changed since 9-11? If so, how?* All 17 officers felt that their screening policies had changed. The most common response to changes in screening policies related to the use of technologies such as x-ray machines and magnetometers, which were mentioned by12 of the 17 officers. Ten officers noted that bag checks were now standard, and 7 stated that random visitor searches were now taking place where they had not before. One respondent summarized the screening policy changes as follows: "We now have x-rays, magnetometers, and wands. We search all bags and do random visitor searches."

The fifth question for non-managerial security officers was: *What are the types of inspections and searches that your security force conducts?* Ten of the security officers stated that searching visitors was a common practice, and 5 of these indicated that looking for suspicious behavior was important. One stated:

> "First thing is physical…you look at the person. That is the very first thing you do. You look suspicious, that is going to automatically give you away. The clothing, are you wearing tight clothing or are you a wearing winter coat during summer time? Are you carrying a big bag? Are you nervous or fidgety while you are in line (IWA, 2005)?"

Nine officers also indicated that bag and package checks were an important form of inspection, and 8 noted that x-rays and magnetometers were useful tools in assisting them in their anti-terror mission. Follow-up interviews with security officers reveled that many believe their increased presence, in combination with x-ray and magnetometer screening methods, may help deter any potential terrorists from entering the museums. Three officers also noted that patrolling the exterior of the building was routine (done on a regular basis throughout the day) now, two described vehicle searches, one indicated the use of K-9's in conducting searches. According to interviews conducted with SI OPS executives, SI OPS used K-9's primarily as patrol dogs until 2000 when it was decided that they should be replaced with bomb K-9's, which have been in use since.

Although the K-9's were in limited use at the Smithsonian prior to 9-11, SI OPS management believed that they provided a twofold purpose post 9-11. The first is their explosive sniffing capabilities. They provide a more hands-off, efficient method of screening visitors outside of museums. Canines are also able to survey a broader spectrum of visitors than one individual officer who is only capable of viewing (not smelling) bags, x-rays and using the wand to check one visitor at a time. Patrol canines and handlers also act as a possible deterrent to those who may be planning or preparing to transport weapons and/or explosives onto museum grounds. They also act as a possible means of increasing public confidence that law enforcement is using all available tools to protect them (Horwitz, 2005*)*. These additional steps of increased security measures implemented by OPS at the museums reveal a more proactive approach to preventing terrorism in the post 9-11 era, than previously attempted. Although there was no tangible means of measuring its effectiveness, interviews with OPS executives revealed that the

new measures coupled with the fact that no major incidences had occurred post 9-11 was a good indication that the measures were effective.

Common Themes from Security Officer Interviews

Screening

An analysis of the interviews reveals that all 17 security officers felt that screening policies had changed since the attacks of 9-11. There were three primary ways in which the interviews indicated screening had changed. First, screening using devices such as x-rays and magnetometers had increased and were the most frequently mentioned change in screening procedures. While some security officers noted that not all buildings were currently equipped with such devices, it was clear from the interviews that this was the biggest area of change since 9-11. In addition, most of the officers noted that all visitor bags and purses were now examined either physically or through the use of technical tools, and these procedures were used only sporadically prior to the attacks of 9-11. Finally, random searches of visitors had increased as a way to bolster the screening process after 9-11.

Policy

Structural Elements to be addressed:

How did SI OPS managers develop post 9-11 security policies?

As previously noted, a security initiative committee was formed after 9-11, consisting of OPS executives and non-security representatives from every SI museum. This meant that the managers of the individual museums were closely involved in the security developments. This initially created difficulties, with some resistance to

proposed initiatives such as changes to visitor and staff screening. Those who resisted the new initiatives were concerned that the new practices would negatively affect employee moral, as well as dissuade the public from visiting the museums due to long lines caused by the increased security. But, over time, it was found that this collaborative approach worked well, with the museum management providing useful input to and feedback on security policy developments (IWA, 2005). The difficulties seemed to have arisen from traditional law enforcement vs. non law enforcement communication and understanding gap. That, in this authors experience, and also as explained in interviews with SI OPS and non-OPS executives, is quite common regarding security management in public institutions (IWA, 2005). The primary disconnects manifest themselves in issues of forethought – meaning security officials generally think in terms of "what would I do if I were a terrorist?" Whereas non-security personnel tend to disbelieve such scenarios are plausible.

Despite these differences, a level of agreement was reached and the primary concern in the post 9-11 Smithsonian environment focused on addressing the major security changes and challenges that were coming to the forefront following the attacks. From the SI OPS management point-of-view the perception of a possible terror attack on SI museums seemed to be quite high, as there was a more nuanced sense that the museums were not necessarily high threat targets, but the area in which SI was located was a high threat area.

According to an interview with a top security executive, "the threat hasn't changed; rather the awareness of the threat has changed (IWA, 2005)." To that end, SI OPS set in motion a series of events to address the change in the awareness of the threat

identified in the previous risk assessments, as well as from a general recognition of a threat based on its location in relation to other, higher value terrorist targets in the National Mall area. The primary change in terms of policy processes in the security management of the Smithsonian has been the use of independent risk assessments in developing policy and strategy. Prior to 9-11 such assessments were not conducted regarding the risk of a terrorist attack; at that time performance was measured against internally defined standards and projects. Mitigation efforts were defined in terms of compliance in accordance with those internally set standards (IWA, 2005). Many of those mitigation efforts successes were based on the principle that no incidents meant the policies were effective.

In addition to the 2002, SI OPS led risk assessment (referred to in the section which addresses screening, above); another all-hazards risk assessment was contracted by the Smithsonian in 2004. Following the events of 9-11, SI OPS used several tools such as the Department of Justice's Vulnerability Assessment of Federal Facilities, the Federal Emergency Management Agency (FEMA) Risk Management Series Publication 452, as well as hired an independent contractor, URS Corporation (URS), to conduct an all-hazards risk assessment of 30 Smithsonian facilities, covering man-made and natural disasters, in an attempt to evaluate and define the specific risks to Smithsonian museums (GAO, 2007). For this risk assessment, SI OPS followed a ten-step risk assessment methodology criterion that was issued by the Department of Homeland Security. These criteria sought to address the following issues:

- Clearly identify the infrastructure sector being assessed
- Specify the type of security discipline addressed, e.g. physical, information, operations
- Collect specific data pertaining to each asset

- Identify critical/key assets to be protected
- Determine the mission impact of the loss or damage of that asset
- Conduct a threat analysis and perform assessment for specific assets
- Perform a vulnerability analysis and assessment to specific threats
- Conduct analytical risk assessment and determine priorities for each asset
- Be relatively low cost to train and conduct
- Make specific, concrete recommendations concerning countermeasures (Vulnerability Assessment Report, 2003).

The assessments were based on the FEMA Risk Assessment Model (2005). Figure 1 displays a chart of that model, which is a five-step process that requires:

> - "The first step is to conduct a threat assessment wherein the threat or hazard is identified, defined, and quantified (Step 1). For terrorism, the threat is the aggressors (people or groups) that are known to exist and that have the capability and a history of using hostile actions, or that have expressed intentions for using hostile actions against potential targets as well as on whom there is current credible information on targeting activity (surveillance of potential targets) or indications of preparation for terrorist acts. The capabilities and histories of the aggressors include the tactics they have used to achieve their ends. The next step of the assessment process is to identify the value of a building's assets that need to be protected (Step 2).
>
> - After conducting an asset value assessment, the next step is to conduct a vulnerability assessment (Step 3). A vulnerability assessment evaluates the potential vulnerability of the critical assets against a broad range of identified threats/hazards. In and of itself, the vulnerability assessment provides a basis for determining mitigation measures for protection of the critical assets. The vulnerability assessment is the bridge in the methodology between threat/hazard, asset value, and the resultant level of risk.
>
> - The next step of the process is the risk assessment (Step 4). The risk assessment analyzes the threat, asset value, and vulnerability to ascertain the level of risk for each critical asset against each applicable threat. Inherent in this is the likelihood or probability of the threat occurring and the consequences of the occurrence. Thus, a very high likelihood of occurrence with very small consequences may require simple low cost mitigation measures, but a very low likelihood of occurrence with very grave consequences may require more costly and complex mitigation measures. The risk assessment should provide a relative risk profile. High-risk combinations of assets against associated threats, with the

identified vulnerability, allow prioritization of resources to implement mitigation measures.

- The final step (Step 5) is to consider mitigation options that are directly associated with, and responsive to, the major risks identified during Step 4. From Step 5, decisions can be made as to where to minimize the risks and how to accomplish that over time (FEMA, 2005: ii)."

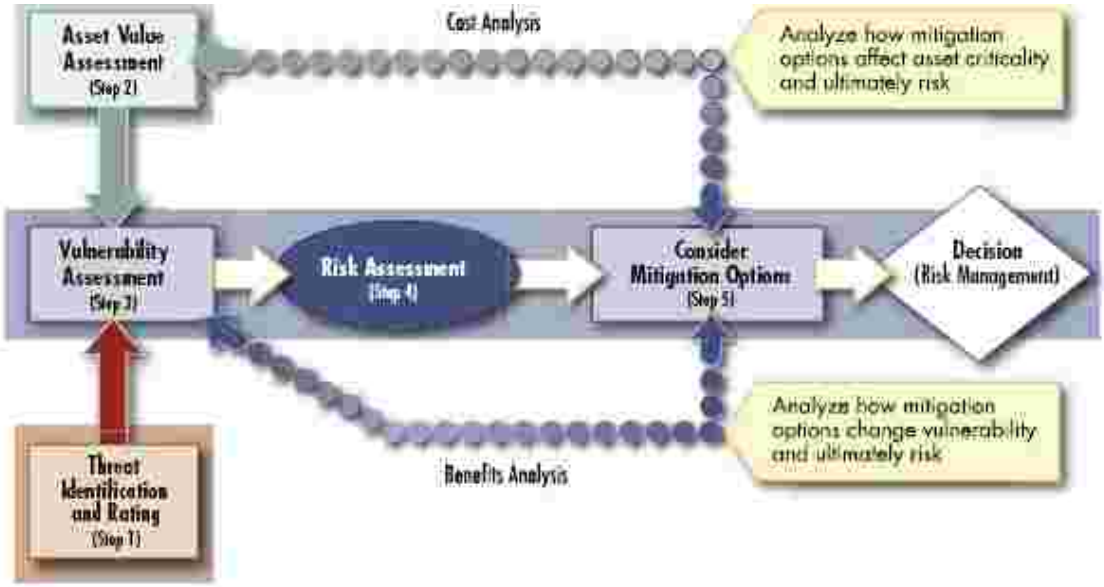


Figure 1 Risk assessment process model

*Source: Risk Management Series: Risk Assessment – A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings – FEMA 452/ January 2005

The SI all-hazards assessments only addressed disaster level risks, including terrorism, with lower-level risks such as pick-pocketing and theft still dealt with in terms of internal physical security standards. Following the risk assessments, the independent assessors were asked to consider the results of all the multi-hazards risk assessments and prioritize the top 30 projects that should be addressed. The prioritization was based on objective criteria, such as considerable loss of life, considerable loss of collections or damage to the buildings (IWA, 2005). A senior SI OPS interviewee for this study highlighted the immense difficulty of deciding how to prioritize actions across such a

large and diverse inventory. It was noted that recommended actions were rarely rejected, but may be prioritized for action over a longer timescale, and their priority may subsequently change in the light of future assessments (IWA, 2005).

A study by the GAO (2007) identified some weaknesses in the communication of information from the risk assessments, with 9 out of 14 museum and facility directors interviewed claiming that they were unaware of the outcomes relating to their own facility (32). It was noted that this meant they were often unaware of how many guards were allocated to their establishment on any one day, and made it difficult for them to work effectively with OPS in facility security management. In fact, the same GAO study found that there was even a "lack of awareness of some museum and facility directors about the all-hazards risk assessment" and this lack of awareness, "limits their ability to work with OPS to identify, monitor, and respond to changes in the security environment of their facilities (32)." It should be noted however, that OPS executives stated during interviews that they did send out email notices of the impending risk assessments, but their emails often times are ignored by non security personnel (IWA, 2005).

