HORIZONTALITY AND CANADA'S OFFICE OF CRITICAL INFRASTRUCTURE PROTECTION AND EMERGENCY PREPAREDNESS: A CASE STUDY

BY

Marina Rountree

A Thesis submitted to
the Faculty of Graduate Studies
In Partial Fulfillment of the Requirements for the Degree of

MASTER OF ARTS

Department of Political Studies
University of Manitoba
Winnipeg, Manitoba

Abstract

This thesis provides a case study of the Government of Canada's former Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) through the lens of horizontal management (part of New Public Management theory). This study demonstrates that the effective use of horizontal management (horizontality) may reduce fragmentation occurring when the goal of critical infrastructure protection requires organizations to work cross-jurisdictionally and in partnerships. This need to collaborate is due to the ownership problem: over 85 per cent of Canada's critical infrastructure is owned by organizations other than the federal government.

Research methods include a background survey of literature on critical infrastructure protection, horizontal management and horizontality, and new public management; and interviews using a snowball sample of eight subjects who held various positions within OCIPEP to better understand what the organizational structure appeared to be from within the organization.

The research concludes that OCIPEP was not given the resources necessary to successfully fulfil its mandate. Results indicate the need for administrative and managerial support for horizontal endeavours, to encourage a "cultural context" of horizontality, as there are many organizational barriers to successfully using horizontality and collaborative methods. There were areas of success for OCIPEP, but more areas of weakness. Recommendations include additional study of the organization, a shift into a better-supported organization (which was accomplished with OCIPEP's inclusion into Public Safety and Emergency Preparedness Canada), and clear delineation of roles between the Government of Canada and the owners of the critical infrastructure.

Acknowledgements:

The author would like to thank Dr. Brenda O'Neill and Dr. Paul Thomas for their exceptional help throughout this thesis in reading and re-reading sections, providing feedback and suggestions, and their endless encouragement. Thanks are also extended to Fischer James, Iris and Brian Rountree, and Sarah Thiele for their support proofreading throughout this process. This degree has been financially supported by the Duff Roblin Political Studies Graduate Fellowship, which has been greatly appreciated.

Table of Contents:

Chapter One: Introduction

The Research Question

This thesis examines Canada's former Office for Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) through the lens of horizontal management (part of New Public Management theory), in order to demonstrate that greater reliance upon so-called horizontal management or horizontality will overcome fragmentation which results from the traditional, vertical divisions within modern governments. The aim is to show that the current use and continued development of horizontal management is the necessary approach for accomplishing Canada's goal of protecting critical infrastructure. In order to understand why, the context within which Canada's model for critical infrastructure protection has been developed must be understood, as must the challenges.

The Context

The creation of Canada's Office of Critical Infrastructure Protection and Emergency Preparedness was announced on February 5th, 2001 by Prime Minister Jean Chrétien, to combine Emergency Preparedness Canada (EPC) and the Critical Infrastructure Protection Task Force. OCIPEP was created due to the widespread belief that both the physical and cyber segments of critical infrastructure were increasingly at risk for incapacitation due to deliberate, accidental, or age-related failures.

In Canada, concerns about the protection of critical infrastructure came to be widely recognized with preparations for the Y2K rollover and the need to update computers and cyber technologies to prevent unpleasant and possibly dangerous consequences, not just with regard to computers but also to all other utilities depending on computerized parts to make them work. This resulted in Emergency Preparedness

Canada working with other departments to compile a catalogue of essential services. After the year 2000 turnover came and went with no major incidents, other uses had to be found for the information already collected. In December 2000, the Government of Canada began a one year Critical Infrastructure Protection Task Force to research critical infrastructure, with the aim to report what (if any) role the Government of Canada should take with critical infrastructure protection. On February 5, 2001, Prime Minister Jean Chrétien announced the creation of the Office of Critical Infrastructure Protection and Emergency Preparedness, a civilian organization located within the Department of National Defence, to build upon and take over the Emergency Preparedness Canada organization. OCIPEP was given the dual mandate to deal with both critical infrastructure protection and emergency preparedness, and was at that time the only organization in the world with such a mandate. The Government of Canada created this office because of the widespread belief that both the physical and cyber segments of critical infrastructure were increasingly at risk of failure, either because of accidental, terrorist or natural disaster causes.

OCIPEP was created to fill specific needs: to provide an over-arching body capable of and dedicated to coordinating the critical infrastructure protection plans of not just the federal government, but also those of private industries, as well as provincial and municipal governments. Such coordination was (and continues to be) necessary due to increased technological integration. After a disaster strikes, first responders and the municipality or province (depending on the location of the disaster) are initially responsible for the response. Determining what role should be played by the Government of Canada can be difficult. After a disaster, blame for what did or did not happen in

response or what was or was not planned for is often passed, ultimately, to the Government of Canada even if the results of the disaster are not under the government's legislated jurisdiction.

From OCIPEP's creation until December 2003 when Prime Minister Paul Martin moved OCIPEP into the newly created department of Public Safety and Emergency Preparedness Canada (PSEPC), OCIPEP acted as a lead agency that had the potential to educate, guide and possibly direct other departments in their actions and preparations for the protection of critical infrastructure. This posed a number of challenges, not the least of which was due to OCIPEP's location within the Department of National Defence and the resulting issues of being within a department that did not really understand OCIPEP's mandate or share its goals, as discussed in Chapter 3. These issues largely have been removed with the move to the new department and integration with the Solicitor General's office, and time will tell if that move will improve the efficacy of PSEPC with regards to critical infrastructure protection, both as an organization and as a resource for other government departments and outside organizations.

Challenges and Opportunities

During its existence, OCIPEP was required to develop knowledge of critical infrastructure protection and the policy and administrative means available to address the complex problems involved. The abrupt beginnings of OCIPEP provided a disadvantage from the start, as the organization was announced and expected to be up and running within a very short time without the benefit of a lead-in time period to set up the organization and get the right people into the right positions. This compounded many of the other challenges that faced OCIPEP. There were challenges with staffing and

financial management and, while it is difficult to rank problems, the ownership challenge was mentioned time and time again as the most important issue that OCIPEP had to contend with.

Roughly 85 per cent of Canada's critical infrastructure is owned by stakeholders other than the federal government (private business, provincial and municipal governments) [1]. This means that while the Government of Canada stated that OCIPEP would be the lead organization to ensure the continuity of Canada's critical infrastructure, it was not as simple as creating and executing plans government-wide. The challenge of encouraging a widely diverse group of stakeholders to work with the government towards the same goals became the single most important one for OCIPEP, made even more difficult by the fact that critical infrastructure is not just one sector but spans ten categories of activity ranging from emergency services to manufacturing. Furthermore, each sector is in some way dependant upon other sectors: emergency services depend on a power source which may be electricity or fuel; each of which are also considered to be critical infrastructure. This emphasizes the need for coordination among all stakeholders.

Ultimately the protection and assurance of critical infrastructure is the responsibility of the owner of that critical infrastructure asset. This is complicated by two factors: that Canadians look to government in times of crisis or emergency to provide (or help others provide) critical services that citizens depend on; and that infrastructures are highly interdependent; that is, that if one utility fails other critical services depending on that utility may also fail. Regardless of which organization actually owns the

---

[1] Canada, Office of Critical Infrastructure Protection and Emergency Preparedness, September 3, 2004. <http://www.ocipep-bpiepc.gc.ca/critical/nciap/synopsis_e.asp>

infrastructure, the Government of Canada is expected to provide guidance and assistance in making services operational and in keeping them operating, and to provide financial assistance during and after emergency situations. This expectation may result from a number of contributing factors: e.g., that many Canadians do not know or understand the constitutional division of jurisdiction between the federal government and the provinces, and thus look to whatever form of government appears to have the most resources (often money-wise) for help. Another factor also hearkens to the constitutional clause of "peace, order and good government,"[2] that has been interpreted through the courts and the emergencies act to allow the federal government the authority to act during a national emergency.

Since many of the critical infrastructures are not owned by the Government of Canada, methods of guaranteeing, or assuring, the services must be developed. This was the potential of OCIPEP—an organization dedicated to (a) risk management, (b) assembling information on best practices, (c) information sharing between stakeholders, and (d) a resource for those responsible for critical infrastructure to use when planning for emergencies, and when dealing with consequences.

Connected to the ownership challenge was the opportunity to clarify roles and responsibilities which was an issue both within the federal government and with the provinces/territories and the private sector. OCIPEP was a de facto lead agency for critical infrastructure protection and emergency preparedness, but it did not and could not protect the infrastructure itself; that was up to the owners and operators. Defining the role of the lead agency versus lead sector departments was a key that could have allowed

[2] Introduction of Section 91 of the Constitution Act, 1867.

OCIPEP to work well or fail completely. This introduces the idea of horizontality: when issues cross boundaries, jurisdictional distinctions become an issue that must be dealt with in order for the work to get done. A great deal of work with horizontal issues must be determining who does what, who leads, and how to partner with other constituents.[3] The challenge was to try to produce a critical infrastructure protection product, at the same time coordinating the efforts of others, in order to reduce redundancy and improve information sharing as much as possible.

The fact that critical infrastructure does not end at Canada's borders must also be taken into account which means that while managing critical infrastructure protection within Canada is challenging in itself, plans must be made in conjunction with other countries sharing infrastructure. Phone lines, power lines, roads, and airspace are among the many shared infrastructures not belonging solely to Canada. Of course the power lines on Canadian land and those on American land are the responsibilities of their respective countries, but the electricity that travels the lines "belongs" to both. This is perhaps the most obvious reason behind the need for horizontal organization, as the Government of Canada cannot dictate to other countries how to behave (even with regard to how they choose to protect the critical infrastructure that might affect Canada), so the protection of critical infrastructure requires collaboration, the sharing of ideas, and a commitment to assuring each section of common infrastructure.

Theoretical Background

New Public Management theory posits that government will become more responsive by behaving more like a private business than by using what traditionally have

[3] Confidential interview, December 15, 2004.

been known as governing behaviours. These new ideas include working towards greater efficiency by reducing redundancy and encouraging organizations to work more closely when conditions call for it rather than holding on to ideas of territory and jurisdiction that have been associated with the traditionally "vertical" public service.[4]

Horizontal Management

Horizontal management, or horizontality, is a method of organization used to work across boundaries such as those within the government (departments, committees) and those outside the government in order to integrate policies and service delivery through the sharing of information and development of new solutions. Horizontality brings people together who have common interests and responsibilities, to use each other's knowledge and ideas to better address common concerns. It can involve any number of actions that resulting in working across traditional boundaries and will be discussed further in chapter 2. Utilizing horizontal management attempts to overcome the fragmentation that commonly arises due to vertical divisions within modern governments and the even greater divisions between governments and business and other, non-governmental industries.

Horizontal management, or horizontality, can be said to exist

> [w]hen one or several managers of one or several organizations address a question no longer based exclusively on preoccupations for which they are responsible, but on a wider approach aiming at including interests, resources and constraints of other stakeholders of this field.[5]

---

[4]Robert B. Denhardt and Janet Vinzant Denhardt, "The New Public Service: Serving Rather than Steering", *Public Administration Review* 60.6 (2000): 549-559.

[5] Jacques Bourgault and René Lapierre, *Horizontality and Public Management* (Ottawa: Canadian Centre for Management Development, 2000) 1.

These ideas are not brand new, as cooperative ventures demonstrating horizontal management have gone under names such as collaborations, alliances, interdepartmental actions, joint ventures, co-actions, and partnerships.[6] The benefits of working in this manner include a more effective use of resources, both financial and human; exposure to differing organizational cultures and perspectives; and decreased redundancies. Further benefits include access to greater sources of knowledge and information sharing, greater potential for coherence and coordination, and the sharing of risks. Gathering together for the purposes of one specific project or initiative people who normally would not work together may allow for unique and inspired collaboration unhindered by the customs and traditions within a particular department or agency.

Such horizontality also has challenges. Dual loyalties of participants to their "home" organizations and to the horizontal project result in gray areas around information disclosure and the level to which an individual has the authority to speak for their home organization or commit it to a course of action. Trust, both inside the group and in the home organization, can be difficult to build and maintain.[7]

Central to the concerns about horizontal government is accountability. The challenge of maintaining a clear sense of accountability is complicated by the crossing of boundaries inherent with horizontal projects, e.g. how to explain such a project and its outcomes to the public[8], as well as the question of personal accountability (for example,

---

[6] Bourgault and Lapierre 1

[7] Bourgault and Lapierre 5

[8] Jacques Bourgault, *Accountability and Horizontal Management: An Approach for the Quebec Federal Council, Report to Marlynn Brisebois* (Ottawa: Treasury Board of Canada Secretariat. 2002) 7.

performance evaluations). In Canada the tradition has been that an individual Minister is responsible for the works of his or her department, but with horizontal projects there is difficulty pinpointing who should take the role of responsibility when the project is part of more than one department. Further, challenges related to building consensus within the project group may lead to "group think", where individuals succumb to the will of the group rather than taking into consideration information which might contradict the sometimes false consensus that group think contributes to. Each of these must be considered when weighing the use of horizontal management. With projects that cross jurisdictional boundaries there is no better way to coordinate the interested parties than to involve them in the development of the project.

For horizontal management to be successful, skilled and effective leadership is key. Such leaders must be able to effectively link the organization back to the vertical structures that have created the horizontal organization through the allocation of resources and/or the granting of authority for the project. A culture of trust and collaboration needs to be developed and maintained amongst the different entities involved, as must the momentum of the project. Support systems (such as a secretariat) must be adapted or created, and fit within existing vertical structures.[9] Such adaptation may be well worth the effort given the positive results that may be realized by a well-chosen and organized horizontal project.

There are two dimensions to horizontality: that of a horizontal attitude or culture where individuals can communicate and share information across boundaries; and that of

---

[9] James Lahey (Chair), *Moving from the Heroic to the Everyday: Lessons Learned from Leading Horizontal Projects* (Ottawa: Canadian Centre for Management Development, 2001) 25.

specific horizontal projects that share resources between and within organizations to work towards a specific outcome. OCIPEP falls within the second dimension. It requires the use of horizontal management to fulfill its mandate of providing national leadership through the provision of a new and comprehensive approach to the protection of Canada's critical infrastructure and to be the primary agency for the delivery of national civil emergency preparedness. By definition, the make-up of Canada's critical infrastructure crosses the boundaries of many departments and consequently affects them all.

OCIPEP and Horizontality

> The Government of Canada defines critical infrastructure as being composed of:
>
> Physical and IT facilities, networks and assets whose disruption or destruction would have a serious impact on: The health, safety, security, economic well-being of Canadians; or the effective functioning of governments in Canada. This includes energy and utilities, communications, services such as financial and food services, transportation, safety (including nuclear safety, search and rescue and emergency services), and government and the government-wide critical systems like pensions, Employment insurance.[10]

OCIPEP requires coordination on both policy and management levels. Horizontal management encompasses both levels which distinguishes it from what is traditionally defined as "management". Due to the inter-disciplinary nature of critical infrastructure protection, including players at all levels of government and in the private sector, much diplomacy and openness are required to plan in a meaningful way and to ascertain best practices. The jurisdiction of each party must be respected while at the same time the

---

[10] Canada, Office of Critical Infrastructure Protection and Emergency Preparedness, *Slides-Presentation to DSAB Asymmetric Threats Study Team* (Ottawa: January 15, 2002).

federal government must feel confident that its critical infrastructure protection will not be compromised through the failure of critical infrastructure under another organization's jurisdiction.

The use of horizontal management creates a challenge for those who are implementing OCIPEP, primarily through the difficulty of creating legitimacy for a new institution, and through the necessity of the involved departments, organizations and governments taking seriously the fact that OCIPEP is in some ways charged with helping them with their implementation of critical infrastructure protection, whereas before it was strictly under their control. These difficulties can be as mundane as getting the same person from each department to attend OCIPEP meetings. Those with whom OCIPEP must negotiate and organize are members of both the public and private sectors, each of whom shares the aim of critical infrastructure protection but may use frameworks that consist of differing norms, values and motivations.

While this paper was written the Office of Critical Infrastructure Protection and Emergency Preparedness ceased to exist as a separate entity within the Government of Canada and was incorporated into the new department of Public Safety and Emergency Preparedness Canada, which brings together the former OCIPEP, the activities of the former Solicitor General, and such organizations as the RCMP and CSIS in order to have all public safety and emergency preparedness activities within one overarching department. This has been a move from the lead-agency status of OCIPEP with its horizontal attitude to a department that still must work horizontally but may be perceived as having the increased legitimacy given by vertical structures. It is a more highly visible department that likely will make it easier to get the attention and cooperation of other

departments and provincial and territorial governments. Most interesting about this development is that while it initially decreases the horizontal aspect of OCIPEP, it likely will improve horizontal functioning through increased legitimacy and a higher profile as others may take it more seriously by feeling obliged to contribute to its activities.

Very little is written about the organizational structure of Canada's critical infrastructure protection plans and about how they were managed. Concern for the ability of Canada to successfully protect its critical infrastructure has been expressed repeatedly by both Americans and Canadians, notably during the August 2003 power outage in Ontario and the North-Eastern United States. The importance of OCIPEP is apparent due to increased awareness of threats to critical infrastructures and their interdependencies, yet not a great deal of research has been done on the way that OCIPEP has been set up and how it conducts the business of protecting critical infrastructure.

When it comes to OCIPEP's relation to business, private industries can do a more effective and efficient job of assuring their infrastructure without any Government of Canada involvement,which means that, unless the government provides reasons for that industry to share its knowledge and expertise, the government will lose out on that business's experience and contributions to best practice models.

Case Study Format

This thesis was written in order to examine carefully, through a case study, a unique example in recent Canadian history of an organization that was set up and expected to operate using horizontal methods. Horizontal methods have been recognized as beneficial for the Government of Canada to use due to their ability to approach problems from multiple angles and ideally to use fewer resources to achieve the best

possible solution. Horizontal management has been put forward by the Government of Canada, largely through the Canada School of Public Service, as a method of achieving what was unlikely to be achieved through traditional, vertical management, with fewer costs.

It has also been recognized that horizontal management can cost greatly in financial, time and human resources, and may not be as efficient as working through the more traditional approach of vertical policy-making and service delivery based on line departments. There have always been multiple challenges when people attempt to work cooperatively, and horizontal projects within government frequently demonstrate this fact. The success or failure of such projects depends greatly on such factors as champions and leadership, tools and resources, how the central agencies react, and accountability. In the time that it existed, OCIPEP had far more challenges and difficulties than it did successes, and this is due to multiple factors to be discussed below, that include staffing, management, finance mismanagement, physical location and the difficulty of convincing stakeholders of the benefits of working with an emerging organization that had not fully been organized. Each of these challenges will be studied for the lessons offered, because the critical infrastructure protection can not be effectively achieved in any way other than horizontally. While it may be possible to retrospectively determine what worked well and what did not, this idea of cooperation and collaboration offers more than any other can to make Canada safer for everyone.

The case study format was chosen for this topic of horizontality and OCIPEP due to OCIPEP's unique position within the Government of Canada. During the time that OCIPEP existed as a stand-alone agency it was unique both because of its mandate

requiring cross-jurisdictional work as its main activity and because of the "building the airplane at the same time as flying it,"[11] that OCIPEP was expected to be functional at the same time as it was developing and determining how it should work. While there is merit to studying the creation of OCIPEP in comparison with other organizations, in this circumstance a case study was determined to be a valuable addition to what is available regarding the development of a new organization and on the bridges built between organizations. The researcher started collecting information about this organization six months after its creation and has been able to assemble information throughout the three years that OCIPEP was in existence and note the evolution of rhetoric and policy even within the publicly available information through the Government. This is an important area for research due to the newness of this organization and the lack of research undertaken on this topic in a specific Canadian context. Ideally, the research will add to what is available on the development of a new organization within government, on the bridges built between organizations as the policy issue crosses traditional jurisdictional boundaries, and on how the organization changes when incorporated into a more traditionally recognized structure within a distinct federal department despite continuing to work horizontally.

An in-depth case study is a useful format to choose when working to increase knowledge about an organization. This idea comes from Harry Eckstein's work on case studies with relation to their utility both in themselves and as an alternative to comparative works with regards to developing theory. Eckstein provides a continuum of views on the validity and utility of case studies, ranging from option one which states that

[11] Confidential interview, December 15, 2004.

case studies and comparative studies are absolutely separate and unequal, with case studies providing only an unsophisticated precursor to a comparison; to option six which describes case studies as the most legitimate test of a theory, over and above comparative studies which may propose probabilities that case studies later can test.[12] Of course extremes are primarily used to demonstrate the extent to which an idea or practice can be carried out. What is more helpful for justification of a case study in this paper is the option only slightly removed from the extreme, option five, which proposes that "…in attempting to validate theories, case studies and comparative studies generally are equal, even if separate, alternative means to the same end."[13] It goes on to allow that the choice between case and comparative studies might be based on arbitrary factors, or those less arbitrary such as "…the particular nature of theories, accessibility of evidence, skills of the researcher, or availability of research resources,"[14]

The previously mentioned uniqueness of OCIPEP and the timeframe for completion of this paper were both contributing factors in the choice of a case study to examine OCIPEP. This also allowed for a more in-depth examination than would have been possible using a comparative method, considering the parameters of a Masters thesis. The utility of assessing the information comparatively would be valuable to "test" ideas put forward here, but is not required in order to learn lessons from a careful examination of OCIPEP.

---

[12] Harry Eckstein, "Case Study and Theory in Political Science," *Handbook of Political Science: Strategies of Inquiry, Volume 7* Eds. Fred I. Greenstein and Nelson W. Polsby (Don Mills: Addison-Wesley Publishing Company, 1975) 92-94.

[13] Eckstein 93.

[14] Eckstein 93.

Research Methods

The underpinning of good research is an appropriate, clearly defined and ethical methodology. This section will detail about the research method including ethical considerations, data collection tools, and procedures for confirming data.

Methodology

In addressing the research aim, "To show that the current use and continued development of horizontal management is the necessary approach for accomplishing Canada's goal of protecting critical infrastructure," the research undertaken was two-fold—the first being a survey of background information available through government publications and on the Internet. The second aspect included in-depth interviews with a select group of government employees who were employed with OCIPEP during some time period between its conception to its absorption into Public Safety and Emergency Preparedness Canada. Interviews were required to collect information on the rationale for the establishment of OCIPEP, its internal operations, and on how the practice of protecting critical infrastructure had changed given OCIPEP's absorption into the new department of Public Safety and Emergency Preparedness Canada, announced December 12, 2003. Given that publicly available information about the organization is filtered through a political lens, interviews were necessary to provide a more informed evaluation.

Elite and Specialized Interviewing

The format chosen for the interviews was that of Lewis Anthony Dexter's *Elite and Specialized Interviewing*. What is unique about this approach is the acknowledgement that each interviewee receives an opportunity to tell their story or share

their information their way, using their definition of the situation. The interviewee is encouraged to structure the interview to what makes best sense for them and with their understanding, and by letting the interviewee introduce what s/he feels is relevant, rather than the interviewer imposing their own views.

The reasons for choosing a non-standardized interview are several. First, a more qualitative, open-ended approach is appropriate for an exploratory study of relatively recent events which are not well-documented or analyzed in secondary literature, and thus are open to differing, subjective interpretations. To capture the nuances and dynamics of these events it was preferable not to force respondents into pre-determined response categories. This allowed the information from later research stages to further contextualize the data collected during the earlier stages.[15] Second, due to constraints of time and cost, only a small number of interviews were conducted. The small sample size meant there was limited potential for any aggregate type of analysis. A more structured interview style might have missed the wealth of information presented by the interviewees by searching for more specific information, and information revealed might have been put aside as not useful because it did not fall within specific parameters.

Third, the reason for interviewing was to access information that would otherwise be unavailable, as what is readily available is filtered through the government. While that information is useful for background it does not necessarily provide insight into reasons

---

[15] "For instance, during the stage of formulating the research questions, some interviewing is already carried out. Findings from the interviews further determine the interview questions, that in their turn give shape to further observation. In short…a continuous moving back and forth between the diverse stages of the research project." Piet J. M. Verschuren, "Case Study as a Research Strategy: Some Ambiguities and Opportunities," *International Journal of Social Research Methodology* 6:2 (2003): 131-132.

behind the decisions made or the climate within the organization at specific times. It was also important to let the information unfold as it would and to be able to use whatever information the interviewees felt was relevant. While questions were prepared to prompt discussion, they were deliberately open-ended.

Subjects and Interviews

Eight subjects were interviewed. The first interviewee was an individual referred to me by my thesis advisor; whose expertise stems from having been employed in the organization for several years. Additional subjects were suggested by the first interviewee (snowball sample). Each subject was asked via e-mail if they would be interested in participating in this study. Interviews took between 30 minutes and one hour, depending upon the length of responses and time that respondents had available. The differences in time were due to the fact that this was not a standard structured interview.

The use of a “snowball sample” was a useful choice for this case study, as only one potential interviewee declined the invitation to be interviewed, and that was through attrition after many efforts to schedule a mutually convenient time. The other prospective interviewees contacted chose to be interviewed and a few passed on additional names of people who might have been willing to help. It was not possible to contact each person who was referred as a potential subject due to time constraints. Initially, the researcher hoped to interview between three and six subjects, however, due to the positive response the final total was eight.

Interviews took place over the telephone as all subjects work in Ottawa, with telephone interviews arranged via e-mail. The e-mail provided a summary of the research questions, information about confidentiality, data storage, and the process with which the

subjects could choose to contribute to the research—the initial interview, follow-up interview(s) if desired, and approval of written information gathered from the interview. Depending upon the subjects' wishes, they might be interviewed once or more than once if they preferred to add to the research at a later date.

Each interview was recorded on audio-cassette, with the researcher taking notes from each recording. The recording was done with a tape recorder connected to the telephone which meant that the conversations could happen normally rather than trying to take notes while the subject was speaking. Each subject was informed of the recording both in the e-mail and at the beginning of the interview and given the option instead to be recorded through the researcher's making notes. Subjects could also change their minds after being interviewed and could have their information removed by contacting the researcher by phone or e-mail. The information would then be removed from the study and destroyed.

Consent was obtained via e-mail and verbally over the phone. Formal written consent was not obtained as subjects' consent was voluntary and understood due to the number of e-mail contacts before an interview took place. Subjects were informed during the telephone interview that they could refuse to answer a question or end the interview entirely at any time without repercussion. Appendix A contains the text of the introductory e-mail. This study involved no deception on the part of the researcher and presented minimal risk to the subjects due to the guarantee of confidentiality on the part of the researcher.

Subjects are not named or identified in any way in the thesis. At the completion of the thesis, notes, audio-cassettes of interviews and electronic files were destroyed. Until

that time, data was stored in a locked filing cabinet at the researcher's personal residence and on a personal computer (which was password protected and not networked to other computers) so that no other people had access to it. There was no compensation for the subject's participation.

Interview Questions

Questions asked of subjects revolved around the subject's involvement with OCIPEP and what their experience had been working in that environment. Questions then revolved around the subject's perceptions and opinions about the rationale for the creation of OCIPEP, the challenges faced by the organization and how they were or were not addressed, and how OCIPEP worked with line departments and provinces. Respondents were asked if OCIPEP was a different environment in which to work because of the cross-jurisdictional nature of the work compared to traditional line departments. If a respondent was involved with the transition after December 12, 2003, questions were asked about this process. Open-ended questions were used to encourage respondents to provide their experiences, perspectives and interpretations. This was important as the subjects know better what was important in their experience and this allows a check to the researcher's biases that may come up through asking one question rather than another, or following one line of inquiry while ignoring other more salient points. The information sought concerned why OCIPEP was created, how it was organized, how it worked with other departments, and how well it fulfilled its mandate.

To provide respondents with the opportunity to review the researcher's interpretation of what they said, the information from interviews was written up and sent to them with their responses highlighted, if applicable. Subjects could give feedback on

the researcher's interpretation and could also choose to remove their information from the study at that point.