Practical Elements implemented to address Structural Elements:

- **Introduction of risk assessments as means to determine weaknesses**
- **Formation of the SI Security Initiative Committee to recommend security policy changes**
- **Increased understanding and awareness of the "threat"**
- **Increase in communication with Security Officers regarding the "threat"**

Manager Interviews

Question-by-Question Analysis

Two questions were posed to OPS managers regarding the security policy formulation process. The first of which was interview question six: *Has your approach to security changed since 9-11? If so, how?* All seven managers stated that their approach to security has changed, with one noting that "I think awareness of what's going on around the country from a security perspective and also from a staff perspective has really increased" and another stating "I think you put more emphasis on certain areas." In terms of how the approach to security had changed, three of the managers noted that the primary change was in an increased understanding of the threats and an emphasis on vigilance. Two noted that communication between officers had increased, with one noting "staff, at the drop of a hat, is willing to report something… suspicious where they hardly would at first."

The second policy planning question was interview question seven: *How do you guide your subordinates regarding post 9-11 security?* Four of the seven managers indicated that teaching security officers to act independently and to trust their instincts was an important aspect of post 9-11 security, with one noting, "My style is that you shouldn't have to call the supervisor if you know what you are doing, if you fall back on your training, your experience and use your common sense." Four managers also noted

that additional briefings, meetings, and information provided to officers allowed them to more effectively do their jobs. Two indicated that increased training (particularly with respect to new technologies) was an important aspect of security, and two indicated that communication among officers and between officers and supervisors was important.

Common Themes from Manager Interviews

Policy Formulation

Results related to several of the questions on the manager interview guide, as well as through a review of several documents indicated that substantial changes in policy were made following the attacks of 9-11. Increased awareness of the possibility of terrorism and a fundamental shift toward an increase in the level of concern about possible terrorist attacks have driven substantial changes in the security process. The risk of terrorism was also heightened because of the Smithsonian's unique role as the protector of "critical assets and symbols of the United States." Additionally, as the Smithsonian itself was not considered a high threat target, its location in The National Mall also made the heightened threat awareness more understandable.

Through training and direction from supervisors, security personnel are meant to be more prepared to handle emergencies and to be more suspicious and guarded in their work. The increased awareness of possible terrorist acts in combination with the findings from the risk assessments has also driven an increased emphasis on using new technologies such as x-ray machines and magnetometers in the course of providing security. Based on these findings SI OPS recommended "several physical and operational procedures at facilities that have the greatest risk of attack (Office of Facilities Engineering and Operations, Office of Protection Services, 2002: 1)." Those

recommendations came in the form of additional screening of both individuals (staff and especially visitors), and thorough bag and package screening procedures.

Training

Structural Elements to be addressed:

- **Introduction of anti-terror curriculum into officer training**
- **Introduction of new search technology into officer training**
- **Lengthening of Officer training**

Following the events of 9-11 the federal government redirected much of its funding towards federal, state, and local law enforcement agencies to enact new anti-terrorism programs. According to Joey Weedon (2002),

> "The terrorist attacks on the World Trade Center and the Pentagon have had a dramatic impact on federal priorities, redirecting them toward efforts to strengthen the government's ability to protect Americans against terrorism. To accomplish this, the Bush administration has proposed shifting federal dollars away from programs that are considered duplicative, unproven or ineffective concerning terrorism preparedness. In light of this, several of the nation's federal crime programs…have become candidates for restructuring, consolidation or elimination. The law enforcement community needs to be proactive in protecting against terrorism and federal funding for these efforts must be proactive (to prevent future terrorist acts) and reactive (to help minimize the damage in the event of future terrorist acts) (18)."

The changes in the nature of security management in the Smithsonian, especially the introduction of screening, have had major implications for the training of staff. A senior SI OPS representative interviewed for this study noted that training for new entrants increased from 2 weeks to 5 weeks after 9-11, with existing employees also having to receive the additional training. Refresher training is also provided. The training includes how to conduct bag searches and how to operate the various types of screening technology in use, as well as anti-terrorism measures. The GAO (2007) report also noted

the change in the length of training and how it also provides "customer service training and instruction on the use of magnetometers, X-rays, and bag searches (72)."

To that end SI OPS received additional anti-terror (AT) funding following 9-11. The below figures show the additional amounts:

- FY03 - $7,719,000 in AT Funds for hiring additional officers
- FY04 - $7,625,000 in AT Funds for maintaining the FY03 training and hiring budget increases above.

Weapons and bomb detection also became a concern of SI OPS, which is evident in their increased training on vehicle and parcel inspections, as well as on the increase in certifications on x-ray and magnetometer use. In addition to the WMD, vehicle and parcel screening training, there were also two other major areas of training that have been the focus of SI OPS since 9-11. The first is certification on x-ray and magnetometer use; and the second is baton and weapons training. Officers also received "verbal judo" training to assist them in calming verbal confrontations (see Appendix II regarding the 5-week Officer Training curriculum).

The anti-terror awareness training was important in that it also expressed the importance of not only being able to identify signs of possible terrorist activities, but it also provided background information on the various groups involved in terrorist acts. This concept was important for the officers because it moved them away from the typical stereotyping of individuals and moved their focus towards trends or patterns. Edwin J. Delattre (2002) wrote about the importance of anti-terror training in the wake of 9-11 and notes,

> "September 11 did not change human nature, any more than it changed the need for both virtue and accountability in policing and every other walk of life where the public trust is at stake. Furthermore, because all know-how can be used both ethically and unethically, the better the training police receive, the more

extensively the public interest depends on their having good character and their being accountable within their departments (1)."

Maintaining adequate training funds has been a continuing effort on the part of SI OPS executives as it is a very expensive venture for federal law enforcement agencies especially during times when budget cutbacks are taking place. Despite these cutbacks more security personnel are needed to accomplish an already daunting task of providing for the safety and security of visitors, staff, and the artifacts. This is in addition to the fact that the Smithsonian is not considered a high threat target, yet, "because of their location, could also suffer collateral damage from attacks on other nearby targets or be attacked as an alternative to attacking a desired target that is more heavily defended (such as the U.S. Capitol) (Office of Facilities Engineering and Operations, Office of Protection Services, 2002: 1)."

Practical Elements implemented to address Structural Elements:

- **Introduction of X-Ray and Magnetometer training**
- **Increase in emergency response scenarios**
- **Increase in length of training**

Manager Interviews

Question-by-Question Analysis

One question was posed to OPS managers regarding changes in Officer training following 9-11. Question three was: *Has officer training changed since 9-11? If so, how?* All of the managers agreed that training had changed since 9-11. Five of the seven indicated that training for the new and more common technological devices was increased (primarily for x-ray machines, magnetometers, and electronic batons); three mentioned that training in emergency management became mandatory. For example:

> "We've had drills where if there's an explosion or something like that on the outside…we have a program called *shelter and place* that designated area that we move the public and staff to for shelter and place. We also have emergency evacuations where we get people from the inside outside."

Two managers indicated that weapons, baton, and use of force policy training was increased (see Appendix II). One noted that training became more frequent (i.e. "Reinstituted in-service training for the officers on a yearly basis, rather than every 2 years") and one noted that training of an interpersonal nature was instituted (i.e. "verbal judo training…and added public interaction skills training"). (See Appendix II for a list of Officer Training Courses).

Common Themes from Manager Interviews

Training

In general, responses to Question 3 on officer training changes since 9-11 indicated that training had changed (with all 7 managers noting that this was the case). The primary area of training was on the use of the new electronic technologies such as x-ray machines, magnetometers, and batons. Some increase in training was also seen in emergency management and the use of weapons, and there was brief mention of interpersonal skills training and an overall increase in the frequency of various types of trainings. From Question 4, however, only 1 of 7 managers stated that the increased funds following 9-11 were used to increase training, and from Question 7 only 2 of 7 managers noted that they guide their subordinates through practices learned from training exercises. Therefore, it appears that following the attacks of 9-11 there were some changes and increases in training, but that these have yet to be fully and successfully integrated into the security process.

Security Officer Interviews

Question-by-Question Review and Assessment

The same question asked of OPS managers was also asked of the officers. The third interview question was: *Has your training changed since 9-11? If so, how?* Sixteen of the officers indicated that their training had increased. In terms of the specific areas of increased training, 14 of the 16 officers who stated that training had increased specified training in the new technologies such as x-ray and magnetometer training. In addition, 3 officers stated that they had received additional search training, and 2 stated that they had received training in shelter usage. (See Appendix II for a list of Officer training courses).

Common Themes from Security Officer Interviews

Training

Sixteen of the 17 security officers felt that training had changed since 9-11. For the most part, training changes were related to the use of the new technical tools. Some training in conducting searches, shelter usage, and other emergency response capabilities also may have increased, but these were mentioned infrequently by the security officers. Some officers, however, did not feel the new training was thorough enough. Regarding this one officer stated, “We need more on the job training regarding fire drill instructions, how to handle terrorist situations, and we need more security officer visibility. We need to be around in large force so people feel safe when they visit the museums.” Another officer stated, “They [management] need to bring some outside security people to train us and bring in new ideas.” A third officer stated, “We need to be more proactive towards security, rather than reactive towards security training.”

The findings appear to show that while officers believe the bulk of new training focuses on the use of new technical devices, there still seem to be some shortfalls regarding anti-terror measures, the need for new security approaches, and finally on changing the overall OPS mindset from a reactive to a proactive force.

Budgets

Structural Elements to be addressed:

- **Increase in budget needed to address new post 9-11 screening technology**
- **Increase in budget needed to address pre-existing security needs**
- **Increase in budget to address high officer turnover and recruitment**

The changes in the nature of the security environment have meant that the costs of maintaining a post 9-11 SI OPS force have increased. This increase was identified and the result was an expansion in the SI OPS budget from $37 million in 2001 to $67 million in 2006 (GAO, 2007:33). The additional funding was used to upgrade officer training and equipment, as well as provide overtime for officers so they could conduct additional exterior roving patrols around the Mall museums.

Yet despite these steady budgetary increases, other organizational costs coupled with the need to address already existing OPS shortfalls, as well as post 9-11 security concerns, OPS was still suffering from a considerable funding shortage and the ability to obtain additional funding has become a major challenge. In 2005, as a response to the growing budgeting challenges the Smithsonian's Board of Regents was required by the GAO to develop and implement a funding plan in response to findings that existing levels were becoming inadequate. It does appear, however, that some of the funding inadequacies could be alleviated by a shift in funds at the Smithsonian. According to the GAO report, the SI OPS is funded entirely through federal government funding, and

Smithsonian officials feel it is the federal government's responsibility to continue to address the security funding issues. The report continues, "While Congress does appropriate funds every year for security expenses, the Smithsonian could raise additional revenue or use unrestricted funds for its security expenses (33)."

One area of inadequacy identified was $31.3 million in security projects that since 1999, had only received $17.6 million to complete those security upgrades. The other area identified related to security officers and their steady decline in numbers since 2003 (GAO, 2007: 33). It has been reported that the Smithsonian's two most visited museums, the Air and Space Museum and the Museum of Natural History, both experienced a 31 percent decrease in security officers since 2003, and that the overall number of security officers had fallen even though the overall size of the museums and total number of visitors had increased. Although more technology security equipment had been installed, it was reported that levels of vandalism and theft increased during that time (GAO, 2007).

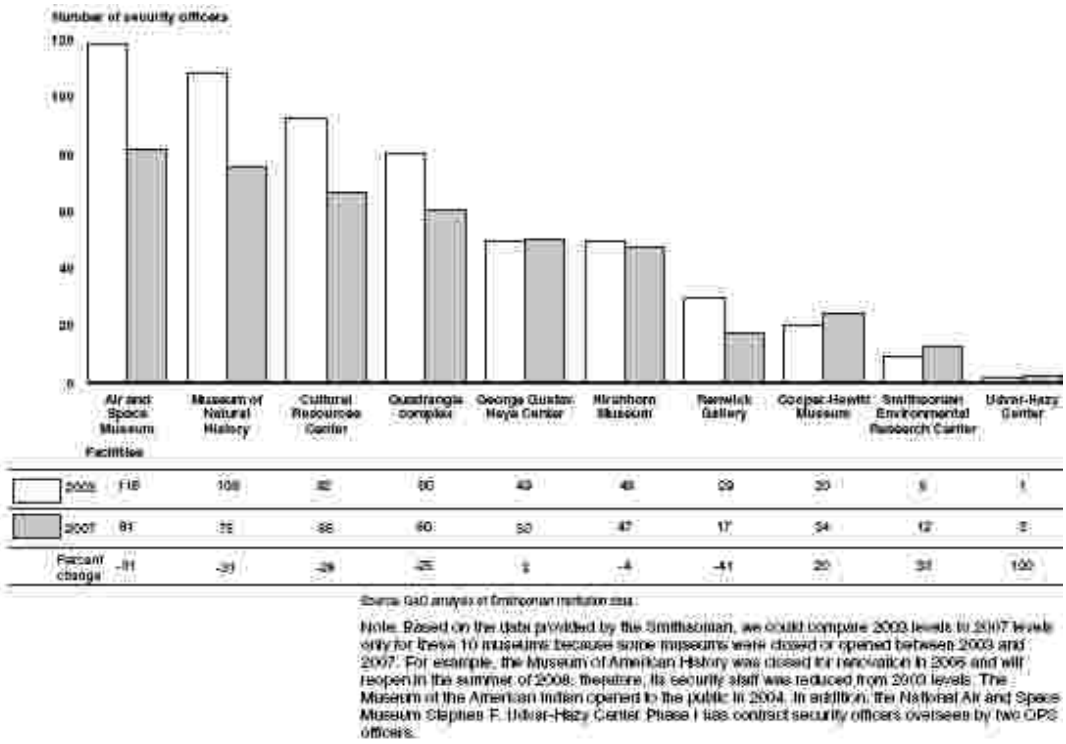
Funding constraints also reportedly made it difficult for SI OPS to recruit and retain security officers because they were regularly able to find higher paying positions at other federal agencies (GAO, 2007). Regarding this one manager noted, "The biggest problem is found in manpower. There just isn't enough money available to hire the adequate number of officers needed to address our new concerns (IWA, 2006)." He continued, "Even when we are able to bring people in and train them, they leave because our salaries aren't as competitive as some other agencies (Ibid)."