Ethical Considerations

The project received ethical approval from the Joint-Faculty Research Ethics Board at the University of Manitoba on November 16, 2004. There was a guarantee of confidentiality for subjects both in the interview process as no subject was identified as having participated or not in when speaking to other subjects or potential subjects, though some contacted parties did agree that their names could be used to invite further subjects to be interviewed. Each subject was sent parts of the thesis to which they had contributed in order to proofread it for accuracy, and to ensure that it was written in a way that was non-attributable. In a small organization such as OCIPEP, where most people know each other, this was important in order to encourage candour and to prevent the identification of opinions with specific individuals. A breakdown of the divisions and positions in which each subject worked is not included here for that very reason, that it could be easy for people with knowledge of the organization and those who worked in it to identify some or all of the subjects.

Study Risks

A potential risk in using a sample where subjects refer further subjects is that the diversity of opinion and experience might not be fully represented, as people are likely to associate with others who share the same experiences or outlooks. This risk was considered and noted, and while it is a possible weakness for this case study, the choice of eight subjects was considered acceptable due to the potential sample size of OCIPEP which was just over 300 people at its end point. Data collected from subjects was not

identical, and while some similarities were noted, there was enough diversity of opinion and presentation that the data was useful. Subjects were located throughout the organization, from a senior management level, middle management, and those who started their careers with OCIPEP. Subjects also differed in age, experience, and current job positions.

Telephone interviewing was the method of choice due to the subjects' location in Ottawa and the researcher's location in Winnipeg. The possibility was considered of the researcher travelling to Ottawa to do the interviews in person, but discarded due to the logistics of trying to set up all interviews in a time span of a week or less, especially considering that subjects referred subsequent subjects. In the case of in-person interviews, multiple trips to Ottawa would have been required, and that was not a possibility financially or time wise for the researcher. An advantage of the telephone interview using audio recording was the relatively low distraction level, and the ease of transcription as the only information available was audio.

Research Outcomes

Research was carried out with due consideration to ethical issues, and according to guidelines provided by the University of Manitoba Ethical Review committee. All efforts were made to ensure that subjects would remain confidential and the information they provided would be unidentifiable to others within the organization. Cooperation shown by former employees of OCIPEP was exceptional, and further research would be expected to be relatively easy to conduct.

While it is always easier to use hindsight to critique an organization, the need for horizontal management when administering a field as diverse as that of critical

infrastructure protection has not changed. The problems with OCIPEP resulted from human error ranging from an unreasonable optimism in thinking that the organization could set itself up at the same time as it could begin to produce results, to unacceptable financial management methods and poor human resource management. All of these were results of people learning about a new system at the same time as trying to operate within it. This is one of the drawbacks of horizontality: it is so dependant upon human cooperation that in the absence of strong leadership and a unifying vision it will fail. This is also its greatest potential, the ability to approach a problem with options and ideas bounded only by the imaginations of the people involved.

Chapter Two: Horizontal Management

The purpose of this chapter is to examine the management of organizations, starting with an examination of new public management and moving on to one of new public management's subsets, horizontal management. First, new public management will be defined, its origin and its connection to more "traditional", vertical management will be examined. Next, horizontal management, which branches out of new public management, will be defined and its origins examined. Benefits of horizontal management for organizations will be followed by an exploration of difficulties of horizontal management. A discussion of the specific issues of leadership, tools and resources, and accountability will round out the chapter, focussing on the case study framework that Herman Bakvis and Luc Juillet used in their 2004 publication for the Canada School of Public Service: *The Horizontal Challenge: Line Departments, Central Agencies and Leadership*.

The study of organizational management is concerned with the structure and style of management, consisting of both vertical and horizontal differentiation; vertical meaning the number of levels in an organization's hierarchy, horizontal concerning the division of labour at the same hierarchical level. It also examines the concentration of authority and the extent to which the decision-making occurs either within the organization or outside it (in the case of a larger company).[16]

New Public Management

New public management is the practice of deliberately making the management of government more like that of a private business in order to reduce expenditures,

---

[16] William G. Scott et al, *Organization Theory: A Structural and Behavioural Analysis, 4th Ed.* (Illinois: Richard D. Irwin Inc, 1981) 160-161.

increase citizen (client) satisfaction, and improve service delivery. This is perhaps not so "new" a way of managing as the name might suggest, as here in Canada the practice of approaching public management using private sector methods has been used intermittently since the early 1900s due to budget crunches and the public's loss of confidence in public institutions.[17] The United Kingdom, the United States, Australia, New Zealand and Canada have each used various forms of new public management in the revision of government administration.

Ultimately, new public management seeks to change the role of the state through "letting the managers manage," by clearing away some of the bureaucratic barriers in order to better serve the citizen-clients and increase citizen satisfaction through "an insistence on results rather than an adherence to prescribed procedures, to the removal of excessive central agency controls over line departments, [and] the delegation of more authority to public managers."[18] Motivation for many of these changes is provided through the need to reduce government spending yet continue to supply the services demanded by society. This is often accomplished through privatization, networks within government, and partnerships with external service providers, volunteer organizations, non-governmental organizations and throughout government[19]. There is also a shift to

---

[17] Mohamed Charih and Lucie Rouillard, "The New Public Management," *New Public Management and Public Administration in Canada* (Toronto: The Institute of Public Administration of Canada, 1997) 38.

[18] Paul Thomas, *Performance Measurement, Reporting and Accountability: Recent Trends and Future Directions* (Regina: The Saskatchewan Institute of Public Policy, 2004) 4.

[19] Charih and Rouillard 27.

implementing pay-for-service fees rather than the funds coming from the general pool of taxes.

Governing under the new public management paradigm often involves transforming the public service from an institution made up of large departments (which is operated on the basis of government-wide systems and rules and with central authorities allocating resources), to a civil service consisting of more diversified entities (other than the traditional departments) with decision-making decentralized and with more insistence on and measurement of results.

Efforts at restructuring the state according to the principles of new public management can be traced back to Margaret Thatcher in the United Kingdom with her efforts to increase the state's responsiveness to the public by decreasing its power, to improve the economic efficiency of government through private management practices, and empower citizens to "counter the dominance of state control over the design and delivery of public services."[20] Devolution was considered to be a primary tool, that is, moving power from the hierarchical centre towards the fringes so that decision-making occurs closer to constituents to improve resource productivity with no decrease in the public service offerings.[21] Successful devolution relies on clear directions given to the people charged with implementing services regarding policy direction and a continuous attention to accountability and responsibility both for front-line service providers and those public servants managing organizations. If the desired direction is unclear the

---

[20] Peter Aucoin, *The New Public Management: Canada in Comparative Perspective* (Montréal: The Institute for Research on Public Policy, 1995) 1.

[21] Aucoin 141.

advantages that devolution promises may be moot due to less successful application of the policy directions.

Ultimately the appeal of new public management is due to the negatives attached to the “old public administration,” such as the limited citizen involvement and slow response inherent in a top-down system directed by a centralized bureaucracy. The very neutrality that is inherent in traditional public administration is still a requirement, but does not require that every decision must be funnelled through a central office, which requires intervention by elected officials in order to speed up the process.

New public management purports to correct this by increasing the ability of members of the public service to be able to solve the clients’ problem directly, which may be quicker and require the use of fewer resources (including financial and human resources). This must be balanced with the maintenance of the traditional neutrality that is required to prevent favouritism towards individuals or groups. Part of this can be due to a flatter organization – more horizontal with fewer vertical levels to go through. Another part of this involves building partnerships to expand the “no wrong door” approach to service delivery as they can reduce redundancy of service provision and identify and close gaps in service.

Horizontal Management

Horizontal management is one way that new public management purports to increase citizen satisfaction, and to improve the coherence and effectiveness of policy approaches. Horizontal Management has developed from new public management in response to the vertical organization of traditional public management and its limited ability to respond to partnership approaches. Such partnerships are required due to

decreased or limited funding and the necessity to work with a number of parties to deliver services in the most cost-effective manner with the greatest response to the citizen/consumer.

Horizontal management, or horizontality, involves working in teams with hierarchical relationships less emphasized or obvious than in traditional public organization. Horizontal management goes under a number of names. In the United Kingdom it is often referred to as "joined-up government", Australians prefer "integrated government", other times it is known as "horizontality". A Canadian Centre for Management Development (now known as the School for Public Servants) publication refers to three degrees of horizontal work:

1. Horizontal attitudes and culture – individuals making conscious decisions to work horizontally in daily work, building informal ties that facilitate sharing;
2. horizontal coordination – organizations coordinating work to reduce or eliminate overlap and duplication;
3. horizontal collaboration – resources, work and/or decision making integrated across organizations.[22]

These dimensions allow for a wide range of projects or operations to be labelled as horizontal depending upon their degree of integration of service offerings and how formal or informal those ties are. In this paper horizontal management is used to mean both horizontal coordination and horizontal collaboration, but not necessarily horizontal

[22] Lahey 2.

attitudes and culture as they are the most difficult to integrate into existing organizations and programs.

While horizontal structures and processes are often on the surface the simplest to implement into vertical structures; actual changes to the flow of information, accountability structures, responsibilities, human resources and financial costs can be time-consuming and difficult to integrate into organizations previously organized vertically. Structural changes can be done relatively quickly but changing the attitudes and day-to-day corporate culture is often described as a slow, uncertain and problematic process taking years, if not decades. For smaller projects, those newly created, or committees, horizontal attitudes and culture can encourage horizontality through the free flow of information among co-workers and peers, yet do not require any sort of formalized procedure or project. Horizontal coordination and collaboration can exist along a continuum of integration, permanence, duration of project and many other aspects and they offer the greatest challenge to the vertical, hierarchical structures that comprise most of government today.

Working horizontally is not the most efficient use of resources, but arguably the most effective due to the goal of service provision with the best use of resources.[23] Jacques Bourgault explains,

> [H]orizontality means having a mandate to address matters of common interest from a broader point of view, alone or in partnership with co-workers inside or outside his or her organization, with due regard for the interests, resources and constraints of a number of stakeholders who are active in his or her particular field…go beyond a concern with his or her

[23] Lahey 3.

> own responsibilities and seek the common good in a spirit of synthesis and cooperation. [24]

The object of horizontal management is to reduce the appearance of vertical differentiation, that is, the number of levels that separate the chief executive from the employees working at the bottom of the organization in order to make the organization more responsive and effective. Considering that many projects cross jurisdictions and require the input of a variety of people who may not be situated within the same department (or organization), bringing these people together to work on projects utilizing their special experience and knowledge reduces duplication of services as compared to trying to do these projects "in-house". Unfortunately, this increases difficulties with accountability and the division of responsibility when traditionally the tool used to achieve these in the Canadian government has been Ministerial responsibility—holding the responsible Minister accountable for what the department does, rather than the individual public servants who carry the work out.

Bakvis and Juillet, in their 2004 paper *The Horizontal Challenge: Line Departments, Central Agencies and Leadership*, state that there are number of conditions which, when in place, make a specific horizontal initiative become a reality. The first is that a problem exists which must be worked on sooner rather than later. Second, there must be leadership available. Such leadership is likely to come from a person or persons who are known for thinking "outside the box," who are located somewhere in the middle of the organization rather than at the top. Third, there likely exists a "…situation of ambiguity or vacuum that allows innovative actors to propose novel solutions to resolve

[24] Bourgault 1.

problems and to use those innovations in a strategic manner."[25] Finally, the resources must be available, which is contingent on someone with power at the top of the organization who believes in the project enough to contribute some level of resources to the project. One department taking this stand to show a level of commitment to the project is often enough to bring other partners on board. The demonstration of support may convince others that it is a worthy initiative.

Benefits of Horizontal Management

Horizontality is less a way to reorganize entire departments and more a way to improve the way resources are used by decreasing duplication of service. Instead of multiple departments working on the same issue in slightly different ways, horizontal management advocates bring interested parties together across departments to work on a common solution.

Horizontality can be said to exist when some combination of managers from different organizations or different parts of an organization agree to address an issue that is broader than they each specifically are responsible for, in order to better solve it, often including other stakeholders and their interests and resources in both the process and the solution.[26] These approaches may be called alliances, interdepartmental actions, joint ventures, co-actions, partnerships, possibly other names as well, and have in common the association with others who have interests in the same area not as a threat but as co-contributors.

---

[25] Qtd in Bakvis and Juillet 19. (M. Barzelay and C. Campbell, *Preparing for the Future: Strategic Planning in the US Air Force* (Washington: Brookings, 2003))

[26] Bourgault and Lapierre 1.

Such partnerships are more likely to work successfully depending upon how clear the mandate given to the partners is and how this mandate is backed up (with resources: financial, human, time and support, both administrative and political). Those who work together must avoid getting bogged down with arguments about symbols and minutiae and maintain the focus on the problem and be able to manage the demands and timeline of the project as well as that of their regular work, if they are not able to devote their entire time to the project. The conduct of the group can also result in either a highly effective project or a disorganized one. This can be helped through the clarification of each member's role and function, even through stating the common values between group members and/or other stakeholders. The point really is to get participants on the same page by letting them feel ownership of the project.[27]

Horizontal management allows the opportunity to divide work based on the strengths and expertise of the participants, more so than some vertical projects, due to the room for movement among tasks and perhaps less emphasis upon prestige and advancement conferred due to different roles and working in teams.

> Horizontal management is not an end in itself or an objective, but rather it is an effective means in some circumstances. It will never replace hierarchical structures. Besides, when horizontal management formulas run into difficulties, it is the hierarchical structure system that comes to its rescue (money, recognition, professional or hierarchical authority).[28]

The reason why horizontal management is an effective organizational tool is that through sharing costs, information, and experience many risks are reduced, including

---

[27] Bourgault and Lapierre 12.

[28] Bourgault and Lapierre 18.

financial, technical, and political risks.[29] It is also effective for the very reason that the aim of improving service quality is not likely to be debated. A great deal of what has been done to "flatten" service delivery has been done due to financial restraints and budget restructuring, and "…criticism tends to be directed at the quality and quantity of the services provided, rather than the structures used for delivering them."[30]

Difficulties of Horizontal Management

The many arguments for the use of horizontal management do not sway all detractors as there are some problems that the use of horizontal management tends to exacerbate. The first is that horizontal management "elongates" the decision-making process, meaning that making decisions is more complicated and time consuming and requires communication and to rally support for the decision made. Considering the difficulties of building relationship between all participants and the need to maintain good relationships while resolving difficulties, a decision most often will come about after some consultation with others participating in the network, and not simply be made by one person. Considering also that many participants will have to "sell" the decision back to their home organization or department it is important for them to agree with, or at least understand, the decision well enough to explain it to others and perhaps convince them of its validity.

---

[29] Bourgault and Lapierre 19.

[30] Lawrence J. O'Toole Jr, "Different Public Managements? Implications of Structural Context in Hierarchies and Networks," *Advancing Public Management: New Developments in Theory, Methods and Practice*, ed. Jeffrey L. Brudney et al. (Washington DC: Georgetown University Press, 2000) 333.

Another difficulty is the possibility of succumbing to "group think", thereby making it near impossible to make the tough decisions. This is due to difficulties inherent with collaboration, among them the desire to limit conflict that may be difficult to resolve to the satisfaction of all participants. At times this leads to the avoidance of actually making difficult decisions, instead culminating in benign, yet meaningless decisions, and "…pursuing consensus at the expense of serving the public interest."[31]

There is also the possibility of a disconnect from the vertical structures that participants belong to and represent. Some participants may not have the ability to commit their organization to a decision or plan of action. If such participants must refer matters back to their leaders at all times the lack of trust or authority may hinder the horizontal project. This is one example of the requirement of trust both within the horizontal group itself and on the part of the organizations involved in the project. On the other hand, a failure by a group member or members to communicate the group's activities back to their vertical structures can cut lines of accountability and authority.[32]

Leadership

The importance of effective leadership and good management of the project cannot be underestimated. Horizontal partnerships require a high degree of maintenance on the part of their participants and leaders due to their organization in a different manner than that of the more common vertical hierarchy of government. Leaders must be able to motivate participants and help them to work towards a common solution despite the multiple viewpoints of stakeholders and varying backgrounds of those involved. Leaders

---

[31] Lahey vii.

[32] Lahey 4.

are also important when the logistics of the group are considered, for example, when people who are new to the project and/or to work in a horizontal manner replace more experienced participants as representatives from their organizations. At those times, the "…leader[s] must create and retain a corporate memory …we do not always want to start over and the group should not suffer any delay every time the representative is replaced."[33] The success of a project also depends upon the priority it is given by stakeholders, and the resources that the project and those participating are allowed. "Resources" refers to all the requirements that the project needs: financial, legal authority, human, information, technological, administrative, the list may continue. The number and diversity of stakeholders or participants tends not to matter as much as the priority they give to it,[34]which can be recognized through the support and resources they are able to allocate. This, of course, depends on what other priorities exist and on to what extent they have "bought in" to the project.

Leadership is a critical aspect of the successful horizontal endeavour in that it can be one of the reasons why horizontal management can work so successfully and it can also be one of the reasons why horizontality can be difficult to administer. Considering that horizontal projects cross boundaries and jurisdictions they are unlikely to carry with them ready-made leaders who are known and accepted by all participants and who know and accept all facets of the project, whether temporary or permanent.

Leaders in any organization are needed to motivate, to provide direction, to assess progress and to guide members back to the original vision when required, as well as to

---

[33] Bourgault and Lapierre 13.

[34] Bourgault and Lapierre 12.

encourage deviation from that vision when necessary. Leading a horizontal project requires a combination of such skills. Leaders also require the ability to mediate in order to bring people from varying backgrounds and organizational cultures together to develop a common lexicon and buy-in so that participants have the ability to speak with the same language and to believe that the project is a valuable one. The leadership team must have the skills to integrate new members or replace former ones and maintain the team's direction and movement. Motivation is needed in any organization, more so, however, in the absence of vertical recognition or formal authority as participants must commit to the project, quite likely along with no decrease in other duties they are expected to perform.

The need for leadership does not preclude the continued need to share the project and its responsibilities. It has been suggested that, in federal programs that have been horizontally managed, successful leadership has been a result of a number of people taking direct control of specific parts of the project, depending upon personal expertise and preferences.[35]

Tools and Resources

In order for a horizontal project to be launched, some of the necessary resources must be in place. This is not strictly dependent on money and finances, but requires additional necessities such as human resources and guides to the tools required to measure costs and benefits (as those tools which are familiar may have been designed for a vertical structure). The remarkable fact is that not all resources need to be in place at the beginning, though the sooner they are available the better. People can and do get by with few resources often at the beginning of a project before adequate resources have been

[35] Lahey 8.

allocated. This was the situation with OCIPEP, which will be examined in detail in chapter 3.

The most obvious resource needed is that of employees: the project will not get off the ground if the right people (which are those with the necessary knowledge and skills) are not available. Many horizontal projects depend on seconded employees, people participating part-time, or even voluntarily, as the horizontal project is added to the work they do in addition to their own jobs. When it comes to people, recruitment is not enough: there need to be incentives such as professional development, training, and/or other rewards in order to make it worthwhile to be involved with the project. An incentive may be as simple as the opportunity to work on a project which fits with personal values or vision of what is important work for the organization. Considering that horizontal work is often in addition to a person's regular duties, such incentives can make the difference between a successful project and one which is consistently replacing players and thus spending more time training people than working towards its goals.[36]

Horizontality may also act as a disincentive, discouraging collaboration. Much of the measurement of the performance of a person or department has to do with serving the Minister, and how the department or agency performs in accordance with their stated aims, not in relation to the collective goals of government. Monetary bonuses are paid for the performance of individuals or programs, not for contributions to joint endeavours. Accountability systems are linear, vertical, and individual in their focus, not collective.

---

[36] Herman Bakvis and Luc Juillet, *The Horizontal Challenge: Line Departments, Central Agencies and Leadership* (Ottawa: Canada School of Public Service, 2004) 20-22.

Next, the requirement of funded operating and capital costs must be considered. One of the continuous challenges is the continued financial priority of the project. In order for a horizontal project to have continued financial support there must be a combination of vertical (or more permanent) structures along with horizontal ones. This is due to the fact that "…even without the real or imagined adversarial relationship among organizations, coordination activities almost certainly will receive a lower priority than activities that contribute directly to the mission of the organization…"[37] Difficulties of allocating financial resources within the budgets of the stakeholders contributes to this, as well as a lingering feeling of temporariness, though there is the possibility of the project being directly funded by government.

Accountability

In the context of horizontality, accountability consists of two components: that of giving a proper account of the activities in question, and of being held responsible for those activities.[38] Another consideration with specific importance for horizontal projects is the need to couple accountability with responsibility and authority. It is not possible to hold a person or organization accountable for a decision or project if they were not in a position of authority or responsibility in the first place. This is one of the requirements that comes up when discussing horizontal projects and their limitations: the need to regularly report back to the home department or organization to make sure that the participant has the ability to commit their organization to a course of action.

---

[37] B. Guy Peters 10.

[38] Bakvis and Juillet 23.

While horizontal projects need to create their own measures of success and accountability, they do not exist within a vacuum and,

> …Mere structural manipulations cannot produce changes in behaviour, especially if the existing behaviour is reinforced by other factors in government. These other factors, including the budgetary process and links between programs and powerful external interest groups, may be difficult to overcome simply by altering formal structures.[39]

This explains why the need to agree upon accountability and responsibility frameworks is critical and is a process that must be done on a case-by-case basis as there is not just one correct framework or accountability structure for each and every circumstance. Challenges arise because accountability structures which have been created by and for vertical organizations do not translate readily for horizontal projects or organizations.

Accountability is of fundamental importance to both the new public management crowd and those working with horizontal management. Accountability can be looked at as an "…obligation to explain, justify action, use resources economically and effectively, prove performance and take responsibility for it with regard to prearranged expectations."[40] It requires relationships where decisions are made about people or groups taking on specific responsibilities. Those who have taken on such responsibilities are obliged to answer for how successful (or unsuccessful) they were. One of the assumptions that relates to accountability is that it will result in penalties for non-performance and rewards for successful performance. These penalties and rewards may

---

[39] B. Guy Peters, *Managing Horizontal Government: the Politics of Coordination* Research Paper 21, (Ottawa: Canadian Centre for Management Development, January 1998) 47.

[40] Bourgault 7.

be tangible (such as demotion or promotion) or symbolic (such as humiliation or praise)[41].

In order to provide penalties or rewards, performance must be measured, which requires that there is a set of goals or objectives that are clear and able to be measured. Performance measurement is a challenge in any area in which it is undertaken: it is more challenging and complex in a situation where there are conflicting jurisdictions and participants with loyalties and obligations to their home organizations, the horizontal project, and other participants.[42] Another difficulty in measuring the performance of a horizontal project is that it requires financial resources that often are better spent in furthering the project itself. Added to this are the divergent views of stakeholders who may have differing opinions as to what is important and what should be measured, as without a clear statement of what will be understood as satisfactory performance (with achievable outcomes) it will be impossible to work together as a cohesive group.

When employees of the public service are evaluated on their performance the benefits of any horizontal work they have been involved with should be incorporated into their evaluation. This is part of the reason why accountability and performance measurement is important as there is little benefit to a person joining a horizontal project if they will not be recognized for the work and successes they have achieved. This argument can also be used in the other direction: unless there are clear roles and responsibilities a manager may be reluctant to commit resources for a project that she or he has no direct control over, but may be expected to explain it in the case of an

---

[41] Paul Thomas, "Accountability Introduction," in *Handbook of Public Administration*, Ed. B. Guy Peters and Jon Pierre (London: Sage Publications, 2003) 549.

[42] Thomas, *Performance Measurement* 2.

unsuccessful outcome. The other reason is that if government wants to use the New Public Management model of increasing responsiveness and decreasing the costs (in time, if not in money) of government, horizontal and cross-jurisdictional work is one method of achieving this goal. Therefore, such projects must be clearly understood, measurable, and responsibilities must be transparent.

This also must be reflected in Ministerial accountability, which includes the move towards personal accountability for bureaucrats but still holds a Minister responsible to Parliament directly for whatever happens within her or his department. The idea of adding the responsibility for complex, high profile horizontal work onto one Minister's portfolio is not likely to be a fair or accurate reflection of that Minister's legitimate responsibilities, as that project likely crosses the jurisdictions of more than one department. In order for horizontal management to be effectively used as a tool for government, accountability frameworks must be re-worked to allow its use.

This does not, however, mean that the traditional vertical accountability frameworks must be thrown out in favour of a not yet established horizontal accountability framework. In fact, in Luc Juillet's work on Federal Councils and Horizontal Governance, interviewees stated that "…the Public Service of Canada should avoid working on the creation of an entirely new accountability framework for horizontal initiatives and focus instead on how the councils' work could best be reconciled with the existing framework of vertical accountability."[43] There is the need to be responsible to partners throughout the horizontal network as well as the need to be responsible to the

[43] Luc Juillet, *The Federal Councils and Horizontal Governance: A Report Prepared for the Regional Federal Councils and Treasury Board Secretariat* (Ottawa: University of Ottawa, 2000) 13.

traditional vertical structures of participant's home organizations. This can result in a great deal of time focused on reporting back, and creating plans to report back, which is a hurdle that must be overcome considering that it may hinder the network's ability to accomplish what it has set out to do by becoming bogged down in housekeeping details. As horizontality may be either a temporary or a permanent measure such details may lessen in time as organizations determine what reporting structures work best for them.

Proposed solutions to deal with the accountability difficulty include requiring each participant within the network to measure their own performance and report the results back through the respective hierarchies; for part of the network to participate in the same exercise and publicly report findings; or for an independent third party to make the necessary assessments and report back to the network and to the vertical structures.[44] Other requirements for collective accountability include a clear definition of roles and responsibilities, demarcation of accountability for different types of action and inaction, known reporting mechanisms, and agreed upon strategies for reporting about outcomes.

Summary

New public management, and horizontal management specifically, are a change from the traditional organization of government and are responses to the fiscal crunches and reduced resources that are a common feature of today's public service. Each requires a fairly dramatic change in how managers think about the organizing of work and the people who do that work, but they offer a more cost-efficient way to provide services to citizens, based on a private-sector approach. In order to implement horizontal management, much work must be done to determine frameworks of accountability,

[44] Mark Sproule-Jones, "Horizontal Management: Implementing Programs Across Interdependent Organizations," *Canadian Public Administration* 43:1 (2000) 104.

leadership and resource allocation; but this extra work brings potential dividends of greater flexibility in service provision, with fewer resources.

Chapter Three: Canada's OCIPEP

> In today's fluid and unpredictable security environment, we need to think differently and respond more creatively. This new environment has highlighted the need for leadership, coordination, and partnerships -- across sectors, across regions, and across borders.
>
> Margaret Purdy, Associate Deputy Minister, OCIPEP (Feb 2001–Apr 2003)[45]

The concepts of critical infrastructure and of critical infrastructure protection have blossomed in the public and bureaucratic spheres. The idea of critical infrastructure protection appears to have been created in order to alleviate fears about a large-scale catastrophe due to on our reliance on technology. Information technology has been one of the main fields on which critical infrastructure protection has focused, in large part due to Y2K fears and the growing dependence on computers for today's economic system.

The interdependence between physical infrastructure systems and the information technology that allows them to operate had been clearly established, with the resulting need to determine ways to protect that which is "critical". This included methods of linking existing research with that which needed further examination, and plans for how better to protect those infrastructures. From computer viruses to hackers corrupting information and countless other situations, computers can be used in ways that they are not intended, by people other than the authorized users. In fact, a focus on information technology and computing has been integral to the ideas and plans of critical infrastructure protection. Critical infrastructure since September 11, 2001 has seen a renewed emphasis on physical infrastructure as well, from more obvious examples such

---

[45] Office of Critical Infrastructure Protection and Emergency Preparedness, September 4, 2004 <http://www.ocipep-bpiepc.gc.ca/critical/nciap/update1_e.asp>

as tunnels to less obvious such as border infrastructure which have become critical in previously unforeseen ways.

It makes sense then that much of critical infrastructure protection is information systems protection; that determining ways to make computers more secure and "hack-proof" is transferable across organizational boundaries, and does not necessarily depend on shared physical infrastructure but rather on shared information infrastructure with transferable protection methods. In order to put critical infrastructure protection into action the varied constituents (from government department to private business owner) must each take care of their own components, which results in improving the security of all. This is due to the complexity of an interdependent system—that if one component fails (and if it's owner had not succeeded in protecting their critical infrastructure), the failure can travel down to others, and can impact even those who may have put into place all the safeguards they can. This is why redundancy in systems is important.