As the post 9-11 budgeting shortfalls have led to high officer attrition rates it has also led to major manpower and security issues within Smithsonian museums. Interviews with OPS security personnel, as well as a review of the GAO report reveal one museum

having to close its main entrance due to an inadequate number of officers; other museums having to share guards; lack of officers to check alarms; and Smithsonian's inability to acquire collections on loan due to lenders concerns with the Smithsonian's inability to protect their pieces (GAO, 2007). The resultant loss of security officers may be the underlying impetus behind a rise in non-terrorism related incidents at Smithsonian museums (compared to previous years) and "according to museum and facility directors…in the absence of more security officers, some cases of vandalism and theft have occurred…35 cases…were reported from January 2005 through August 2007 (33)."

The findings outlined in Table 6 show an officer decrease in five of the ten Smithsonian facilities of 25 percent or more; one with 28 percent; another with 41 percent; while two of its most visited museums experiencing reductions of 31 percent in 2007 compared with 2003 (36). The GAO report further notes that the manpower issues occurred despite a reduction in the number of opened Smithsonian facilities that were in operation. This reduction is also coupled with a recent increase in the attendance of visitors to these facilities (GAO, 2007). SI OPS executives attempted to address the manpower problems by submitting a request during the budgeting process to raise officer starting salaries from General Schedule 4 and 5 to a General Schedule 6 beginning in FY04. This request was denied, however, by Smithsonian management based on inadequate funds in the Smithsonian budget, as well as higher internal budgetary priorities (37). These budgeting priorities are a result of a situation in which OPS security funding needs must compete with maintenance needs for facilities, which "forces a balancing of priorities in both areas, sometimes against one another (34)."

Table 6 - Identifies the decline in security officer levels at SI facilities.



*Source: GAO-07-1127 - Report to Congressional Requesters: SMITHSONIAN INSTITUTION Funding Challenges Affect Facilities' Conditions and Security, Endangering Collections, 2007.

The budgeting constraints have also spilled over into other areas in addition to those encountered with hiring and maintaining an effective security officer corps. Interviews with security officers revealed complaints about poor equipment (radios, weapons, etc), as well as an inability to receive an adequate number of uniforms. Interviews conducted with management revealed a frustration with the budgeting situation because they believed OPS was in a "lose-lose" situation. The findings from the interviews, as well as the supporting GAO study appear to conclude that on one hand OPS is a vital asset to the museum because is provides protection to the visitors, staff, and the art from theft and vandalism. Yet on the other hand, because SI is considered a

low risk target obtaining the needed additional funding is difficult because policy makers believe it could be better used in areas where a more urgent need exists.

In an effort to assist the officer shortfall, the Smithsonian implemented a new program in the summer of 2007 to hire college students to act as gallery attendants. The primary purpose of the program is to place attendants in the galleries with the greatest officer shortfalls, and to have those attendants act as additional security for OPS (GAO, 2007).

Practical Elements implemented to address Structural Elements:

- **Steady increase in budget post 9-11**
- **New technology purchased and implemented at most museums**
- **Funding shortages and inability to provide better compensation continue to hinder retention and recruitment**
- **Implementation of college students attendant program**

Manager Interviews

Question-by-Question Review and Assessment

One question regarding the budget was asked of the managers. The fourth interview question for managers was: *Has the OPS budget changed since 9-11? If so, how?* All seven managers indicated that the budget had increased since 9-11. Six of the seven managers indicated that funds were used to hire more security officers, but three of these said that more personnel still needed to be hired. As stated by one manager, "We received extra money for antiterrorism and to hire new officers. Despite that we still have a lack of resources and I'm sure if you talk to other managers the personnel shortage is basically our number one issue right now." Three managers stated that the additional funding was used for new technologies and equipment, but a fourth stated that they still lacked the equipment to be effective in detecting people entering the museums carrying

explosives or other weapons. When asked about his use of the term “effective,” the manager stated that without the proper screening and detection equipment his officers would be less able to detect all of the different types of materials that could be hidden on one’s person and carried into a museum. One other manager indicated that additional resources were used for increased training.

Common Themes from Manager Interviews

Budgeting

Question 4 on the manager interview guide related to whether the OPS budget had changed since 9-11. All seven managers indicated that the budget had increased since 9-11. In terms of where the additional funds were spent, hiring additional security personnel was the most common response (given by 6 of the 7 managers). However, three of these six managers cited problems with staffing and noted that more security officers were still needed. New technologies such as x-rays and magnetometers were mentioned by 3 managers as purchases made with the larger budget (and 1 of these 3 indicated that still more new technological devices were needed). Only one of the seven managers indicated that additional funds were used to increase training. Therefore, we can conclude that (a) managers have seen an increase in funds since 9-11, (b) that the bulk of the new funds were spent on hiring additional security personnel but that more are needed, and that (c) the additional funds were also used to increase the use of technology in the security operations.

Security Officer Interviews

Question-by-Question Review and Assessment

The same question regarding the budget that was asked of the managers was also asked of the officers. The sixth and final interview question for the non-managerial security officers' interview guide was: *To your knowledge has the OPS budget changed since 9-11? If so, how?* Fourteen of the officers stated that they did not know if the budget had changed, two noted that funding had increased, and one felt that it had decreased. Representative responses to this question were: "Don't know, but we need better equipment," "I don't know, but we need updated equipment like radios, weapons, and better uniforms," and "If it has, then we don't see any of it. We need more and better equipment. Need better weapons, and more training regarding counterterrorism would be helpful."

Common Themes from Security Officer Interviews

Budgeting

Only one interview question addressed issues related to budgeting, and by and large the respondents did not provide relevant information regarding the budgeting process. In fact, 14 of the 17 officers interviewed stated that they did not know if the security budget had increased, decreased, or stayed the same since 9-11. Of the three who had an opinion, two felt that funding had increased and one felt that it had decreased.

Summary of Findings

The managers and security officers interviewed for the current study were nearly unanimous in feeling that budgets, screening processes, training, and security policies had changed dramatically since the terrorist attacks of 9-11. The most frequently mentioned changes were related to new technologies for screening (both for objects such as bags, purses, and packages, and for individuals including staff and visitors) and the security process in general. In addition, the bulk of training opportunities provided to security officers were related to the use of new technologies. However, some managers stated that budgeting increases were most commonly used for hiring new security personnel rather than for the purchase of new technological tools or training despite the fact that the previous section indicates SI Executives stated and the 2007 GAO report indicates that technology enhancements were a major purchase. While all managers indicated that budgets had increased after 9-11, several indicated that the initial increase in funding had not been sustained, and that the hiring of new security personnel had not been satisfactory. Furthermore, a review of documents has indicated that budgeting constraints have hindered OPS' ability to hire and retain security officers and has led to a rise in non-terrorism-related incidents.

In terms of broad changes to security policy, it was clear from the interviews (particularly those with the security managers) and a review of documents that the focus had shifted from concerns about theft, vandalism, and other traditional crimes to concerns about terrorism, and that this shift in focus has resulted in infrastructure changes in the security apparatus. Greatly enhanced screening procedures (particularly those involving

the use of new technological tools) coupled with an increase in security training were the primary outcomes of the new focus on the potential for terrorist activity.

Chapter 6

Summary and Discussion

The purpose of this chapter is to highlight some of the central themes that are woven throughout this dissertation; expand on the connection between the four factors; and to compare the changes within a similar low risk, high threat area, publicly accessible organization.

Three observations are evident following the analysis of the literature and interviews three dominant observations have become evident in this dissertation. The first relates to response in the wake of a major crisis; specifically the tendency for governments and organizations to respond quickly to crises, and implement measures to ensure a similar event does not occur. However, once the crisis passes without another reoccurrence there seems to be a fall back to pre-crisis thinking and behavior. The second theme relates to PET and how it provides a means to consider organizational changes after a dramatic event, and the anticipated characteristics of the changes. The third and final theme explores how organizations confronted with the terrorist threat after 9-11 are useful places to explore how organizations respond to the events. This third theme applies particularly to organizations that must balance the security demands encountered in areas that allow virtually unfettered public access, while at the same time not overburdening the public with such an intense security environment that it will deter them from visiting the organization (the National Gallery of Art in Washington, DC is another example of a similar organization). The emphasis of this dissertation has been on one such organization – the Smithsonian Institution.

The primary factors used to examine the process of change in SI OPS, as found in Chapter 5 are: screening, the policy process, budget, and training. The manner in which these variables were approached by OPS pre and post 9-11 shed some light on the broader question of how a low risk target in a high threat setting responded to the changes in the security environment caused by 9-11. This chapter reviews the relationships predicted by PET and what empirical research finds concerning those relationships; the findings of this study and whether these are consistent with existing research findings; the policy implications of the findings; and types of additional research that would further contribute to the state of knowledge about punctuated equilibrium and organizational change.

The use of PET to explain change in SI OPS

This section will consider how well PET has helped put the SI OPS changes into an organizational framework in the years following 9-11. Specifically, the findings support the belief that there was an increase in the post 9-11 security posture; however there have also been subtle/underlying tensions and issues that have also been brought to the forefront regarding the applicability of this study towards other similar organizations. PET, as it relates to this study tells us that in the pre 9-11 years SI OPS moved along in a state of limited or no change only to be jolted by the terrorist attacks of 9-11. This event caused OPS to quickly adjust the way they were conducting business across the four factors being studied in an effort to adapt to the crisis.

As previously noted, the use of PET in this research is not intended to provide any major theoretical advancement within PET literature. Rather, it provides a background to be used to examine and understand the SI OPS post 9-11 security changes. It is also

useful in helping organizational managers in SI OPS and similar institutions better plan for and implement change to maximize effectiveness after a crisis. For example, it could demonstrate that some processes of change cannot be effectively explained by the punctuated equilibrium model, at least in the form in which it is currently defined in the literature, and help stimulate the development of refined or alternative models.

This dissertation demonstrates that one can investigate actual organizational change in the aftermath of a major external crisis. This type of change can also be studied within the framework of the punctuated equilibrium model. This dissertation has also shown that there are three primary manifestations resulting from this scenario: (1) after the crisis there is an initial definitive shock to the organization (SI OPS) which then prompts a push for immediate change within the organization (screening, policy, training, and budgetary needs); (2) some of the initial changes are sustained, while others are dismissed due to financial reasons, impracticability, or due to fears that visitors will be negatively impacted and not return to the facilities; and/or (3) some of the changes are sustained in an environment where they are unwanted (visitor screening at some of the museums).

If PET provides a useful framework for explaining the changes that occurred in SI OPS after 9-11, it can be expected that a number of factors will be observed to be present in the organization, as indicated by the model itself and by previous empirical studies. These are: 1) evidence of a relatively long period of gradual, incremental change, followed by a relatively short period of radical change in response to extraordinary events; 2) knock-on effects from change in deep structure variables to other aspects of the organization (see underlying issues); 3) the development of a relatively stable

reconfigured organization which has adapted to changes in the external environment; 4) evidence of a change in the issues given focus or attentiveness by the organization and its members, and 5) evidence of considering the costs of implementing changes in response to external events.