This chapter constitutes a case study examining what Canada has done for the protection of critical infrastructure with the creation of the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP). In preparing a case study about OCIPEP, the framework used to organize the analysis is based on Herman Bakvis' and Luc Juillet's study, *The Horizontal Challenge: Line Departments, Central Agencies and Leadership* (2004). The study examined four cases in which horizontal management was used. Each case is investigated in terms of its catalysts and champions, costs and benefits, tools and resources, the role of central agencies and the challenge of accountability. Adapting this framework for use in this case study allows OCIPEP to be compared to Bakvis and Juillet's four cases. This puts the OCIPEP case into a broader

context and allows for a further test and possible refinement of the theoretical framework used in the CSPS study. Evaluation will also take place with regard to accomplishments, factors contributing to success, and factors impeding success.[46]

The reasoning behind choosing a case study format to analyse OCIPEP was primarily due to OCIPEP's special place within the Government of Canada. This special position situated OCIPEP as the lead agency for critical infrastructure protection and emergency preparedness, within the greater context of the Department of National Defence (DND). The fact that OCIPEP's work was atypical compared to DND's usual responsibilities meant that OCIPEP was able to set their own direction a great extent of the time. The fact that OCIPEP's mandate specifically required horizontal work was also unusual. The lack of lead-up time for OCIPEP to organize itself before becoming operational also makes it a rare case, as the people within the organization were truly developing the organization at the same time as it needed to be operational, which is not the optimal (or even a common) situation. Each of these reasons makes OCIPEP a case worthy of study on its own, but the three taken together demonstrate what a unique case OCIPEP was.

History

The origins of OCIPEP as a specific entity date back to 1996[47] when a preliminary review on the implications for Canada of the information technology

---

[46] Canada, *Guide to Building Dialogues on Horizontality: Discussion Paper.* Environment Canada and the Synthesis Workshop on Horizontality for the Canadian Centre for Management Development's Action-Roundtable on the Management of Horizontal Issues, November 8, 2000.

[47] Through the establishment of Emergency Preparedness Canada, can be traced back to 1948.

revolution was produced, due to concerns about the threat of information warfare. This review stated that the Government of Canada needed to update methods of identifying and protecting Canada's important facilities, due to the effects of the change to a computer-based infrastructure had upon the significance of particular facilities.[48]

By 1998 the decision was made to look instead to year 2000 preparation, and to postpone an in-depth examination of the identification and protection project. Y2K demonstrated the interdependence between infrastructures, considering the various redundancy plans and back-up measures for not just computers, but most systems upon which Canadians depend (such as water treatment, medical equipment, and heating, to name a few). Emergency Preparedness Canada and other offices and departments compiled a detailed catalogue of essential services. This information was the beginning of Canada's critical infrastructure protection planning post Y2K.[49]

In December 2000 the Government of Canada initiated a one-year task force on critical infrastructure with the objective of advising as to any ongoing role that the Government of Canada should take with regard to critical infrastructure protection. At this point a Y2K-based definition named critical infrastructure as "those things that would have a serious impact on health, safety, security and economic well-being of Canadians."[50] This ultimately is a "modern version of the vital points program of the Cold War years."[51/52]

---

[48] James Harlick, *Standing Senate Committee on Defence and Security: Evidence* (Ottawa, 19 July 2001), online, Parliamentary Search Engine, Internet, 20 April 2004.

[49] Jennifer Ditchburn, "Business, Government Reap Rewards of Y2K Planning in Wake of Sept. 11." *Canadian Press Newswire*. October 10, 2001.

[50] Harlick 19 July 2001.

Beginnings

OCIPEP was in existence from February 5, 2001 until December 12, 2003. During that time it was the Government of Canada's lead agency responsible for assuring critical infrastructure and maintaining emergency preparedness, which involved working on a partnership basis with other federal departments, provincial and territorial governments, and private owners and operators of critical infrastructure.

OCIPEP was behind from the very beginning. Normally when departments want to establish a program they request special funds, and to do so they must produce a memorandum to cabinet. A memorandum to cabinet (MC) is a document that travels through the requesting department's Minister to a committee of cabinet at which stage it becomes a committee report, which then goes before the whole cabinet. The cabinet may choose to approve it with a record of decision, may reject it, or may require modifications). The Privy Council Office may contribute to the MC through the drafting of both committee reports and records of decision. The record of decision is sent back to the presenting Minister, who must submit it to Treasury Board with a request for approval for human and financial resources.[53] When a MC is approved it is normally not announced right away, rather it is kept quite confidential, while the department is given

---

[51] Standing Senate Committee on National Finance, *Evidence* (Ottawa, 23 October 2001), online, Parliamentary Search Engine, Internet, 21 April 2004.

[52] The vital points program was for identification and security assessment of what is now called critical infrastructure, and focused on security threats only.

[53] Kenneth Kernaghan and David Siegel, *Public Administration in Canada, 3rd Edition* (Scarborough: Nelson Canada, 1995) 388-390.

time (up to six months) to set up the organization. That way, when that announcement is made the organization is already up and ready for business.[54]

In the situation of OCIPEP, it was a rare case where the machinery decision preceded the policy framework decision.[55] The plan had been to present the MC in November of 2000, however due to the election it was postponed first to January of 2001, then again until February. In February 2001, Prime Minister Jean Chrétien went to Washington to meet with President George W. Bush, and Chrétien announced to the President that Canada had a new organization called the Office of Critical Infrastructure Protection and Emergency Preparedness. This was prior to the proposal being approved by cabinet (it was approved later). With the announcement it was expected that the organization would soon be up and running. Instead OCIPEP was created that same week from people who were within the former Emergency Preparedness Canada (EPC) and from the Critical Infrastructure Protection Task Force (CIPTF), and placed within the Department of National Defence, which was where EPC had been located. Senior Management was not given any warning and Government expected OCIPEP to be functional that same day.[56]

The Mandate

From the beginning, OCIPEP was given a "two-pronged mandate":

> -to provide national leadership of a new, modern and comprehensive approach to protecting Canada's critical infrastructure-the key physical

[54] Confidential interview, December 1, 2004.

[55] Confidential interview, December 15, 2004.

[56] Confidential interview, December 1, 2004.

> and cyber components of the energy and utilities, communications, services, transportation, safety and government sectors; and
>
> -to be the government's primary agency for ensuring national civil emergency preparedness-for all types of emergencies.[57]

This two-pronged mandate was believed to be unique in the world, and attracted considerable attention. Others watched to see if Canada's experiment would succeed.

With such ambitious objectives, OCIPEP purported to fulfil this broad mandate through partnering with other government departments, the private sector, and even other countries in order to determine the best support strategies for critical infrastructure protection. Of equal importance was improving lines of communication through the many people and organizations that had an interest in critical infrastructure and in the "core elements of securing critical infrastructure - protection, detection, response and recovery."[58] This was attempted by issuing advisories about new computer viruses, hosting workshops to bring together representatives from different sectors, and administrating financial programs that share costs between the federal and provincial or municipal governments in order to develop and improve existing capabilities for critical infrastructure protection and emergency preparedness.

OCIPEP began with an assumption that cyber-threats would be a driving force with which to work. This focus should have meant that the Government of Canada would end up with strong capabilities in the cyber-threat area, but the mandate was not specific

---

[57] Office of Critical Infrastructure Protection and Emergency Preparedness, Home page, Internet 17 Jan. 2003.

[58] Margaret Purdy, Associate Deputy Minister, National Defence, *Speech: "Critical Infrastructure Protection and Public Safety" Strategies for Public Transformation 2002 Conference: Terrorism and Technology: Prevention, Protection and Pursuit* (Whistler, B.C. 29 Apr. 2002) Internet, 9 Oct. 2002.

enough to provide the focus needed. Many other organizations had cyber-mandates already—Treasury Board Secretariat was responsible for computer security, information technology principles, maintenance; the RCMP were responsible for cyber-crime; the Communications Security Establishment was responsible for the maintenance of government signal security. Another factor that contributed to this fragmentation of responsibility was the location of OCIPEP within the Department of National Defence, which was not particularly well-linked to the cyber-mandate, and thus was unable to command the attention required to catch the notice of departments and agencies. OCIPEP could not contribute through research, as that ground was covered by Computer Emergency Response Teams all over the world, largely supported by the private sector and academic interests. By 2003, cyber-threats had been reduced in priority.

OCIPEP was also to provide guidance through “best practices” or “smart practices” to private industry, and provincial and municipal governments. This coordination is necessary due to increasing technological integration between each of these players. For the government to be useful in assuring its own critical infrastructure and helping to assure that of others, clarity is necessary. The Government of Canada had its own Critical Infrastructure Protection Plan, while the National Critical Infrastructure Assurance Plan (one of OCIPEP’s initiatives) was designed to help other organizations to establish best practices and better assure their critical infrastructure.

OCIPEP used an “all-hazards approach” to creating plans for critical infrastructure protection and emergency preparedness. Thus regardless of the origin of the threat, OCIPEP was involved with plans for mitigation, preparedness, response and recovery. The outcomes of damage to infrastructure must be dealt with in similar ways,

regardless of what initially caused the damage. This meant that threats arising from natural, deliberate or accidental instances were all included as events to prepare for.

OCIPEP hit the ground running. The agency faced two considerable challenges: to build upon the accomplishments of the former EPC (and lessons learned in the CIPTF) and to recruit, train and retain the required staff. Not surprisingly, it was a challenge to staff OCIPEP as there was neither time nor resources to carefully examine what the needs were and what skill sets were required. OCIPEP expanded from the approximately 75 full-time equivalent (FTE) staff positions in the former EPC to around 300 FTE positions by the time that OCIPEP was dissolved. In addition to the existing EPC staff, many people were brought in from the CIPTF or as seconded, temporary, and casual employees. In some instances, new employees were brought in with promises that they would fill positions when the human resource situation stabilized, creating concern about their employment future.[59]

At that same time, other government departments were also looking for people to develop their own critical infrastructure protection. This led to a shortage of people with the required knowledge and skill sets, which also contributed to serious difficulties in staffing OCIPEP. Corporate services (such as human resources, finance, information management and information technology[60]) were not staffed appropriately or with the right people. This situation lasted the entire time that OCIPEP was in existence.[61] Added

[59] Confidential interview, November 16, 2004.

[60] Confidential interview, December 15, 2004.

[61] Confidential interview, December 1, 2004.

to this was the fact that OCIPEP existed between four different locations in Ottawa, which led to feelings of isolation, incoherence and instability within the organization.

A Unique Position

OCIPEP was uniquely positioned in Canada to work with circumstances previously unidentified and un-owned within the Government of Canada. The matter of critical infrastructure protection developed through EPC, the fears around the Y2K rollover, and the CIPTF. OCIPEP was created because, until that time no existing government department had the responsibility of coordinating critical infrastructure protection throughout the federal government. Other departments had parts of the responsibility, for example Industry Canada had the telecom portion, but there was no critical infrastructure protection framework within which that sector could work that covered more than just their specific organization(s). The task force made people realize that within the Government of Canada there was no one particular organization responsible for critical infrastructure protection, yet the task force could not create a policy framework and pass it on to a relevant department because no department was named as responsible. Furthermore, no department would volunteer for the responsibility because it was not known whether or not additional resources would be attached to that responsibility.[62]

All of these factors; from OCIPEP's quick start, staffing challenges and physical discontinuity, were added to the fact that it was working to organize itself and at the same

[62] Confidential telephone interview, December 15, 2004.

time trying to produce on a wide range of fronts.[63] The phrase offered by an interviewee was that of "building the airplane while flying it."[64]

An organization with the title of Office of Critical Infrastructure Preparedness and Emergency Preparedness suggests a primary mandate to protect critical infrastructure. However, it was quickly discovered that the Government of Canada owned less than fifteen per cent of Canada's critical infrastructure. This meant that while OCIPEP's mandate was to protect critical infrastructure, it had no authority to compel other departments or organizations to improve their plans and methods of protecting critical infrastructure. OCIPEP was in a position strictly to advise, to persuade, to facilitate, and to coordinate.[65] This meant that, in order to fulfil their mandate, OCIPEP required voluntary partnerships with other departments, provinces and municipalities, and private industries.

The rhetoric of partnerships and joint-enterprises is found throughout government. In this case, however, while some departments saw the benefits of working with OCIPEP, others departments or organizations (such as the Solicitor General's office, the RCMP and CSIS) adopted a zero-sum game perspective insisting that any policy or administrative leadership shown by OCIPEP was a loss to their authority and influence. These rivalries were compounded by the fact that OCIPEP was located in the Department of National Defence, not in the Solicitor General's office, which had implications for the

---

[63] Confidential telephone interview, November 16, 2004.

[64] Confidential telephone interview, December 15, 2004.

[65] Confidential telephone interview, November 16, 2004.

security of information and what would be shared with whom.[66] There was, therefore, a reluctance to share information and to collaborate in a way to allow OCIPEP to fulfil its mandate. This "vertical cultural context" within government contributed to difficulties that OCIPEP had to overcome in order to work towards its mandate, with varying success. This is now less true due to the relocation of each of the previously listed organizations within the new department of Public Safety and Emergency Preparedness Canada (PSEPC).[67]

Legislation

OCIPEP never had a statutory base. The legislation that guided OCIPEP was the Emergency Preparedness Act, in which OCIPEP was not mentioned because the organization was created after the act's last revision in 1988. This act also instructs all federal ministers to develop emergency response plans in their areas of accountability. In 1995 the government approved a Federal Policy for Emergencies, which outlined the procedure for selecting a lead minister in the case of emergency, and outlined the responsibilities for individual departments in emergency situations. After a lead minister has been determined, OCIPEP was chiefly to coordinate consequence management by providing support and linking departments, both federally and provincially.[68] The process

---

[66] An example of this situation occurred after September 11, 2001 when the proposed legislation Bill C-36 (the omnibus legislation) included an amended Emergency Preparedness Act, yet that was blocked by the Office of the Solicitor General as there was no agreement on division of powers.

[67] Confidential telephone interview, December 15, 2004.

[68] James Harlick, *Standing Senate Committee on Social Affairs, Science and Technology, Issue 20 Evidenc*e (Ottawa, 17 September 2003) online, Parliamentary Search Engine, Internet, 20 April 2004.

through which this was undertaken was by issuing regular national situation reports that summarized relevant information. Such reports would be sent to all federal departments, to the provinces via the regional OCIPEP offices, and possibly to private sector entities.[69] OCIPEP was also the designated lead for certain types of emergency, notably those which required invocation of the National Support Plan (NSP). The NSP covers federal assistance for catastrophic disaster such as a massive earthquake in BC.

The primary activities that OCIPEP performed were information sharing about threats and vulnerabilities, issuing of timely advisories and alerts, the compilation and dissemination of best security practices for information technology, promotion of common security solutions, and coordination of response to cyber incidents.[70] Specific preparation for emergency situations is the responsibility of provincial and municipal governments, and OCIPEP was in place to:

> …enhance the capacity of individuals, communities, business and governments…to effectively manage risks to their physical and cyber environments…[B]y acting as a facilitator, a coordinator, a leader and a catalyst, or by filling gaps in the overall risk management environment in Canada.[71]

OCIPEP's influence was further limited by its budget of $95 million[72] (which will be discussed further in this chapter) and its small staff of roughly 300 FTE in a large

---

[69] Standing Senate Committee on National Security and Defence, *Evidence* (Ottawa, 20 October 2003), online, Parliamentary Search Engine, Internet. 20 April 2004.

[70] James Harlick, *Standing Senate Committee on Defence and Security, Evidence* (Ottawa, 10 July 2001) online, Parliamentary Search Engine, Internet, 20 April 2004.

[71] Standing Senate Committee on National Finance, 23 October 2001.

[72] $95 million was OCIPEP's budget in 2001. Office of the Auditor General of Canada. *Report of the Auditor General of Canada: National Security in Canada—The 2001 Anti-Terrorism Initiative -- Air Transportation Security, Marine Security and Emergency Preparedness*. April 2005. Chapter 2: 35.

department of 20 000 employees. OCIPEP was a low priority for the Minister of National Defence, as had been the same for the former EPC (within DND, EPC did not have a high profile). This was partly due to the fact that the Minister of National Defence had significantly more demanding priorities with respect to the Armed Forces and the department, so OCIPEP became a tertiary responsibility. The issues lacked significant political attention, and the fact that the Minister had no provincial or territorial counterparts to speak to helped to keep OCIPEP as a low priority.[73/74]

What Constitutes Critical Infrastructure?

Determining what infrastructures can be considered to be "critical" is in no way consistent between countries, or even provinces. Initially, Canada's definition of critical infrastructure was:

> Physical and IT facilities, networks and assets whose disruption or destruction would have a serious impact on: The health, safety, security, economic well-being of Canadians; or the effective functioning of governments in Canada. **This includes energy and utilities, communications, services such as financial and food services, transportation, safety (including nuclear safety, search and rescue and emergency services), and government and the government-wide critical systems** like pensions, Employment insurance.[75]

While this was the definition used from OCIPEP's conception until 2003, it was amended after consultations with stakeholders revealed that certain infrastructures had been left

---

[73] Confidential telephone interview, November 16, 2004.

[74] Confidential telephone interview, November 24, 2004.

[75] Office for Critical Infrastructure Protection and Emergency Preparedness. *Slides-Presentation to DSAB Asymmetric Threats Study Team*. Ottawa: January 15, 2002.

out,[76] and subsequently added water, manufacturing, and health care, and changed categories so that finance, food, and government became their own sections, ultimately creating ten distinct sectors.[77] In order to identify and rank critical assets, the following criteria had been developed:

1. characterize or standardize asset: due to the size of a potential list of assets, the need to standardize what exactly is critical and what is not is helpful. This could include assessment by a team to determine what mechanical part in a specific system (such as a gauge in water treatment) is at risk of failing, and might have no backup. That asset would then be considered critical infrastructure. Such assets would need to be ranked at consistent levels of risk.
2. establish criticality: while it is relatively easy to determine what is a critical asset, it is more difficult to determine how a particular asset compares to another asset, or how critical one particular item is. While there are many ways of ranking, the outcome of failure or loss of the asset will be used to determine how critical each asset is, and use low, medium and high to categorize assets.
3. assess impact of loss of asset: impact factors are the criteria used to prioritize critical assets. The following impact factors are used to determine the impact of the loss of an asset:
    1. concentration of people and assets
    2. economic impact or direct cost to the enterprise
    3. critical infrastructure sector
    4. interdependency or cross-sectional impact
    5. service delivery impact to the general economy
    6. public confidence
4. assess consequence of loss of asset: determine what consequences might occur if the asset was lost, using the impact factors.
5. use a rule-set to rank assets: assessing whether the loss of the asset would be considered low, medium or high when all the above is considered. This ideally will be as objective as possible, which is generally attempted through assigning

---

[76] Office of Critical Infrastructure Protection and Emergency Preparedness, National Critical Infrastructure Assurance Program, *An Assessment of Canada's National Critical Infrastructure Sectors (July 2003)*
25 April 2004, <www.ocipep-bpeipc.gc.ca/critical/nciap/nci_sector1_e.asp>

[77] Office of Critical Infrastructure Protection and Emergency Preparedness, *Fact Sheets: National Critical Infrastructure Assurance Program*. 25 April 2004, <www.ocipep-bpiepc.gc.ca/info_pro/fact_sheets/general/CIP_NCIAP_e.asp>

numeric values to standard criteria, and culminating with a number ranking the priority of the asset.[78]

Canada's Ten Sectors

In order to grasp the magnitude of the challenges for coordination, one must have an idea as to the magnitude of what OCIPEP was working with. These descriptions of the ten sectors that OCIPEP used to categorize Canada's critical infrastructure are not meant to be exhaustive, but rather to illustrate both the benefits and challenges inherent in such a task.

Energy and Utilities

The provision of energy and other utilities such as natural gas, oil production and transmission systems, and electricity are basic necessities to function in the world today. Many of the other categories of critical infrastructure require energy of some sort to run, which means that if energy and/or utilities are threatened or damaged there is a likelihood of failure of other critical infrastructures.

One of the most obvious examples of the interdependence of most critical infrastructure with electrical energy comes from the August 2003 blackout in Southern Ontario and North-Eastern United States. The failure of the power-grid in Ohio and the resulting cascade of power outages that reduced or eliminated power for a number of days effectively shut down the entire effected area, with people unable to access their high-rise apartment buildings; public transport unable to operate; refrigerators unable to chill food. Laying blame was a constant past-time, perhaps not from the official

---

[78] Public Safety and Emergency Preparedness Canada. *National Critical Infrastructure Assurance Program Selection Criteria to Identify and Rank Critical Infrastructure Assets,* 20 January 2004.
<www. ocipep-bpiepc.gc.ca/critical/nciap/nci_criteria_e.asp> (May 4, 2005).

spokespeople, but from the news media and citizens, and along with the inconvenience a great loss of public confidence occurred. This power outage will be discussed more in depth with regard to weaknesses later on in this chapter.

Communications and Information Technology

Telecommunications, broadcasting systems, software, hardware and networks such as the internet are critical when one considers that in an emergency each of these allow information to be shared. Emergency response depends on reliable, accurate communications between responders, from the government, to local authorities, to emergency response units, to hospitals, to citizens, right down the line.

A primary method of communications used today continues to be telecommunications, including everything from landlines to cellular phones, from fax machines to computers connected through modems. Regulating such a large realm is not easy and is made more difficult when one considers the number of private corporations that are in business providing these services. It would be possible for a terrorist organization to knock out communications towers as their first strike because the resulting confusion and panic would likely be absolutely devastating, just like it would be if a natural disaster knocked out such infrastructure.

Health Care

Health care and the ability to offer it to citizens is critical. Health care includes hospitals (the buildings themselves, and those people who staff them, almost entirely under the province's ownership and regulation, local marketplace), blood supply facilities, laboratories and pharmaceuticals (federal regulation, global marketplace).

Finance

Financial services are of great importance as they provide the means for people to obtain the goods and services essential to life. Financial services do not consist simply of currency itself, but all paperless forms of monetary exchange (including debit and credit transactions), and are dependent upon their issuing institutions' ability to use their networks which are connected not only nation-wide, but also worldwide. Banks, securities and investments are all named as examples of critical infrastructure in this category. Banking machines are the most obvious example at the consumer level (dependent on power, information technology, phone lines, transport and the buildings and businesses in which they are situated). There is another less visible dimension for the financial sector: international confidence in our ability to identify terrorist financing. Another key symbol of sovereignty are financial markets. Maintaining a sense of public confidence in finance is critical for the government to be supported by citizens.

In the original definition of critical infrastructure, services as diverse as food, emergency and financial services were lumped together in one category. The administration of such a category would be challenging at best, completely disjointed at worst, and so the actual administration in a disaster is left to the department in charge of each component. In the subsequent definition of critical infrastructure these were separated into their own sectors, still not linked to specific departments. This means that while water is its own sector, all departments that might have to do with water will still be responsible for maintaining their critical water infrastructure. The newer, more elaborate sectors may have increased the ability to network and work across jurisdictions for each particular issue because it might have been easier to spot allies and potential

partners. Increased partnerships would increase redundancy in systems protection, and would help to reduce gaps that might otherwise be left unfilled.

Food

The food sector encompasses all aspects of Canada's food supplies, from food safety and distribution to the industries of agriculture, food production and processing. Canadians' reliance on food services is almost complete, as only a minute number of people can support themselves and their families on what they grow.

Along with food itself is the requirement that it must be transported to where it is needed and it must be stored safely during this process from the producer to the consumer. While food is one of the few absolute necessities for life, it is one of the more vulnerable critical infrastructures when we consider that the population of Canada largely exists in cities, and depends on the supportive critical infrastructures to receive food, such as transportation, energy, water, finance, and emergency services if necessary.

Water

Water was entirely left out of the original definition of critical infrastructure--there was no specific mention of it even within any of the sectors. It is an important addition due to its necessity for all life, and potential for tragedy when damaged. This was demonstrated during the Walkerton Tragedy, where a small community in Ontario was affected by an e-coli contaminated water supply. Seven citizens died and 2 300 became ill (with possibilities of lasting health concerns).[79] The Walkerton contamination was due to human error, not malicious intent, yet Canada's water supply or the physical

---

[79] Dennis R. O'Connor, *Part One, A Summary. Report of the Walkerton Inquiry: the Events of May 2000 and Related Issues* (Toronto: Ontario Ministry of the Attorney General, 2000).

structures that the supply depends upon could be a target for terrorist attacks or natural disaster.[80] Wastewater management is also part of this sector. In many cases, water management and treatment is tested and regulated by computer-based operating systems and networks, again, the interdependence of sectors is demonstrated.

Part of the argument for the inclusion of water as a sector unto itself is that when OCIPEP compared their definition of critical infrastructure with those definitions from seven other countries,[81] those countries choose to include water as a specific critical infrastructure. It qualifies also when the potential devastation caused by an attack on water is considered.

Transportation

Each form of transportation (air, rail, marine and surface) is included as critical infrastructure. This does not mean, however, that every road and bridge in Canada is considered to be critical: each must be categorized according to OCIPEP's criteria.[82] Transport Canada is the lead agency for this sector, and they cooperate with Canada Customs with regard to border security and safety of items that enter Canada.

---

[80] Office of Critical Infrastructure Protection and Emergency Preparedness, National Critical Infrastructure Assurance Program, *An Assessment of Canada's National Critical Infrastructure Sectors (July 2003)* <www.ocipep-bpeipc.gc.ca/critical/nciap/nci_sector2_e.asp> (April 25, 2004)

[81] The United Kingdom, Australia, the United States, Germany, Sweden, Norway, the Netherlands, Switzerland.

[82] Office of Critical Infrastructure and Emergency Preparedness, National Critical Infrastructure Assurance Program, *An Assessment of Canada's National Critical Infrastructure Sectors* July 2003, <www.ocipep-bpeipc.gc.ca/critical/nciap/nci_sector1_e.asp> (April 25, 2004)

Safety

Public safety is a large field, covering law enforcement mechanisms (such as Police, the Canadian Forces), emergency services, search and rescue, and the safety of devices and substances that are hazardous in themselves, such as chemical, biological, radiological and nuclear safety, and finally dams.

Government

Government systems are what control each of the responses to critical infrastructure damage. There are a wide variety of services that fall under this sector, often these may fall under other sectors as well, and include the operation of government departments such as government services and facilities, government financial services such as the distribution of pensions, Employment Insurance, disaster relief, transfer payments, information networks, assets and key national sites and monuments.

The addition of key national sites and monuments is due to the possibility that if such infrastructure was damaged or destroyed, it would have an effect upon the morale of the Canadian population. The ability to protect certain symbols from harm, e.g. Parliament Hill, is also a test of the government's ability to retain public confidence in an emergency, which is a very practical, rather than merely symbolic matter: for example, such sites of historical significance as provincial and national archives, and national/provincial/territorial galleries and museums, the records and artefacts inside which could not be replaced if destroyed, and monuments such as war memorials that, while they may be only physical structures to some, to others have both personal and societal significance.

The greater reliance on computers in the recent past extends to the government as well. Keeping records electronically make filing quicker, information retrieval faster, and means that when those files are tampered with, lost, or “hacked”, receiving the government services to which one is entitled can be much more difficult.

This is one category that demonstrates the flexibility of the definition of “critical”, and brings to mind the question of whether it is possible for some infrastructures to be considered more critical than others. In OCIPEP’s mandate and many definitions, the stakeholders are the citizens of Canada specifically. In an emergency, of course, the requirement of protecting the National Art Gallery is arguably less “critical” than safe water to drink and shelter. The acknowledgement that symbols are important is a nod to the notion of public confidence and an acknowledgement that it affects morale. Citizens look to particular infrastructures to symbolize them as a people, and should such symbols be damaged or destroyed the resulting loss of confidence might be larger than otherwise would be expected when one considers that a symbol is not necessary to maintain life.