These five factors are used to review the organizational changes which occurred in SI OPS in relation to the four key areas of activity, defined in terms of the punctuated equilibrium theory as deep systems: screening, the policy process, budget and training. Finally, the overall changes that occurred in SI OPS are summarized and considered in relation to the model. The following sections related to the four factors will explore the pre and post equilibrium differences, if any, that took place at SI-OPS (See Appendix II).

Screening

Data derived from interviews and document reviews revealed that SI OPS underwent dramatic changes in its screening processes to adapt to the changing and evolving threat environment caused by the events of 9-11. Prior to 9-11, protection of the galleries, artifacts, and other property was of primary concern, since theft or vandalism had been the main perceived threats for a prolonged period of time. Screening consisted mainly of random and infrequent bag checks for members of the public entering galleries; only a few manager participants in this research mentioned other screening devices such as cameras and other security equipment. In the aftermath of 9-11 many changes took place to increase the overall security of the museums, including an increase in visitor, parcel, and bag searches; perimeter roving patrols; an increased use of canine searches; an increase in the use of x-ray machines, magnetometers, and wands; as well as a general increase in security awareness. Prior to 9-11, the screening processes used had been

relatively unchanged; this distinctive change suggests that the punctuated equilibrium model may be an effective tool for understanding the developments that occurred regarding screening.

The model also appears to fit what has happened over time since 9-11 in this area of SI OPS' work. The initial period of intensive screening of visitors was a temporary one, which was subsequently replaced by a series of more discrete measures such as random screening protocols, electronic screening of mail, and the use of surveillance technology used throughout SI in the form of closed circuit television cameras. The pattern of change in SI OPS' screening processes pre and post 9-11 can therefore be seen to fit the punctuated equilibrium model very closely. First, a relatively stable, continuous period of little change existed for years prior to 9-11. The reaction to the terrorist attacks sparked a period of radical change in which screening was used very intensively, and which resulted in considerable disruption, inconvenience and cost to the organization. This included a considerable increase in visitor complaints three years after the 9-11 attacks when levels of public concern about security had perhaps subsided a little. Finally, the organization implemented a new range of screening measures that addressed more of the security concerns of the post 9-11 environment, which were also more acceptable to its employees and visitors, resulting in a return to a more comfortable environment for visitors and employees, in which screening is still robustly conducted but in a way that alleviates some of the immediate post 9-11 "fears." One of the goals was to implement a screening procedure that portrayed a sense of safety for the employees and visitors rather than a sense of fear.

The interview data also revealed that although terrorism was something that managers and security officers were aware of, they had given this factor little attention or consideration in developing screening techniques prior to 9-11. This may be due to the lack of major terrorist incidents in the United States prior to 9-11 and it (terrorism) was therefore perceived as a low threat. The events of 9-11 brought about a serial shift in which disproportionate attention was suddenly placed on terrorist threats compared with other factors, as per Jones and Baumgartner's (2005) refinement of the punctuated equilibrium theory, which suggests that decision makers must determine which information to attend to, and which information to assign a priority to. In the post 9-11 OPS process, this meant that terrorism became a much larger priority, than it ever had been in the past and thus more resources were deemed necessary to address the security issues related to it. Jones and Baumgartner's institutional friction model can also be seen to explain the changes in screening processes, in that these changes incurred very high costs to SI OPS, which could not have been justified prior to the 9-11 attacks.

The costs of implementing these changes also forced SI OPS executives to tailor their initial screening suggestions. As previously noted in Chapter 5, the SI Security Initiative Committee proposed a number of anti-terrorism measures to implement at all SI facilities. These measures included vehicle barriers, electronic screening of the public, installation of anti-shatter window film, and a separate screening facility located near the National Mall, to name just a few of the proposals. However, due to limited funding, the committee looked at the findings from the most recent SI facilities risk assessment and opted to strategically implement some of the proposals at the higher risk facilities rather than at all facilities.

Security policy process

The punctuated equilibrium theory model of policy change (True, Baumgartner, and Jones, 1993) states that policy generally changes only incrementally as a result of restraints including lack of institutional change and the bounded rationality of individual decision-making. Regarding this they note, "Stasis, rather than crisis, typically characterizes most policy areas. However, crises often occur. Dramatic changes in public policies are constantly occurring…as public understandings of existing problems change (97)." Under this assumption, policy is characterized by long periods of stability, punctuated by large, but rare, changes due to large shifts in society or government.

The research findings derived from interviews and reviews of pre and post 9-11 OPS policies support this notion. There was little evidence from the research of any major developments in OPS policy in the period preceding 9-11. In the aftermath of the terrorist attacks OPS executives participated in the SI Security Initiative Committee, commissioned two all-hazards risk assessments, implemented a new Basic Officer Training curriculum to include x-ray, magnetometer, baton training, and anti-terror training, and implemented new screening policies throughout Smithsonian facilities. This seems to represent an unprecedented level of policy change in SI OPS, which was sparked off by a single extraordinary event, and therefore fits the punctuated equilibrium model well.

An immediate response to the changed external environment was the formation of the security committee, consisting of OPS executives and non-security representatives from every SI museum that met regularly in the year following the attacks. This committee was instrumental in first defining the issue the organization needed to address

and framing this in terms of a policy agenda. From this starting point, it was largely responsible for revising and implementing new security policies and helping to ensure that all personnel were aware of the security threat and the new policies and procedures, even though there was evidence of weaknesses in its effectiveness in the area of communication.

One of the major changes which occurred in policy was the increased involvement of museum managers themselves in the development of new security policies and procedures, a collaboration which was very important in contributing to their effective implementation. However, this did not go entirely smoothly, since there were conflicts between security and non-security specialists and apparent gaps in communication in some areas (see Chapter 7 for further analysis regarding communication). Once again, this finding fits with the explanation of punctuated equilibrium theory in terms of a period of relative disorder and disorganization, while the organization adapts its structures to the changed external environment.

The key change in the policy process in OPS security management has been the use of independent risk assessments in developing policy and strategy. Prior to 9-11 such assessments were not conducted regarding the risk of a terrorist attack; at that time performance was measured against internally defined standards and projects and mitigation efforts were defined in terms of compliance with those standards (IWA, 2005). In line with the punctuated equilibrium model, therefore, a new approach to policy making which reflected the changed external environment eventually replaced the traditional one.

Budget

Baumgartner and Jones (1993) also apply different models of punctuated equilibrium theory to budgeting. One in particular that appears to fit the model of SI OPS is the agenda-based model of national budgeting, which implies that generally "budgets change only incrementally." However, sometimes issues move from subsystem politics to macro-politics, and national attention in the Congress and in the presidency is, of necessity, given to one or a few high-profile items at a time…policies and programs can make radical departures from the past, and budgets can lurch into large changes (165)."

This demonstrates how the process of change occurs through knock-on effects through various levels of deep structure in an organization, following an internal or external shock. In the case of SI OPS, the 9-11 attacks resulted in a radical policy change that required and facilitated a significant expansion in budgets to support new security measures. Prior to 9-11, there was reportedly a steady, incremental increase (5% to 10%) in SI OPS budgets over time. In the period following 9-11 however, major increases in funds were required to purchase, install and provide training in the new screening technology and to recruit additional officers to increase the security presence and to address the high turnover being experienced at this time. As a result, there was an expansion in the SI OPS budget from $37 million in 2001 to $67 million in 2006 (GAO, 2007:33).

Despite these increased budget provisions, meeting the new security demands has continued to be a problem. Many managers reported that funding shortages and the inability to provide better compensation were continuing to hinder retention and recruitment of officers. The post 9-11 salary shortfalls have led to high officer attrition

rates and also to major manpower and security issues within Smithsonian museums, especially a rise in non-terrorism related incidents such as vandalism and theft, which eventually resulted in the implementation in 2007 of a scheme using college students as gallery attendants. Although attributed primarily to the budgetary shortcomings, the increase in non-terrorism incidents might be explained in terms of Jones' disproportionate information processing theory. This theory suggests that decision making inputs do not relate directly to the outputs and "As a consequence, there is an imperfect match between the adaptive strategies people devise and the information the receive (2001:9)." This is seen during the post 9-11 period where the focus of attention in SI OPS, as well as its funding, became disproportionately directed on the threat of terrorism at the expense of other types of risks.

At the same time, budgeting was shown in the study to play an integral and prominent role in relation to other areas, such as screening policies, officer retention, and overall security policy decisions. In understanding the specific processes by which change throughout the organization takes place, the role of budgets cannot be underestimated, since they act as a constraint on what is possible, and a tool for directing the resources which facilitate and drive change within an organization.

Training

The changes in the nature of security management in SI, especially the introduction of screening, have had major implications for the training of staff. The primary implication came in both the quantity and the content of training that was developed within a short time after the 9-11 attacks. Traditionally, officers received two weeks standard training on entry, but this was increased to five weeks training after 9-11,

with existing employees also having to receive the additional training, and refresher training also being provided. The new training has a more explicit emphasis on anti-terrorism measures, including how to conduct bag searches and how to operate the various types of screening technology in use, as well as more general anti-terrorism awareness training more generally.

The anti-terrorism awareness component was a particularly significant aspect of the training and one which represented a novel approach. It provided officers with background information on the various groups involved in terrorist acts. It was hoped that this training would move their focus towards patterns of behavior or characteristics. Officers also received "verbal judo" training to assist them in calming verbal confrontations.

The radical change in the amount and nature of training provided to SI OPS officers again fits well with the punctuated equilibrium model, representing a clear break with the situation that existed with regard to training pre 9-11 and establishing a new pattern in its place. However, the qualitative research revealed weaknesses and gaps in the provision of training to all officers, as well as reported shortcomings in budgetary provision for the delivery of training.

These findings can also be explained by the punctuated equilibrium model. The changes in training which occurred post 9-11, can be seen to be dependent, knock-on effects of the policy developments which were a response to increased awareness of the terrorism threat, and of the increased budgets that were made available to support the implementation of these policy developments; it is unlikely that change in training provision would have occurred independently as a direct impact of the events of 9-11.

This also provides a good example of the way in which change occurs throughout an organization disturbed by an external event, as movement in one level of deep structure has knock on effects on other levels in the process of reconfiguring the deep structures which make up the organization. Developments in training were an indirect rather than a direct response to the terrorist attacks, and were therefore subject to the multiple effects of any constraints or weaknesses which emerged as other deep structures such as policy and budgets were reconfigured, resulting in less radical changes overall in this particular area of activity. Training budgets were somewhat constrained, in particular, by the continued official categorization of the Smithsonian as a low-threat target, despite being located in a high-risk area.

Similar Organization, Similar Circumstances?

The 9-11 related organizational changes in the screening, training, budgeting and policy practices of the SI OPS have parallels with other similarly situated institutions. . Following the events of 09-11, federal agencies located on the National Mall (SI, Department of Agriculture, the National Park Service, Department of the Interior, and the National Gallery of Art) have allocated approximately $132 million towards physical security enhancements to include additional security personnel, facility upgrades, barriers, and equipment and technology (GAO, 2005) with the hopes of protecting the facilities and the visiting public from any future attacks.

The National Gallery of Art (NGA) provides a useful point of comparison for this study for two primary reasons. First, similar to the SI, the NGA is located in a high threat area of The National Mall in Washington, DC, but is itself considered a low risk target. Second, similar to SI, NGA must balance its role as a public institution which thrives on

allowing virtually unfettered public access, with maintenance of a security force that is placed under greater demands to provide a safe environment for all employees, visitors, and the cultural objects housed within the buildings following 9-11. This presents an opportunity to examine how a facility similar to that of SI was particularly challenged by 9-11.

The National Gallery of Art (NGA) was created in 1937 for the people of the United States of America by a joint resolution of Congress, accepting the gift of former Treasury Secretary, financier and art collector Andrew W. Mellon. Since its founding, NGA has been supported by in an effort to ensure the operation, protection, and care of the nation's art collection, thus enabling the Gallery to remain open year round at no charge to visitors.

An NGA Office of Security Executive was interviewed regarding the types of changes, if any, that have taken place since 9-11, how those changes were manifest, and which factors were driving those changes. Examination of budget, training, policy and screening were chosen because it was believed they would be able to provide additional insight on the question of change in relation to the same changes at SI OPS.

Data derived from interviews and document reviews revealed that NGA underwent dramatic changes in its screening, physical security and security budget to adapt to the changing and evolving threat environment caused by the events of 9-11. Prior to 9-11, protection of the galleries, artifacts, and other property was of primary concern, since theft or vandalism had been the main perceived threats for a prolonged period of time. Screening consisted of bag checks for members of the public entering galleries.