Manufacturing

The final sector is that of manufacturing, for example the defence industrial base and chemical industry. Canada’s manufacturing processes have increasingly competed with those of other countries and our chemical resources (such as petro-chemicals) are a source of economic wealth and prosperity for many regions of the country. Such manufacturing and chemical resources are also a source of parts, fuel, and other essential components for other critical infrastructure sectors. Canada’s defence industrial base comprises the physical aspect of Canada’s defence abilities. Moreover, Canada exports defence materials to the US, which is undoubtedly Canada’s leading partner in North

American security. Integrating and updating the components of this sector allow for a better integrated defence platform across the two countries, and increase security.[83]

Additional Vulnerabilities

Canada is also vulnerable to critical infrastructure disruptions as Canada's population (and therefore its infrastructure) has moved from being located primarily in large and widely spaced rural areas to the increasingly smaller and more concentrated areas of cities and their surroundings.[84] This means that service disruptions affecting a physically small area can affect large numbers of people, for example the incapacitation of just one water treatment plan could put thousands, if not millions, of people at risk. Cities are often at risk due to multiple hazards: threats of terrorism, natural disasters and the ever-possible threat of human error can all threaten a city at any given time. Interconnectivity in cities becomes so complex that it is difficult to model or predict accurately, for example, New York City in 2001 experienced unforeseen events after the terrorist attacks on the World Trade Centre. Therefore flexibility in all-hazards planning is especially critical.

---

[83] Office of Critical Infrastructure Protection and Emergency Preparedness, *National Critical Infrastructure Assurance Program: An Assessment of Canada's National Critical Infrastructure Sectors July 2003* <www.ocipep-bpiepc.gc.ca/critical/nciap/nci_sector2_e.asp#sector> (May 4, 2005)

[84] The 2001 Census reveals that the four large urban regions of Ontario's Golden Horseshoe, Montreal and adjacent region, British Columbia's lower mainland and South Vancouver Island, and Alberta's Calgary-Edmonton Corridor when combined contain 15.3 million Canadians, or 51 per cent of the country's population (compared to only 41 per cent in those regions in the 1971 Census).
2001 Canadian Census: A Profile of the Canadian Population.
<http://geodepot.statcan.ca/diss/highlights/Page9/Page9_e.cfm>

The aging process is another factor that threatens the critical infrastructure in Canada as older infrastructure requires an increased amount of upkeep to avoid potential failures, due either to natural disintegration or sabotage. The need to replace and upgrade critical infrastructure must be balanced with the need to keep expenditures down and balance budgets. Critical infrastructure protection is generally focused on emergencies and unexpected critical infrastructure failure but it is important to realize that systems and equipment do require upkeep and replacement on an ongoing basis. This issue is compounded by the fact that over 85 per cent of critical infrastructure is owned by the private sector[85], which may or may not have contingency plans in place, and yet citizens and companies expect the government to keep systems running in the case of emergencies. This ownership challenge is the crux of critical infrastructure protection in Canada, that coordination and planning is neither uniform nor entirely enforceable from sector to sector, business to business.

Climate change appears increasingly to be a reality which results in more frequent and severe extreme-weather events. This threatens critical infrastructures directly and indirectly—a severe rainstorm and accompanying flash flood may wash out an important bridge, and it also might disable electrical stations. Or another example, in the case of hurricane Juan in September 2003, weather forced the brief closure of the national hurricane centre in Halifax, arguably a critical infrastructure failure[86]. As previously stated, the increased reliance on advanced technologies means that should computers, the

---

[85] Canada, "National Critical Infrastructure Protection Program," *Emergency Preparedness Digest* January – March 2002: 4.

[86] *Emergency Measures Organization Debriefing for Hurricane Juan*, (Dartmouth NS, 29 October 2003) 62.

networks they are linked to, or their sources of electricity be damaged, other services people rely on might also be withdrawn.[87]

Canada is also vulnerable to critical infrastructure failures in the US or their effects owing to the inherent linkage of the economy and many common systems. Even purely domestic incidents can affect foreign perceptions of our critical infrastructure preparedness abilities, and can reduce confidence.

The all-hazards approach does not mean that a simple, "one size fits all" plan is helpful when one considers the variety of systems, objects, people, information and services that constitute critical infrastructure. The departments responsible for each component of critical infrastructure are ultimately in charge of each component, and their ability to plan for emergencies and to implement disaster mitigation measures may determine to what extent OCIPEP provides guidance in that particular sector.

During an Emergency

In the case of an emergency, the Minister of Public Safety and Emergency Preparedness Canada takes a lead role to assist affected departments. The emergency itself determines which department leads the response, but PSEPC is there to help coordinate information from many different locations and organizations into a comprehensive whole. Some emergency situations are pre-planned, for example, the National Counter-Terrorism Plan which clearly identifies roles and responses. If the emergency does not fall within a pre-established plan then the response is made up at that time. Many organizations have skills to help in a number of situations, like the Canadian Forces that may be able to assist in a number of ways. The basics are worked out at the

[87] Harlick 19 July 2001.

local level. There are also a number of emergency committees that can meet within a very short timeframe if necessary.

Regional OCIPEP

In addition to the national OCIPEP based out of Ottawa, there were regional satellite offices. Regional offices supported the province financially and provided coordination between Ottawa and the province. Should the province ask for assistance, these offices were the link between the province and the government of Canada. They also administered the Disaster Financial Assistance and Joint Emergency Preparedness Programs.

At the simplest level, the physical side of critical infrastructure and emergency preparedness was dealt with by the regional branches, while the information technology threats were dealt with by the headquarters in Ottawa. Creating partnerships with the private corporations that own critical infrastructure was a responsibility of both the satellite branches and of headquarters in Ottawa. Partnership on the national scale often involves national organizations. The regional organizations primarily dealt with emergency preparedness, mitigation, and response. Indeed, most response in Canada is handled at the provincial or municipal level.

Another part of the regional branch's role was to encourage business to do Business Continuity Planning, to determine what businesses must do in order to maintain their operations during and after an emergency, or to resume operations if they were disrupted (what they must do within one hour, within two hours, within one day and so on). Such continuity planning is a core government function in planning for critical

infrastructure failure. A self-help guide for businesses instructed how to go about creating a business continuity plan, which was available both on-line and in hard copy[88].

Key Events

During its existence, OCIPEP had to deal with a number of events that dramatically raised awareness of critical infrastructure protection and emergency preparedness issues. The actions taken by OCIPEP were sometimes criticized harshly, perhaps undeservedly, as many people did not understand its nature as an organization; that it was there to assist other federal departments and external organizations to respond to threats, rather than to provide infrastructure protection on its own. From the events of September 11, 2001 to SARS, BSE, West Nile, the August 2003 blackout in Ontario and the US; each of these events had some direct relation to OCIPEP. In particular, the response to the 2003 blackout was negative with regards to the Government of Canada and OCIPEP in particular, discussed in depth later in this chapter.

OCIPEP and Jurisdiction

> The challenge is to coordinate three orders of government – the federal order that funds (and plans); the provincial/territorial that administers (and plans); and the municipal order that actually responds. A lot of things have to go right if responders across the country are to be properly outfitted and trained to respond effectively to any number of potential disasters.[89]

The concept of responsibility for critical infrastructure protection became murky due to issues of jurisdiction, as OCIPEP was called the lead agency but was not

---

[88] Canada, Office of Critical Infrastructure Protection and Emergency Preparedness, *Self-Help Advice for Businesses and Institutions: A Guide to Business Continuity Planning* (Ottawa: Minister of Public Works and Government Services) <http://www.ocipep-bpiepc.gc.ca/info_pro/self_help_ad/general/busi_cont_e.asp> (15 February 2005)

[89] Standing Senate Committee on National Security and Defence, *Canada's Fragile Front Lines*, 48.

specifically responsible for any critical infrastructure itself, and did not have any authority to require departments to take action on its recommendations. In other words, rather than real power, OCIPEP had to rely on influencing others to take action. It was there to provide information and to encourage the use of that information, and to manage financial resources such as the Joint Emergency Preparedness Plan (JEPP) and Disaster Financial Assistance (DFAA).

Each government department is responsible for the actual planning, protection, and maintenance of the critical infrastructure that falls within its mandate. Thus many departments have specific structures in place to work with critical infrastructure protection, specifically to prevent and manage emergencies should they arise. Departments are responsible for the upkeep of specific critical infrastructure and for protection plans, the creation of which is legislated under the Emergencies Act. This act states that the departments in question must be able to respond in four types of emergencies: public welfare emergencies (for example severe natural disasters like floods, earthquakes, ice storms), public order emergencies (that threaten the security of Canada), international emergencies (acts of intimidation or use of force against Canada or its allies), and war.[90] The *Emergencies Act* is the modern *War Measures Act*, and has never been invoked. There exists also the *Emergency Preparedness Act,* which requires departments to conduct emergency planning.

Summing Up: Criteria to Evaluate OCIPEP's Performance

In order to discuss which goals were successfully accomplished it is necessary to establish which determinants of success can be measured: what constitutes success, and

[90] From the emergencies act.

what constitutes failure. Ideally this should be undertaken as a cost-benefit analysis, although it is a retrospective one, due to the difficulty in obtaining objective numbers or measurements to compare the organization's mandate and mission. In short, when the mandate was to improve the safety of Canadians by providing national leadership to protect Canada's critical infrastructure and to be the government's primary agency for ensuring national civil emergency preparedness,[91] it was difficult to quantify to what extent the country was impacted by the work of this organization. Of course it is extremely difficult to measure precisely what caused a particular outcome, as it is impossible to control for all variables. When the aim is to prevent or reduce an undesirable outcome, in this case to reduce threats to critical infrastructure and to mitigate problems should they arise, a measure of success is primarily based upon the opinions of those closely allied to the project. In this case the opinions of the people who worked for OCIPEP during the organization's lifespan, because it is difficult to objectively measure processes or outcomes that do not occur.

Instead the processes and outcomes that have occurred, such as meetings attended, stakeholder consultations held, and information distribution, can be measured. Some of the information products are possible to quantify when the distribution statistics are looked at, though they can also be deceiving: the fact that an e-mail bulletin is sent out can not be assumed to also mean that the information it contained was read and acted upon. This paper relies on the perceptions of success and failure by people who were employed within OCIPEP, which are their impressions of outcomes. While this is an imperfect measure, it is preferable to relying solely on measuring outputs for the main

---

[91] Office of Critical Infrastructure Protection and Emergency Preparedness, *Home page*, Internet <www.ocipep-bpiepc.gc.ca> (17 January 2003).

reason that OCIPEP was in existence for such a short time (just under three years) that data collection relying on quantifiable (output) data could be misleading and result in the impression that less (or more) was done than really was. Considering the short lifespan of this organization it is necessary to depend on the opinions of those who actually worked with these projects as they were familiar with what went well and what was more difficult or unsuccessful. As with many of us, these former OCIPEP employees use output data as part of their impression of how the organization met outcomes.

The Departmental Performance Reports of the Department of National Defence are also used as an internal description of what was accomplished during the time that OCIPEP was an entity. These reports are considered by the writer of this paper to be less helpful than the interviews as they do not include any suggestions for improving how things were done, or any admission that the process that OCIPEP uses was anything but the best process for the situation. While it is somewhat helpful to see what was done in particular fiscal years, the descriptions are suspect due to their entirely positive slant.

Accomplishments

In the short time that OCIPEP was in existence it did successfully accomplish some of its goals, significantly those of building relationships and partnerships with others working on critical infrastructure protection, both within the government and in the private sector. Relationship building takes time. Trust must be developed slowly and can be eroded or lost entirely through specific events. While at the beginning trust-building was somewhat difficult (with challenges that included getting the same people to attend meetings, or getting the “right” people), it had progressed to the degree that at the end of OCIPEP the partnerships were beginning to pay off in the sense that contacts were

established and they could be consulted on particular issues or for projects relatively easily.[92] Even the recognition of critical infrastructure protection as a concept outside the federal government was helped along by OCIPEP raising awareness through presentations, meetings and consulting with constituent groups; along with external events such as September 11, 2001 and the southern Ontario power outage.[93]

Partnerships in the international arena were also successful, as consultations with the United States, the United Kingdom, Sweden, France and Australia took place in order to create partnerships for the protection of national critical infrastructures. These were identified as each recognized the importance of critical infrastructure protection.[94] OCIPEP inherited EPC's international responsibilities, especially within NATO Civil Emergency Planning, and with the support of like-minded nations was successful in bringing critical infrastructure protection to the NATO agenda.[95] There was praise for the cyber partnerships built. These partnerships were of the greatest importance if all were to benefit from early warning. For example, if Australia warns Canada and other partners of a virus attack, this gives Canada and the US a 14-hour warning (if the attack is set to happen at a certain time on a certain day), allowing time to send out warnings and advisories to computer users. The Cyber and International Directorates in particular did a good job exchanging information about cyber threats and building partnerships. There

[92] Confidential telephone interview, December 17, 2004.

[93] Confidential telephone interview, December 15, 2004.

[94] Confidential telephone interview, December 1, 2004.

[95] Confidential telephone interview, November 16, 2004.

was also the sense that OCIPEP was better known internationally than within Canada.[96] The CRBN (Chemical, Radiation, Biological, Nuclear) program of setting international policy has focussed on establishing policy both domestically and internationally (though given the lack of federal policy it is questionable what legitimate contribution Canada could make internationally.[97] Canada's experience in Emergency Planning and critical infrastructure protection is recognized and OCIPEP participation at international conferences on emergency preparedness and critical infrastructure protection was sought after. Sharing of best practices and information in critical infrastructure protection was a tenet of OCIPEP's existence and thanks to this attitude, Canada had been in demand to participate in conferences and other activities to share best practices, and had created a niche for itself in the critical infrastructure protection world.[98]

Costs and Benefits

In case studies of horizontal projects, the cost-benefit analysis often must be done retrospectively as these initiatives are often difficult to measure and do not fit into established measurement tools. A cost-benefit analysis is done to determine if the horizontal initiative was worthwhile and whether or not the anticipated results will be (or were) worth the investment of time and money.

When examining OCIPEP in terms of costs and benefits, it has been helpful to consider the factors contributing to success as the benefits, and the factors impeding success as the costs. This is partly because the data used for this case study, personal

---

[96] Confidential telephone interview, December 1, 2004.

[97] Confidential telephone interview, November 24, 2004.