The discussion with the NGA security executive yielded similar responses to those of the SI OPS interviews conducted at an earlier time. The primary pre 9-11 security concerns at the NGA were to prevent vandalism and theft of the museum buildings, art objects, and to staff and visitor personal items. As the primary pre 9-11 security focus was aimed at non-terrorism related activities, the security force itself was primarily focused on checking visitor bags for items that could be used to vandalize the art such as paint, razors, etc. They also had monitors patrolling the various display rooms throughout the museum. They also required guests to bag check backpacks, strollers, umbrella's, and any other items that could be used to smuggle items out of the museums or cause any damage to artifacts. Since the screening processes used had been relatively unchanged before this time, this suggests that the punctuated equilibrium model may be an effective tool for understanding the developments that occurred in relation to screening.

Similar to the SI OPS immediate post 9-11 security environment, NGA quickly changed its focus to a terrorism based preventative program. According to a 2005 Government Accountability Office report "National Malls: Steps Identified by Stakeholders Facilitate Design and Approval of Security Enhancements" the NGA has taken a number of steps between Fiscal Years 2002-2004 towards physical security enhancements. Among these enhancements includes: new magnetometers, x-ray machines, closed-circuit television cameras, and body armor for its officers. The GAO report further notes how the NGA has also obligated funds for additional security enhancements such as: an Integrated Security Management System, the review of its

disaster management plan, and a review of past vulnerability assessments for security against explosive devices (18).

In addition to the funds requested to implement the physical security enhancements, as well as those funds obligated for future security upgrades, the NGA has also proposed a set of physical security enhancements amounting to approximately $2.2 million that they would like to implement in the near future:

- conduct additional studies to evaluate its camera monitoring systems and determine the need for an Emergency Operations Center (EOC)
- upgrade perimeter security against explosions and hazardous agents
- install additional equipment upgrade technology to include improving access controls, adding biometrics, perimeter cameras, and new screening devices (18).

PET also provides a useful framework that helps us to understand what has happened over time since 9-11 in NGA's overall security mission. The initial period of intensive screening of visitors continues, and the use of surveillance technology is now used throughout NGA facilities in the form of closed circuit television cameras. The pattern of change in NGA's screening processes pre and post 9-11 can therefore be seen to fit the punctuated equilibrium model very closely. It appears that NGA experienced a level of change within the areas of screening and its budget that, unlike SI OPS, has yet to level off to an equilibrium state. Although the visitor screening was continuously occurring in the years preceding 9-11, NGA security executives took additional action to step up the process with electronic screening devices. An additional change was the development of

levels of screening that corresponds to the color code system of the Department of Homeland Security.

Similar to SI OPS, NGA first went through a relatively stable, continuous period of little change prior to 9-11. As previously noted, the events of 9-11 sparked off a period of revolutionary change in which new screening procedures were introduced and used very intensively. However, it does not appear that these changes resulted in considerable disruption or inconvenience to the visitors or staff. The majority of cost to the organization, as noted above, came in the form of purchasing new surveillance equipment, x-ray machines, magnetometers, and adding additional security personnel. Although NGA conducted visitor bag searches prior to 9-11, the new range of screening measures were more suited to the post 9-11 environment.

The post 9-11 environment ushered in a change of focus for the NGA, as the security concerns began to include terrorism. That's not to say that terrorism was not a concern prior to 9-11; rather it was just something to be aware of. To address those concerns NGA added additional officer training for magnetometers, X-ray machines, shelter in place drills, and evacuation scenario training. The primary goal of these additional protocols has led to a greater awareness of the consequences of terrorism and has led to a process to put in place or eventually put in place measures to deter, stop, or mitigate any terrorist events within the NGA facilities.

Fear of Complacency

In the aftermath of 9-11, many authors and government officials have suggested the possibility of Americans becoming complacent regarding security and terrorism issues. The primary focus seems to be that as Americans become more comfortable, they

will become more impatient with security "inconveniences" such as waiting in the TSA line at airports, or waiting in line at the museum to have their bag checked. DHS Secretary Chertoff recognized this problem and notes, "in the short run I worry about a developing complacency and cynicism about the threat we are facing…People [are] starting to be unwilling to make the necessary sacrifices in order to make sure we can continue to disrupt and repel attacks on the US (Cook, 2007)." Chertoff further notes that the, "Great weapon they (terrorists) have is persistence and patience, and the one weakness we have is the tendency to lose patience and become complacent (Green, 2008)." Michael J. Heimbach, the assistant director for the FBI's Counterterrorism Division commented on his increasing concerns and notes, "As we approach almost seven years after Sept. 11, I'm really concerned about the complacency setting in amongst the American people (Green, 2008)."

Similar sentiments were voiced immediately following 9-11 as well. In an October 2001, article in *Security Management*, Sherry Harowitz notes; "Sadly, the widespread expressions of resolve to deal with terrorism are not new. Similar determination was voiced after the 1993 bombing on the World Trade Center and after the 1995 attack in Oklahoma City. Both were deemed 'wake up calls.' Yet somehow—each time—the nation returned to a sense of complacency, making it difficult for public and private security professionals to gain support for needed protection measures." Harowitz further employs the findings of Paul Pillar, a CIA officer and former deputy chief of the DCI counterterrorism center who notes, "The pattern that interest and concern amongst the American public and the U.S. Congress about counterterrorism

waxes and wanes according to how long it's been since the last major terrorism incident (Harowitz, 2001)."

Former Ambassador L. Paul Bremer dismisses the previous inclinations of the Congress and the American public because 9-11 marked, "a different order of magnitude…This is not only the worst terrorist attack in American history, it is the worst terrorist attack in history, period (cited in Harowitz, 2001)." Bremer's premise however, seems to be eclipsed by others' (notably Chertoff and Heimbach) notions that the American people will not remain vigilant in accepting the efforts to thwart terrorism. According to former CIA Agent Burton Gerber, "Often American people will not get energized until tragedy hits them…We're sitting here and we're completely happy and a crisis is going to happen tomorrow (Plumb, 2006)."

As this dissertation explored the issues of post crisis change and punctuated equilibrium, the subject of complacency was raised during questioning of SI OPS Executives, as well as with the NGA Executive. First, the interviewees generally stated that security personnel tend to be less complacent about post 9-11 terrorism issues because they view themselves as being on the "front lines." Secondly, the inferences from SI OPS personnel tended to focus on non-security personnel (vs. security personnel) being more willing to relax security monitoring due to lower threat levels. "The primary objective is open access", noted one SI OPS security official "and sometimes the curators and museum managers think security lines will make visitors not want to visit the museums (IWA, 2008)." This seems to be the current posture, while initially (immediately following 9-11) security was much stricter, and then it eventually skewed back towards open access.

As indicated by the above comments there may be some complacency that builds in organizations or within the general public in the aftermath of a major event or crisis. This complacency can be the result of a number of factors such as (but not limited to) a considerable amount of time passing between events or the event or crisis being of such a unique nature that the possibility of a second similar event/crisis occurring would be unimaginable. Although the general public may find repeated crises as unimaginable or unique, and as noted at the beginning of this section, interviews with SI OPS and NGA security personnel have identified a difference between security and non-security personnel regarding post event/crisis complacency. These differences show that, perhaps there is more to the complacency perception of the non-security SI personnel than meets the eye.

Instead of reaching complacency, perhaps what OPS security personnel are witnessing is the onset of a new period of equilibrium. Looking at PET in relation to SI OPS it is evident that 9-11 spurred an onset of dynamic change within the four factors studied in this dissertation. What they are now experiencing appears to be the onset of deep structures reestablishing or as previously noted, the onset of a new equilibrium period within OPS. As SI OPS continues to address SI's security concerns, it may be that they are losing the resource battle and are therefore being pushed into equilibrium causing management to incrementally address those resource and security concerns until crisis occurs.

Wollin (1999) looks at this period as "sorting" which can be seen as the outcome after the coming together of cooperative and competitive processes, as they interact to find their niche saturates within a new equilibrium. In other words, punctuation takes

place; the organization regroups, reconfigures its deep structures, and then sorts its priorities. In this instance SI OPS is just one of many competing entities for additional post 9-11 SI funding.

Other Relevant Findings – Underlying Issues/Practical Applications

The findings in this research have direct application to other similarly situated organizations. The first finding is that organizations need to develop emergency plans with local law enforcement agencies. Organizations should have a well laid out plan outlining the roles and responsibilities of all parties involved in responding to an event or crisis. The response plan should describe in detail all the objectives, strategies, elements, and procedures associated with the organization. The plan should document how the site protects against these unacceptable risks by addressing some of the following questions: What are the risks in a manmade or natural disaster scenario? What response plans are in place to address these risks?

Secondly, there is no "one size fits all" model for security. There is recognition that some sites are better trained and have more resources available than other sites. As such, security managers should make a reasonable assessment of the site's security strengths and weaknesses and develop a plan to address the weaknesses as fiscally and politically prudent as possible. As resources affect the quality of equipment and training, it also affects the quality of the applicant pool for security officers. This lack of financial resources may result in an organization hiring less qualified personnel. In such instances, it is suggested that security managers continually stress the importance of the role of the security officers as deterrents, as well as in the protection of life, limb, and property.

Finally, as security managers seek new ways to strengthen their respective security forces they should ensure they are not strengthening one area at the expense of another. For example, as SI implemented new enhancements to their screening technology and procedures the shift towards a more proactive terrorism stance coupled with the shortage of officer manpower led to a slight increase in petty crimes within some of the museums.

The objective should be a holistic approach to security that takes into account all reasonable threats to the facility in question. As previously noted, there is an understanding that some sites have more resources on hand than others; therefore they will be able to address security issues more substantially than others. For instance, if manpower shortages are an issue perhaps the installation of strategically placed security cameras and a vigilant monitoring presence in the Central Alarm Station (CAS) will suffice. This may free security officers to monitor troubled areas and then respond to calls from the CAS when needed.

Summary and Conclusions

This case study of SI OPS and how it responded to the events of 9-11 provides a valuable opportunity to examine the use of punctuated equilibrium theory as a tool for understanding organizational change. Theory argues that extraordinary events are the main drivers of radical organizational change and are not that uncommon. Yet, it can be difficult when studying organizational change to disentangle the effects of the many internal and external influences on organizations to identify which factors are significantly important to be regarded as drivers of radical change, or to define appropriate time periods for analysis. The tragic events of 9-11, however, had a very

clearly identifiable impact on SI OPS along with many other high-profile American institutions, with a starting point clearly defined. This provides a fairly unique opportunity to apply the punctuated equilibrium model to what would appear to be a very distinct example of the pattern of organizational change which it claims to explain.

Using PET as a framework to explore the security changes across the four factors in SI OPS following 9-11, may help provide an explanatory model for organizational change more generally. Even more importantly, however, the model can help provide SI OPS and organizations experiencing similar types of change to predict, understand and impose more effective control over change processes, in order to maximize their benefits for the organization. For example, the model predicts a certain degree of disorganization and disorder as an organization adapts its deep structures to a changed external environment. By anticipating this, an organization can take steps to minimize any adverse effects and implement measures which help hasten adaptation of its structures to the new environment.

In the case of SI OPS, the research findings indeed provide considerable evidence that the change processes which occurred after 9-11 can be explained to a very large extent by punctuated equilibrium theory. The study focused on four main factors, or deep structures of the organization: screening, policy, budgets and training, and found evidence of radical changes in each of these areas which were clearly the direct or indirect impacts of the extraordinary events of 9-11. In the area of screening, random and infrequent bag checks were replaced by a sophisticated range of high-tech screening measures, as well as extensive visitor searches. A whole new security policy regime was implemented which was based on pro-activity rather than compliance checks. Budgets

were increased considerably to support the new measures, and the amount and nature of training for officers also changed significantly in the post 9-11 period.

As predicted by the model, these changes involved a certain amount of disruption and disorder for a period of time. Most notably, officer turnover increased significantly and problems of recruitment and retention were experienced, placing more pressure on remaining officers who were already having to contend with considerably increased demands on their time. Moreover, the budgetary increases, although significant, appeared to be inadequate for the immense task of implementing the new security policies, as well as covering the additional recruitment and retention costs.

Despite this, it can be seen that SI OPS is now in many respects at the final stage of the change process as defined by the model, in that new structures and ways of doing things have generally been bedded down in the organization, and previous deep structures have been reconfigured as a result. Most importantly, it is apparent from the research findings that a significant culture change has taken place which has infiltrated all areas. There is a strong emphasis on terrorism-awareness and in being proactive on the part of all managers and security officers on identifying and addressing possible terrorist threats. This is generated in part by the new forms of training they receive, but is also driven by the changed culture of the organization more generally. A new equilibrium is in the process of being developed in which various structures of the organization reinforce and support one another and are adapted to the current external environment, which for the time being continues to be dominated by the threat of terrorism. Other threats and risks to the Smithsonian museums, such as vandalism and theft, are no less significant than before, but disproportionate information processing is currently diverting attention away

from these in favor of terrorism-prevention. It remains to be seen whether future extraordinary events will bring about further changes in SI OPS, and whether the ongoing pattern of change will continue to fit the punctuated equilibrium model.

Chapter 7

Conclusions, Implications, and Future Research

The complex of SI museums is a low risk target for a terrorist attack, but is located in a high threat area. Balancing the risk of a direct attack or the consequences of an attack nearby, with the priority for free and open access to the institution for large numbers of people is a challenge for museums, court houses, monuments, government buildings and tourist attractions across the country.

The Approach Taken in This Study

This research was conducted as a qualitative exploratory case study that drew upon interviews with various members of the Smithsonian Institution, data made available by SI OPS for review, and documentation from secondary sources. This research consisted of examining the experiences and perceptions of security and non-security personnel in the pre and post 9-11 security environment, as well as an examination of SI OPS documentation to compare actual changes and outcomes in training, policy, budget, and screening. Secondary sources were used to supplement these observations and to reach beyond the experience of the SI OPS in its context as a low risk target in a high threat area. The research questions of this study focused on the effects of 9-11 on SI OPS by examining four key organizational factors—screening, policy, budget and training. Interview questions focused on the ways that employees perceived and experienced changes in these key variables as implemented across SI. Three sets of interview questions designed by me were utilized to gather information on the variables from security managers, security non-managers, and non-security managers.

Where do we go from here?

The findings outlined in chapters 5 and 6 provide insight into organizational efforts to address security in a post 9-11 world. Identifying and implementing the right balance between security and open access in an institution such as SI can provide insight for other similarly situated organizations at a low risk for a direct attack, but residing in a high threat area. Several key topics have been identified throughout this study and a few warrant further discussions regarding their future direction. These broader topics came to light during the interviews and from general observations before, during, and after the interviews. Suggestions are provided to security managers, especially in organizations with similar properties, conditions and situations, as those identified in this study, to strengthening their basic security operations.

Strengthen Communication

Communication and cooperation between different law enforcement agencies and jurisdictions are vital to a robust security plan. 9-11 played an important role in increasing communications between the different levels of law enforcement—federal, state, and local—as well as between different jurisdictions. One concept that could be considered is for low threat targets in high threat areas to appoint a liaison to have frequent interaction with the local Joint Terrorism Task Force (JTTF)[3]. This communication could also be useful in forecasting trends in terrorism and will allow key information to flow into the hands of the people who can use it to prevent future acts of terrorism.

[3] JTTF is a multijurisdictional task force consisting of representatives from a number of federal, state, and local law enforcement agencies, brought together to pool resources and expertise in order to better fight terrorism.

Communication is vital within individual organizations as well. Some interviews with non-security personnel at SI revealed a lack of upper management communication between SI OPS and non OPS personnel (IWA, 2008). SI OPS communications prior to 9-11, while somewhat open and frequent within the security department, appeared to be more constricted and closed in relaying information to the non-security related personnel. Although it may not have been purposely conducted in this manner, there appears to be a lower propensity to share information on the part of people at all levels outside of SI OPS. One non-manager security officer remarked that security directors and managers were sharing information with officers during the morning officer briefings, while one non-security manager noted that overall; there was not as great a flow of information throughout the SI regarding security, at least from the security office prior to 9-11.

According to security and non-security managers and non-managers, the openness and frequency of communications and information increased significantly after 9-11 (IWA, 2008). Rather than filtering meeting notes and other information through layers of managers, most information is now sent via e-mail to all SI employees, including correspondence from the Director of OPS. Regarding this new communication effort, one non-security manager interview respondent commented that, "SI Directors, at all levels, shared information before 9-11 and continue to do so. I'm not sure OPS was doing that before. We usually heard of things by happen stance through a facility security manager (IWA, 2008)." He further stated that prior to 9-11, "non-security personnel did not really know where the SI OPS leadership wanted to go, what they were doing or what they thought about anything…Things have changed a lot since 9-11. I would like to have more contact with the OPS Director however. I don't think I've ever met him (IWA, 2008)."

This same non-security manager was questioned about the process of communication being a two-way street. If he had never met the Director of OPS, has he (the non-security manager) ever made efforts to facilitate a meeting or open up communication channels? His answer was "no" but he furthered, "although more work needs to be done, the communication chain is getting much better (IWA, 2008)." Perhaps OPS management can implement a "security management by walking around" policy (Behn) in which they designate particular days of the month to visit each museum and engage in conversations with non-security management. They can use this interaction as a way to exchange vital security information, changes, or concerns with those non-security personnel.

Despite some of the communication shortcomings nearly all interviewees said that there was a greater emphasis on better and more communication post 9-11. Regarding this greater effort, one interviewee noted, "We all have different ideas of what is important at the museum…some may say the art or antique furniture is the most important because it is irreplaceable, but in the end the real importance lies in saving lives of visitors and employees. We need to make that the plan and not worry so much about the other things (IWA, 2008)."

Continue a Vigorous Screening Process

Throughout this research process the item that stood out the most was the idea that the NGA "got it right" regarding its screening process; "screen everyone, all the time, and leave nothing to chance (IWA, 2009)". Although those exact words were not uttered that appeared to be the underlying mantra. SI OPS on the other hand appears to be facing more internal issues regarding the types and duration of screening. Despite the visitor survey (outlined in chapter 5) that clearly noted visitor understanding and

willingness to stand in lines for security screening, there still appears to be an internal issue with the "screen everyone, all the time…" mindset. That was the process in the immediate aftermath of 9-11. However, interviews with security personnel have intimated that that has been replaced with two to three well placed screening intervals during the day in which visitors are screened (IWA, 2007).

Although SI OPS faces stiff budgetary challenges in the coming years that will affect manpower and equipment purchases perhaps this is the time for them to implement a more stringent screening policy that will become a 'deep structure' in the impending years. This new process could follow that of the NGA. SI OPS could conduct manual bag searches at all facilities and adjust its use of the magnetometers and x-ray machines based on the DHS Color Code System[4]. This will allow OPS managers more flexibility in determining manpower needs at the various facilities, and it allows them some flexibility to conduct "random" full scale screenings at various times during the day to prevent screening predictability.

Manpower Shortages

As previously noted OPS has been suffering through severe security officer shortages and high turnover for several years. One of the causes of this is believed to be of the low salary for officers. Another is due to a less qualified applicant pool, which may also be a result of the low salary. Perhaps in an effort to increase the quality of officers OPS could look to hire officers on a part time basis (thus alleviating the need to pay benefits, etc) but pay them higher wages. One pool of applicants may be retired military personnel and police officers who currently have medical and retirement benefits and who have a desire to work part time "to make ends meet" or "stay active." These recruits

[4] The higher the color code = more intense security screening and vice versa.

can be found by contacting local police departments and military transition offices and putting out information that OPS is looking to fill a number of part time security officer positions at a very competitive hourly rate. Although this may not solve all of the immediate security needs it may help alleviate some of them.

Future Study

The literature for this dissertation explored theories of PET, and security management. As the literature provides practical insights into security policies at the Federal Aviation Administration (FAA) and DHS following 9-11 it fails to address security issues at locations not considered low risk, high threat areas that also provide open access. As previously noted in the literature review, there is a tendency for terrorist groups to focus on less traditional, lower risk targets such as malls, night clubs and hotels. Conducting empirical studies into how these types of organizations react to the changing threat environment will expand our knowledge and provide valuable insight into how smaller, less traditional targets can adapt to and address those changes.

Further research could build on these findings by replicating this study as closely as possible in other federal agencies, museums, or universities. The primary value in replicating the study is to test the contingency theory, i.e., measure whether the findings hold regardless of environment or situation. In leveraging (not replicating) this study, researchers could attempt to identify and characterize behaviors of other similar security departments.

The importance and effect of formal structures is another area ripe for future research. Empirical studies to date have not analyzed the effect of formal Security Councils or security related decision-making teams. While this research found that the SI

Security Initiative Committee (SI/SIC) was very instrumental in determining the most advantageous routes for improving overall security at SI facilities, further research could be helpful to determine the effectiveness of similar groups in other organizations. SI OPS executives indicated the SI/SIC to be effective in its mission. This may lead researchers to believe that formal structures are needed prior to, rather than following, a crisis to help move organizations toward important enhanced security implementation steps, such as managerial commitment and securing budgetary needs.

Future research should examine more closely the effect of formal and informal teams, groups, and processes on the enhanced security measures decision making process. In particular, practitioners need to know much more about whether formal structures (such as the SI Security Initiative Committee) should be continued or dissolved, and if so, what the optimal times and methods are for creating them and/or phasing them out. There is a great need among practitioners for empirical data on the importance and nature of formal decision making structures.

Other types of research could be conducted to attempt to show causality. For example, causality could be measured using an experimental and control group design (with and without security enhancements) along with a longitudinal research design (multiple observations over time before and after the crisis). A longitudinal study could also be used to examine the effects of a crisis on long term outcomes, such as product/service quality and external/internal stakeholder satisfaction. While a single study site could be utilized to measure results before and after a crisis, such a study would require an immense amount of documentation of precisely what was done (policy processes) to implement the security enhancements, as well as what other events occurred

in the intervening time period. Intervening changes and events would need to be controlled for.

Ideally, any further research that is conducted in the field should include both quantitative measures and qualitative documentation and measurement of the nature of implementation efforts. For the reasons discussed above, additional case studies or quantitative analyses alone are unlikely to contribute empirical knowledge about the effects of security enhancements following a crisis.

APPENDICES

APPENDIX I

Post 9-11 Public Laws

2001

- Public Law 107-56 – The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (US Patriot Act) .

- Public Law 107-63 – The Department of Interior and Related Agencies Appropriations Act, 2002

- Public Law 107-66 – The Energy and Water Development Appropriations Act

2002

- Public Law 107-71 – The Aviation and Transportation Security Act

- Public Law 107-107 – The National Defense Authorization Act for FY 2002

- Public Law 107-115 – The Foreign Operations, Export Financing, and Related Programs Appropriations Act, 2002

- Public Law 107-116 – The Department of Labor, Health and Human Services, and Education, and Related Agencies Appropriations Act, 2002

- Public Law 107-117 – The Department of Defense and Emergency Supplemental Appropriations for Recovery from and Response to the Terrorist Attacks on the United States Act, 2002

- Public Law 107-173 – Enhanced Border Security and Visa Entry Reform Act of 2002

- Public Law 107-188 – Public Health Security and Bioterrorism Preparedness and Response Act of 2002

- Public Law 107-197 – The Terrorist Bombings Convention Implementation Act of 2002

- Public Law 107-206, The 2002 Supplemental Appropriations Act for Further Recovery from and Response to Terrorist Attacks on the United States

- Public Law 107-228, The Foreign Relations Authorization Act, FY 2003

- Public Law 107-248, The Department of Defense Appropriations Act, 2003

- Public Law 107-273, The 21st Century Department of Justice Appropriations Authorization Act

- Public Law 107-287, The Department of Veterans Affairs Emergency Preparedness Act of 2002

- Public Law 107-295, The Maritime Transportation Security Act of 2002

- Public Law 107-296, The Homeland Security Act of 2002

- Public Law 107-306, The Intelligence Authorization Act for Fiscal Year 2003

- Public Law 107-314, The Bob Stump National Defense Authorization Act for FY 2003

2003

- Public Law 108-7, The Consolidated Appropriations Resolution, 2003

- Public Law 108-11, The Emergency Wartime Supplemental Appropriations Act, 2003

- Public Law 108-87, The Department of Defense Appropriations Act, 2004

- Public Law 108-90, The Department of Homeland Security Appropriations Act, 2004

- Public Law 108-108, The Department of the Interior and Related Agencies Appropriations Act, 2004

- Public Law 108-136, The National Defense Authorization Act for FY 2004

- Public Law 108-137, The Energy and Water Development Appropriations Act, 2004

- Public Law 108-175, The Syria Accountability and Lebanese Sovereignty Restoration Act of 2003

- Public Law 108-183, The Veterans Benefits Act of 2003

- Public Law 108-188, The Compact of Free Association Amendments Act of 2003

2004

- Public Law 108-276, the Project BioShield Act of 2004
- Public Law 108-287, the Department of Defense Appropriations Act, 2005
- Public Law 108-334, the Department of Homeland Security Appropriations Act, 2005
- Public Law 108-375, the Ronald W. Reagan National Defense Authorization Act for FY 2005
- Public Law 108-447, the Consolidated Appropriations Act, 2005
- Public Law 108-458, the Intelligence Reform and Terrorism Prevention Act of 2004
- Public Law 108-487, the Intelligence Authorization Act for Fiscal Year 2005

Appendix II
Post 9-11 Officer Training

New Officers Basic Entry Level Training

Week #1

Day 1

- Personnel Processing
- ID Credentials (Photo & Fingerprinting)
- Personnel Verification Process

Day 2

- Roll Call and Administrative Announcements
- OPS Welcome
- BELT Course Introduction
- OPS Organization
- Museum Protection Officer-Position Description
- Security Officer / Special Police Officer
- SI-Accessibility Program & (Tape Preview)
- Customer Service

Day 3

- Roll Call and Administrative Announcements
- Blood Borne Pathogens
- Pay Category
- Overview of Museum Personnel and Functions

Day 4

- Roll Call and Administrative Announcements
- Drug Testing Program
- Welcome to Office of Protection Service
- Federal Appointment / Performance
  Employee Assistance Program

Week # 2

Day 5

- Roll Call and Administrative Announcements
- OPS Sensitivity Background Review
- Ombudsman
- Radiation Awareness Training
- Duty Hours

Day 6

- Roll Call and Administrative Announcements
- Leave Administrative
- Overtime/Special Events-How It Works
- Prevention of Workplace Harassment

Day 7

- Roll Call and Administrative Announcements
- CPR/AED

Day 8

- Roll Call and Administrative Announcements
- Policy Awareness and Applications
- Handling Medical Emergencies
- Ethics
- Dignitary/ VIP Visits
- Scheduling and How It Works

Day 9

- Roll Call and Administrative Announcements
- Conflict Resolutions
- Interpersonal Communications
- Controlling Your Attitude
- Lost and Found / Lost and Missing Children
- Violence in the Workplace

Week # 3

Day 10

- Class Formation and Administration Briefs
- Conducting Formations
- Work Ethics/Ready, Willing, Able
- Interviewing Techniques
- Blotters
- Case Records

Day 11

- Formations and Administrative Announcements
- OPS Organization Chart
- Chain of Command
- Dealing with Other Agencies
- Rules and Regulations for SI Buildings
- Enforcement Duty , Authority, Jurisdiction

Day 12

- Formations and Administrative Announcements
- Disaster Preparedness
- Giving and Receiving Orders
- Magnetometer and Wand Training

Day 13

- Formations and Administrative Announcements
- Arrest Procedures
- Homeland Security Threat Levels
- Bomb Threat
- Shelter in Place Procedures
- Emergency Evacuation
- Impact of Breaches in Security

Day 14

- Formations and Administrative Announcements
- Fundamentals Of Physical Security
- Post Orders and Boundaries
- Post Abandonment
- Post Inspections and Patrol Techniques
- Crowd Control
- Museum Closing Procedures

Week # 4

Day 15

- Formation and Administration Announcements
- Uniform Issuance
- Professional Image Projection
- Uniform Appearance Guideline
- Equipment and Uniform Responsibilities

Day 16

- Formations and Administrative Announcements
- Safety Awareness
- First Responder Awareness
- Visitor Reception Center
- Use of Force

Day 17

- Formations and Administrative Announcements
- Basic Principles of Handcuffing

Day 18

- Formations and Administrative Announcements
- Use of Force Report Writing
- Missing and Stolen Artifacts
- Protecting the Crime Scene
- OPS Training Overview
- Contractor Escort
- Motivation and Success

Day 19

Students Scheduled Day OFF Preparation for Saturday Museum Orientation Duty

Day 20

- Formations and Administrative Announcements
- OPS Awards and Recognition Program
- Pickpocket Awareness Training
- BELT Transition to week Five

Day 21

- Reporting to Units NASM/NMNH
- Formation Observation
- Post Inspection/Patrol/Abandonment of Post
- Exhibit Damage
- Alarms
- Tours of Central Control/Fire Suppression System
- Unit Control Room Tour
- Random Screening Observation/Museum Closing Procedures

Appendix III
Factors and Changes

	Screening	Budget	Policy	Training	Implications for Practice
Pre 9-11	No terrorism focus	Focus was on addressing pre-existing security needs (uniforms, equipment maintenance)	Focused on common security threats to cultural institutions (theft of artifacts, vandalism, theft of personal property)	See Appendix II and IV for Training outline	
	Lack of technology	3%-10% gradual yearly increases in budget	Little interaction between security and non security personnel regarding security policy		
	Lack of communication between security and non security personnel	Hiring of new security officers was limited due to budgetary constraints			
	Sporadic searches of visitors and bags				
Post 9-11	Immediate shift to terrorism focus	Immediate increase in Anti-Terrorism funds (hiring new officers, purchase of new equipment, expand officer training) $37 million in 2001 to $67 million in 2006	Introduction of risk assessments as means to determine weaknesses	See Appendix II and IV for Training outline	Develop an emergency response plan with local law enforcement and engage in conversations regarding the nature of the threats Begin "Management-by-Walking Around" – to help build communication with non-security personnel. Use this time to talk about security concerns regarding threats and mitigation efforts
	Implementation of new screening technology (x-ray machines, magnetometers, hand wands)	Despite rapid increase, OPS still has a shortfall due to increased post 9-11 security concerns	Formation of the SI Security Initiative Committee to recommend security policy changes		
	All visitor bags searched by officers or through new technological devices	Budget changes have not increased enough to address high Officer turnover	Increased understanding and awareness of the "threat"		Determine how to address manmade and natural threats equally Awareness of vulnerability shift – as you increase security in one area make certain it doesn't cause security gaps in another area
	Random searches of visitors implemented		Implementation of college students attendant program (to help offset officer retention issues)		Changes must be sustainable – what processes and practices can be implemented without hampering other areas?
					Communication in structural and practical elements that are tailored to the individual institution – one size doesn't fit all
					Diagnosis of labor pool to determine methods to alleviate high turnover

Appendix IV
Training

	Prior to 9-11	2003	2006	Present
Firearm (.38 Cal. Revolver) **ASP Baton** **O.C. (oleoresin capsicum) Spray** **Handcuffing (all of the above addressed in this block)**	Officers were carrying a total of 12 rounds (6 in weapon / 1- 6 round speed-loader) Basic weapons training was 32 hours and included O.C. Spray Course of fire (firearms proficiency test) was very basic and not comparable to other Federal Agencies and held at Ft. Meade Minimum proficiency required to meet agency standard for firearms ASP Baton wasn't in consideration O.C. certification consisted of exposure only (not realistic) and no weapons retention after exposure Handcuff familiarization only	Officers increased to a total of 18 rounds (6 in weapon / 2-6 round speed-loaders) Basic weapons training was increased to 40 hours and included O.C. Spray and weapon retention drill after exposure and during hostile actions Course of fire was changed to increase proficiency and held at Ft. Meade Moderate proficiency required to meet agency standard Handcuff familiarization only	ASP Baton added to the Use of Force Module as an intermediate weapon and taught on the FLETC standard O.C. spray and handcuffing also taught on the FLETC standard	Basic weapons training increased to 56 hours and includes ASP Baton Certification Use of Force Module changed (April 2007) to be compatible with responding Federal Agency (U.S. Park Police) Course of fire on the same standard as most Federal agencies and conducted at FLETC Firearms proficiency on the same level as other Federal Law Enforcement agencies

Bibliography

ASIS INTERNATIONAL GUIDELINES COMMISSION. (2003). General Security Risk Assessment Guideline. URL: http://www.asisonline.org/guidelines/guidelinesgsra.pdf.

Atlas, R. "Designing For Homeland Security." Retrieved September 26,, 2004, from www.cpted-security.com/cpted20.htm.

Atran, S. (2003). "Genesis of Suicide Terrorism." Science **299** (5612): 1534 - 1539.

Benbasat, I., D. K. Goldstein, et al. (1987). "The Case Research Strategy in Studies of Information Systems." MIS Quarterly **11**(3): 369-386.

Berman, E. M. (1997). "Dealing with cynical citizens." Public Administration Review **57**(2): 105(8).

Birkland, Thomas A. “Learning and Policy Improvement After Disaster: The Case of Aviation Security.” American Behavioral Scientist 48, no. 3 (2004): 341-364.

Birkland, Thomas A. 2005. An Introduction to the Policy Process: Theories, Concepts, and Models of Public Policy Making, 2nd ed. (Armonk, NY: M.E. Sharpe).
(First edition, 2001).

Bryman, A. (2001). Social Research Methods. Oxford, Oxford University Press.

Burke, W. W. (2002). Organization change: theory and practice, Sage.

Bush, G.W. (2002). The Department of Homeland Security. Washington, DC: The White House.

Bush, G.W. (2002). The National Security Strategy of the United States of America. Washington, DC: The White House.

Bush, G.W. (2002). National Strategy for Homeland Security. Washington, DC: Office of Homeland Security.

Childress, M. T. (2002). "9-11: The Uncertain Implications for State and Local Governments." Foresight **9**(3).

Cigler, B. A. (1988). Current Policy Issues in Mitigation. Managing Disaster: Strategies and Policy Perspectives. L. K. Comfort. Durham, Duke University Press**:** 39-52.

Comfort, L. K. (1988). Designing Policy for Action: The Emergency Management System. Managing Disaster: Strategies and Policy Perspectives. L. K. Comfort. Durham, Duke University Press**:** 3-21.

Comfort, L. K. (1997). "Models of change: a dialogue between theory and practice. (Initiating Change: Theory and Practice)." American Behavioral Scientist **40**(3): 259-264.

Comfort, L. K. (2002). "Institutional re-organization and change: security as a learning strategy." The Forum **1**(2).

Comfort, L. K. (2002). "Rethinking Security: Organizational Fragility in Extreme Events." Public Administration Review **62**(Special Issue): 98-107.

Cook, D. (2007). Homeland Security chief: US growing complacent on terrorism. The Christian Science Monitor. URL: http://www.csmonitor.com/2007/0621/p25s08-usmb.html, accessed June 21, 2007.

Corbin, M. (2003). Funding for Defense, Homeland Security and Combating Terrorism Since 9-11. Security After 9-11 Strategy Choices and Budget Tradeoffs. M. Corbin. Washington, DC, Center for Defense Information.

Dalton, D.A. (2003). Rethinking Corporate Security in the Post 9-11 Era. Butterworth-Heinemann.

Delattre, E.J. (2002). Character and Cops: Ethics in Policing (4th ed.). AEI Press.

Department of Homeland Security – Office for Domestic Preparedness. (2003). Vulnerability Assessment Methodologies Report. Washington, DC.

Department of Homeland Security. (2004). Securing Our Homeland--The DHS Strategic Plan. Washington, DC.URL: http://www.iwar.org.uk/homesec/resources/dhs/strategic-plan.htm.

Department of Homeland Security. (2004). Final Draft: National Response Plan. Washington DC. URL: http://www.dhs.gov/interweb/assetlibrary/NIMS-90-web.pdf

Doyle, C. (2002). The USA PATRIOT Act: A Legal Analysis. CRS Report for Congress. Dated April 15, 2002.

Durant, R. F. (2002). "Whither Environmental Security in the Post-September 11th Era? Assessing the Legal, Organizational, and Policy Challenges for the National Security State." Public Administration Review **62**(Special Issue): 115-123.

Eldridge, N. and S. Gould (1972). Punctuated equilibria: An alternative to phyletic gradualism. Models in Paleobiology. T. J. Schopf. San Francisco, Freeman, Cooper & Co.**:** 82-115.

Emerson, S. D. and Nadeau, J. (2003). A Coastal Perspective on Security. Journal of Hazardous Materials, 104, 1-13.

Falkenrath, R. A. (2001). "Problems of Preparedness (readiness for domestic terrorism in the U.S.)." International Security **25**(4).

Faye, J. J. (2002). Contemporary Security Management. Boston, Butterworth-Heinemann.

Fayol, H., 1949. General and Industrial Management. Trans. Constance Storrs, London: Pittman Publishing.

Federal Emergency Management Agency. (2005) Risk Management Series: Risk Assessment. A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings. FEMA 452.

Flynn, S. E. (2002). "America The Vulnerable." Foreign Affairs **81**(1): 60.

Fontana, A., and J. Frey., "Interviewing: The Art of Science," in Handbook of Qualitative Research, Denzin and Lincoln (eds). Sage Publications. Thousand Oaks, 1994: 361-376.

Ford, J. K., J. G. Boles, et al. (1999). "Transformational Leadership and Community Policing: A Road Map for Change." Police Chief Magazine: 14-22.

Gall, M. D., Borg, W. R., & Gall, J. P. (1996). Educational research: An introduction. White Plains, NY: Longman.

General Accounting Office (2003). AIRPORT PASSENGER SCREENING: Preliminary Observations on Progress Made and Challenges Remaining, Washington, D. C.: U.S. Government Printing Office.

General Accounting Office (2007). SMITHSONIAN INSTITUTION Funding Challenges Affect Facilities' Conditions and Security, Endangering Collections, Washington, D. C.: U.S. Government Printing Office.

General Accounting Office (2005). NATIONAL MALL: Steps Identified by Stakeholders Facilitate Design and Approval of Security Enhancements, Washington, D. C.: U.S. Government Printing Office.

Gersick, C. (1991). "Revolutionary change theories: A multilevel exploration of the punctuated equilibrium paradigm." Academy of Management Review **16**(1): 10-36.

Gersick, C. (1994). "Pacing strategic change: the case of a new venture." Academy of Management Journal **37**(1): 9-45.

Gersick, C. J. G. (1988). "Time and transition in work teams: Toward a new model of group development." Academy of Management Journal **31**: 9-41.

Green, J.J. (2008). 'Complacency' worries top FBI counterterrorism official. URL: http://www.wtopnews.com/?nid=778&sid=1439724, accessed on July 16, 2008.

Haque, M. S. (2002). "Government Responses to Terrorism: Critical Views of Their Impacts on People and Public Administration." Public Administration Review **62**(Special Issue): 170-180.

Harowitz, S. (2001). "A Different Order of Magnitude." Security Management **45**(10): 8.

Harowitz, S. (2004). "What is homeland security?" Security Management **48**(6): 8.

Haynes, R. A. (1998). "Should companies adopt community policing practices?" Security Management **42**(5): 118-120.

Heyman, P. (2001/2002). "Dealing with Terrorism." International Security **26**(3).

Hillyard, M. J. (2002). "Organizing for Homeland Security." Parameters **32**(1): 75-86.

Hwang, P. J. and J. D. Lichtenthal (2000). "Anatomy of Organizational Crises." Journal of Crises and Contingency Management **8**(3): 129-140.

Jones, B. D. and F. R. Baumgartner (2004). "A model choice for public policy." Journal of Public Administration Research and Theory **15**(3): 325-351.

Kaplan, B. and D. Duchon (1988). "Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study." MIS Quarterly **12**(4): 571-587.

Kaplan, B. and J. A. Maxwell (1994). Qualitative Research Methods for Evaluating Computer Information Systems. Evaluating Health Care Information Systems: Methods and Applications. J. G. Anderson, C. E. Aydin and S. J. Jay. Thousand Oaks, CA, Sage**:** 45-68.

Kettl, D. F. (2003). "Contingent Coordination: Practical and Theoretical Puzzles for Homeland Security." American Review of Public Administration **33**(3): 253-277.

Kettl, D. F. (2004). Systems Under Stress: Homeland Security and American Politics. Washington, DC, CQ Press.

King, C. S., K. M. Feltey, et al. (1998). "The question of participation: toward authentic public participation in public administration." Public Administration Review **58**(4): 317(10).

Kirlin, J. J. and M. K. Kirlin (2002). "Strengthening Effective Government-Citizen Connections through Greater Civic Engagement." Public Administration Review **62** (Special Issue): 80-85.

Kosiak, S. M. (2003). Funding for Defense, Homeland Security and Combating Terrorism Since 9-11. Security After 9-11 Strategy Choices and Budget Tradeoffs. M. Corbin. Washington, DC, Center for Defense Information**:** 9.

Kurtus, R. (2002). What is Security? URL: http://www.school-for-champions.com/security/whatis.htm.

Lecompte, M.D. and J. Preissle. (1993). Ethnography and Qualitative Design in Educational Research, Second Edition. Academic Press.

Lichtenstein, B. (1995). "Evolution or transformation: a critique and alternative to punctuated equilibrium." Academy of Management Journal (Business Module): 291-295.
Lin, Z. and K. M. Carley (2002). "Organizational design and adaptation in response to crises: theory and practice." Retrieved March 20, 2005.

Lyons, W. (2002). "Partnerships, information and public safety." Policing: An International Journal of Police Strategies & Management **25**(3): 530-542.

McCrie, R. D. (2001). Security Operations Management. Boston, Butterworth-Heinemann.

Merriam, S. B. (2001). Qualitative research and case study applications in education (2nd ed.). San Francisco: Jossey-Bass Publishers.
Newman, O. (1996). Creating Defensible Space. New Brunswick, U.S. Department of Housing and Urban Development Office of Policy Development and Research.

National Gallery of Art Security Executive Interview. Person to Person. January 13, 2009.

Newmann, W. W. (2002). "Reorganizing for National Security and Homeland Security." Public Administration Review **62**(Special Issue): 126-137.

9-11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States. (2004). New York: W.W. Norton.

Nunn, S. (2004). "Thinking the Inevitable: Suicide Attacks in America and the Design of Effective Public Safety Policies." Journal of Homeland Security and Emergency Management **1**(4).

O'Connor, T. (2005, 03/22/05). "The meaning and components of community policing." Retrieved 04/04, 2005, from http://faculty.ncwc.edu/toconnor/205/205lect13.htm.

Orr, J. E. (1998). "Images of Work." Science, Technology, & Human Values **23**(4): 439-455.

Pape, R. A. (2003). "Dying to Kill Us." New York Times.
Pateman, C. (1970). Participation and democratic theory. Cambridge [Eng.], University Press.

Price, Brian. (1990). "Frank and Lillian Gilbreth and the Motion Study Controversy, 1907-1930" in A Mental Revolution: Scientific Management since Taylor, Daniel Nelson, ed. The Ohio State University Press.

Report of Committee on Commerce, Science, and Transportation on S. 1214, 2001. URL: http://www.thomas.gov/cgi-bin/bdquery/z?d107:SN01214:@@@S.

Romanelli, E. and M. L. Tushman (1994). "Organizational transformation as punctuated equilibrium: An empirical test." Academy of Management Journal **37**(5): 1141-1167.

Rosenthal, U. (1988). Disaster Management in the Netherlands: Planning for Real Events. Managing Disaster: Strategies and Policy Perspectives. L. K. Comfort. Durham, Duke University Press**:** 274-295.

Rosenthal, U., M. T. Charles, et al. (1989). Coping with crises: the management of disasters, riots, and terrorism. Springfield, Ill., U.S.A., C.C. Thomas.

Rubin, C. (2004). "Major Terrorist Events in the U.S. And Their Outcomes: Initial Analysis and Observations "Journal *of Homeland Security and Emergency Management* **1**(1).

Ryan, G. W. & H. R. Bernard. (2003). Data management and analysis methods. In N. K. Denzin & Y. S. Lincoln (Eds.), *Collecting and interpreting qualitative materials* (2nd ed.). Thousand Oaks, CA: Sage.

Scheider, M. C. and R. Chapman (2003). "Community Policing and Terrorism." Retrieved September 26,, 2004, from www.homelandsecurity.org/journal/articles/Scheider-Chapman.html.

SI OPS Non Security Executive Interview 1. Person to Person. September 4, 2008.

SI OPS Non Security Executive Interview 2. Person to Person. September 4, 2008.

SI OPS Non Security Executive Interview 3. Person to Person. September 4, 2008.

SI OPS Security Executive Interview 1. Person to Person. August 31, 2007.

SI OPS Security Executive Interview 2. Person to Person. August 31, 2007.

SI OPS Security Executive Interview 3. Person to Person. August 31, 2007.

SI OPS Security Manager Interview 1. Person to Person. August 8, 2005.

SI OPS Security Manager Interview 2. Person to Person. August 8, 2005.

SI OPS Security Manager Interview 3. Person to Person. August 8, 2005.

SI OPS Security Manager Interview 4. Person to Person. August 9, 2005.

SI OPS Security Manager Interview 5. Person to Person. August 10, 2005.

SI OPS Security Manager Interview 6. Person to Person. August 11, 2005.

SI OPS Security Manager Interview 7. Person to Person. August 11, 2005.

SI OPS Security Officer Interview 1. Person to Person. August 8, 2005.

SI OPS Security Officer Interview 2. Person to Person. August 8, 2005.

SI OPS Security Officer Interview 3. Person to Person. August 8, 2005

SI OPS Security Officer Interview 4. Person to Person. August 8, 2005.

SI OPS Security Officer Interview 5. Person to Person. August 9, 2005.

SI OPS Security Officer Interview 6. Person to Person. August 9, 2005.

SI OPS Security Officer Interview 7. Person to Person. August 9, 2005.

SI OPS Security Officer Interview 8. Person to Person. August 9, 2005.

SI OPS Security Officer Interview 9. Person to Person. August 10, 2005

SI OPS Security Officer Interview 10. Person to Person. August 10, 2005.

SI OPS Security Officer Interview 11. Person to Person. August 10, 2005

SI OPS Security Officer Interview 12. Person to Person. August 10, 2005.

SI OPS Security Officer Interview 13. Person to Person. August 11, 2005.

SI OPS Security Officer Interview 14. Person to Person. August 11, 2005.

SI OPS Security Officer Interview 15. Person to Person. August 11, 2005.

SI OPS Security Officer Interview 16. Person to Person. August 11, 2005.

SI OPS Security Officer Interview 17. Person to Person. August 11, 2005.

Sprinzak, E. (1998). "The Great Superterrorism Scare." Foreign Policy.

Stake, R. E. (1995). The art of case study research. Thousand Oaks, CA: Sage.

Strauss, A. and J. Corbin (1998). Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. New York, Sage Publications Inc.
Taylor, F.W. (1911). The Principals of Scientific Management. New York: Harper.

Theoharis, A.G., T.G. Poveda, S. Rosenfeld and R.G. Powers. (2000). The FBI: a comprehensive reference guide. Greenwood Publishing Group.

Tushman, M. L., W. H. Newman, et al. (1986). "Convergence and Upheaval: Managing the Unsteady Pace of Organizational Evolution." California Management Review **29**(1): 29-44.

Tushman, M. L. and E. Romanelli (1985). Organizational evolution: A metamorphosis model of convergence and reorientation. Research in Organizational Behavior. L. L. C. A. B. M. Staw. Greenwich, CT, JAI Press. **7:** 171-222.

United States Senate. (2001). USA PATRIOT Act. H. R. 3162. URL: http://epic.org/privacy/terrorism/hr3162.html

Walsham, G. (1993). Interpreting Information Systems in Organizations. Chichester, Wiley.

Wamsley, G. and A. D. Schroeder (1996). "Escalating in a quagmire: the changing dynamics of the emergency management policy subsystem." Public Administration Review **56**(3): 235(9).

Wamsley, G., A. D. Schroeder, et al. (1996). "To politicize is not to control: the pathologies of control in federal emergency management." American Review of Public Administration **26**(3): 263(22).

Waugh Jr, W. L. (2000). Living With Hazards: Dealing With Disasters - An Introduction To Emergency Management. Armonk, M.E. Sharp, Inc.

Waugh Jr, W. L. and R. T. Sylves (2002). "Organizing the war on terrorism." Public Administration Review **62**(Special Issue): 145-153.

Wilson, J. and A. Oyola-Yemaiel (2001). "The evolution of emergency management and the advancement towards a profession in the United States and Florida." Safety Science **39**: 117(14).

Winegardner, Karen E. n.d. “The Case Study Method of Scholarly Research.” URL: http://www.tgsa.edu/online/cybrary/case1.html, accessed on 3 August 2002.

Wollin, A. (1999). "Punctuated Equilibrium: reconciling theory of revolutionary and incremental change." Systems Research and Behavioral Science **16**(4): 359-369.

Yin, R. K. (2002). Case Study Research, Design and Methods. Newbury Park, Sage Publications.