[98] Confidential telephone interview, November 16, 2004.

interviews, information available from the former OCIPEP and present PSEPC, and a report from the Auditor General of Canada discuss problems and challenges, and initiatives that were more successful, rather than simply looking at costs and benefits, or the pluses and minuses of the program. With OCIPEP, as with many cases that are not just in a book, what may appear initially to be a cost might later be revealed as a benefit due to the learning accomplished in the process, and vice versa. The description will begin with what worked well, the benefits of OCIPEP; and will follow with what did not work as well, the challenges. The second section is undoubtedly longer, however this should not immediately be construed to mean that the costs outweighed the benefits as the length of time that OCIPEP had to work with these issues was short enough (just under three years) that some of the challenges might have been benefits that were simply not given enough time to be realized.

Benefits: Factors Contributing to Success

A significant strength identified was the dedication of OCIPEP employees. There was a strong impression that many employees put in numerous overtime hours when necessary and were on call in case of emergency, all the while dealing with uncertainty about job prospects due to that fact that they were still classified as temporary or seconded employees.[99] "I'm so impressed by the amount of dedication I see in the people working here. I think that has less to do with the organization and more to do with the fact that people really feel that their work is important to Canadians…That is what makes people stick around—the work."[100]

---

[99] Confidential telephone interview, November 16, 2004.

[100] Confidential telephone interview, December 17, 2004.

Another factor that contributed to how seriously the need for critical infrastructure protection was taken was the threat environment that the world found itself in. September 11, 2001 changed the world's perception of what safeguards were needed both to improve the safety of people, and for the protection and organization of critical infrastructure. More diligent border security measures were taken through the Smart Border declaration with the United States on December 12, 2001. The recognition that financial institutions could be shut down due to an attack on one physical location changed the business continuity plans for many organizations, both public and private. Even the need to work on business resumption and continuity plans was a realization that had not been made sufficiently clear prior to 9/11.

This built onto the recognition that Y2K had initially alarmed people, yet after no major catastrophes the need for cyber security had perhaps moved off the primary agenda. An increase in cyber incidents (hacking, viruses) brought attention to the requirement that cyber security was also critical infrastructure and thus needed to be taken seriously and have resources allocated to it.

A further opportunity that was seized upon through the creation of OCIPEP was the recognition of cyber security as important enough to be a main component of the organization. Prior to OCIPEP there was no organization dealing specifically with cyber security in this way--keeping on top of vast amounts of information, putting out advisories and alerts to interested parties, and creating networks of contacts in other countries in order to warn each other and share information to work to reduce cyber threats.[101]

---

[101] Confidential telephone interview, December 15, 2004.

Factors Impeding Success

For an organization like OCIPEP with a broad mandate that includes the prevention of events, and involves reliance upon other organizations, any attempt to define and to measure effectiveness is inherently difficult. This is demonstrated when one considers that the preferred paradigm of accountability for collaborative undertakings is a results-based model. Measuring results resulting from projects purporting to prevent incidents is tricky at best, so instead the measures the organization relied upon were output-based (e.g. the number of computer virus warnings sent out). The fact that a certain number of emails go out warning people of specific computer viruses does not necessarily mean that they would not have been caught by virus prevention software, for example. In Margaret Purdy's speech at a conference in April 2002, she said:

> We [OCIPEP] are not an intelligence-gathering body. We do not enforce laws. We do not regulate the protection of critical infrastructure or enforce emergency management strategies. Instead, we act as a catalyst for action - a coordinating body that can exercise national leadership because we have a national mandate and a transnational perspective. Key to that is developing close working relationships - partnerships - with Canadian and international law enforcement agencies, intelligence services, emergency services, armed forces as well as our provincial and territorial governments.[102]

Measuring an organizations' ability to "catalyse action" is a task that would stump many people, and while close working relationships with the groups mentioned above could certainly be a huge job (hence the need for a federal organization to undertake it), the link to critical infrastructure protection is tenuous. The idea that a national body could exercise national leadership without any specific power is interesting, as voluntary adherence to any guidelines or proposals that OCIPEP makes would likely be undertaken

---

[102] Purdy 3-4.

only if organizations felt that it was in their best interests, and that could be a tough sell when one considers that about 85% of critical infrastructure is owned by the private sector which may not have a vested interest in cooperating with government.

The challenge of managing critical infrastructure plans and disseminating information to all stakeholders create difficulties for those who are implementing OCIPEP. First because of the difficulty of creating legitimacy for a new institution, and through the requirement that the involved departments, organizations and governments take seriously the fact that OCIPEP was now charged with overseeing their implementation of critical infrastructure protection.

Other challenges were as mundane as getting the same person from each department to attend OCIPEP meetings. Those with whom OCIPEP needed to negotiate and organize were members of both the public and private sector who all had different norms, values and motivations, all of which needed to be managed and brought together to produce a consistent security plan and preparations.

Subjects interviewed identified significant factors that were impediments to success. Subjects commented on weak areas that included corporate services (human resources, central finances), a tendency for OCIPEP's divisions not to communicate with each other, incoherent management, power struggles, and the fact that even within government, few people knew what OCIPEP was and why it was important to work with it.[103] Naturally such factors worked collectively, and in isolation might not have a great deal of influence, but when combined the impacts were considerable.

[103] Confidential telephone interview, December 17, 2004.

Most of the respondents stressed repeatedly that the most significant challenge facing OCIPEP arose from the fact that 85% of Canada's critical infrastructure was (and continues to be) owned and operated by others than the federal government, either the private sector or the provinces and municipalities. This has resulted in difficulties around bringing together involved parties to discuss critical infrastructure due both to a sense that the Government of Canada did not have much to add to critical infrastructure protection, and that the Government would not have been able to protect information that private business passed along. When it came to working with the provinces/territories and municipalities the difficulty was added of trying to protect infrastructure on a very limited budget.[104]

This meant that the owners of critical infrastructures could choose their level of cooperation with OCIPEP and there was nothing that OCIPEP could do to compel their cooperation. That alone could have rendered the organization ineffective and a misuse of government resources. Complete non-cooperation would have been unlikely due to the high value placed both nationally and internationally on critical infrastructure protection and a growing realization by Canadians of its importance, yet OCIPEP was not the only venue to work with critical infrastructure protection[105], and its existence was somewhat dependent on an ability to engage the owners of critical infrastructure and provide the best value for any resources they might have chosen to allocate.

---

[104] Confidential telephone interview, July 26, 2004.

[105] Many sector organizations worked to share information on smart practices and methods of protecting critical infrastructure, one such example is the Canadian Electricity Association. There were also other government departments providing information on specific aspects of critical infrastructure protection, such as the RCMP and the Solicitor General's Office.

While partnerships were considered by many to be successful, this was largely due to no threat of regulating relationships, and there also existed a prospect of improved information being available to partners. As time passed and the partners sensed the impotence of OCIPEP to effect change, the effectiveness of the partnerships diminished. Also, the partnerships with the provinces were noted as something of an exception to this "success". Part of this was that the burden of critical infrastructure protection was viewed as one way, that the federal government (through OCIPEP) proposed new policy initiatives, and the provinces with their very limited capacity, had to respond to those initiatives instead of looking at it from the other direction—that of identifying the provinces' and municipalities' legitimate needs and using OCIPEP to support them. The "Ottawa-cenric" nature of the OCIPEP-provincial relationship was another factor that inhibited success, as regional offices were sparsely staffed compared with staffing in Ottawa. When one considers that the majority of the owners and operators of key critical infrastructure who would be the first responders in the event that something went wrong were out in the regions, the concentration of OCIPEP in Ottawa made it remote from the front-line issues. This resulted in a top-heavy policy arm, and a bottom-light program delivery arm.[106]

A key challenge facing OCIPEP was to define not only its own role and responsibilities as the lead agency for critical infrastructure protection and emergency preparedness, but also to do so in relation to other lead departments that had direct responsibilities for protecting/assuring their critical infrastructure sector, and for sectoral

[106] Confidential telephone interview, November 24, 2004.

preparedness itself.[107] That was the role of the departments that were in charge of each critical infrastructure, and OCIPEP's role was to help them do that through providing best or smart practices, helping with business continuity plans, providing alerts and advisories about cyber threats. OCIPEP also lacked any sort of policy leverage to compel departments to take steps to protect their own critical infrastructure, it depended strictly on the departments realizing that such preparations were in their best interest. There was not any coordinated decision-making about which department should get what level of critical infrastructure protection funds, nor were accounting requirements set up to be able to determine afterwards how the monies had been spent.[108]

Within government it is normal for departments to have trouble sharing "issues," as each issue may come with some funding or cachet attached to it. Thus existing organizations or departments that also have responsibility for an existing issue may react as if the new organization was trying to take away part of the issue (the zero-sum game idea that if one takes something, the other loses it) rather than as an opportunity for cooperation.[109] While this is not unusual, it did affect OCIPEP, perhaps more than necessary due to OCIPEP's location within DND. If it had been placed within the Solicitor General's Office at the start, some of that power struggle might have been eliminated.[110] It was also noted that cooperation happened when necessary, that infighting did not endanger programs.[111]

---

[107] Confidential telephone interview, December 15, 2004.

[108] Confidential telephone interview, November 24, 2004.

[109] Confidential telephone interview, November 10, 2004.

[110] Confidential telephone interview, December 15, 2004.

One more challenge identified was that of defining the end state and aligning federal resources to get there. Knowing what the ultimate end goal of OCIPEP was might have increased cohesion as an organization, and provided more specific targets to work towards. As it was, there was a lack of communication horizontally within OCIPEP, each division would do their own work and other divisions would not necessarily know what was going on.

A final obstacle to OCIPEP as an organization was the reorganization of the United States' national security departments and organizations into the overarching Department of Homeland Security. While Canada is in no way tied to mirroring the organizational changes that the United States make, there is a necessity to be able to speak with the right people at the right times, and in having a complementary framework to work through. OCIPEP was too small and too specifically oriented, considering that it did not have access to the Solicitor General portfolio, especially those resources surrounding terrorism information and responses. It made more sense, considering the vast amount of shared critical infrastructure and shared threats between Canada and the United States, to enable organizations to work more effectively together and reduce redundancy and additional effort that working with multiple organizations causes. The move to the new department of Public Safety and Emergency Preparedness Canada (PSEPC) mirrors more closely what the United States' Department of Homeland Defence does. Also, the fact that PSEPC has emerged as a high-profile department lends a credibility to the organization that it never had as an office within the Department of National Defence.

---

[111] Confidential telephone interview, November 10, 2004.

One major threat for OCIPEP was the possibility of being viewed as a lame-duck organization. When OCIPEP was created there was a feeling of excitement within the government about the opportunity that OCIPEP provided to play a very important role in safeguarding the security of Canada. Over time this feeling of excitement waned, as OCIPEP was not making a noticeable change to policy or visible improvements to critical infrastructure protection in Canada. Connected to this were the external threats that occurred between the creation of OCIPEP and its dissolution—the events of September 11, 2001, SARS, West Nile, BSE, the blackout. To the public, OCIPEP played no visible role in any of these, other than the apparent lack of information provided during the blackout.

August 2003 Blackout

OCIPEP was criticized during and after the blackout in August of 2003 due to what was viewed as a failure of the federal government to respond to a crisis. When the power went out in Ottawa just after 4 pm on August 14, 2003 there was no indication of the extent of the power failure, that it extended past Ottawa to all of Southern Ontario and the North-Eastern United States. Given the time of day many public servants went home. As the extent of the blackout was be discovered, the media called their contact number for further information, which was the number of the public affairs department of OCIPEP. OCIPEP had its own challenges with technology failure during a critical hour when the blackout first occurred, which gave rise to media allegations that public affairs were not working. The irony in this situation was that, although OCIPEP was ineffective in many of its endeavours as an organization, the power outage was portrayed as

evidence of OCIPEP's ineptitude, in reality it demonstrated a lack of foresight within the Government of Canada as a whole and not OCIPEP specifically.

Such a failure of OCIPEP's own critical infrastructure resulted in a loss of confidence in government, and the public was given the impression that even among those whose job it was to provide information about critical infrastructure protection and emergency preparedness, there was no ability to "weather the storm."[112]

That situation was a benchmark for people's confidence in the government, and it failed. Much of government planning neglected to consider that the Government of Canada might itself be the victim of critical infrastructure failure. Some departments are better equipped than others, and OCIPEP was not responsible for the business continuity planning of other departments.[113] An example of this was in the telecommunications sector, when during the 1998 ice storm that affected Southern Ontario and Québec, those working with telecommunications realized that back-up generators require fuel in order to work. Unfortunately, during the emergency it was realized that telecom was low on the priority list for fuel, meaning that communications broke down.[114] By the 2003 power outage this oversight had not been remedied, and thus the lack of telecommunications was again a problem. Thus even within sectors, "lessons learned" were not necessarily acted upon.

---

[112] Confidential telephone interview, November 16, 2004.

[113] Confidential telephone interview, July 26, 2004.

[114] Bruce Stock, "Emergency Preparedness in Quebec: the Position After the Great Ice Storm," *Emergency Preparedness Digest* (October – December 1998); online, Public Safety and Emergency Preparedness Canada, Internet, 20 June 2005.

Many felt that OCIPEP was under-funded and under-resourced. The question of funding is a common concern in government today, but the fall-out from the lack of funding contributed to staffing challenges (including employees who continued to be classified as seconded or temporary), which were notably difficult.

Leadership

Another resource that OCIPEP lacked was recognition on the part of their Minister, who was often more focussed on national defence issues than on critical infrastructure protection and emergency preparedness, leaving OCIPEP without a widely recognized political champion to build recognition within government. This contributed to OCIPEP's perceived lack of legitimacy among other government departments. The Minister of National Defence also did not have direct counterparts within provincial governments and there were not well-established channels of communication between the two orders of government at the bureaucratic level. Most provinces did have some sort of office to do with emergency preparedness,[115] however, the responsibility for critical infrastructure was often other than for emergency preparedness, thus requiring a major effort to find the right people and coordinate with them.[116] The public servants who worked in the Department of National Defence had to deal with the issues that OCIPEP brought up and OCIPEP was not their main focus or area of specialty, yet another factor that contributed to OCIPEP's alienation within its home department.

The rush at the beginning to set up OCIPEP and make it operational meant that there had not been the time necessary for a careful consideration of priorities and what

---

[115] Confidential telephone interview, November 10, 2004.

[116] Confidential telephone interview, January 5, 2005.

skill-sets staff needed to fill those priorities. Part of the creation of a new organization involves looking for some relatively easy products to deliver in a short period of time, which must be achievable with the skill-sets that people bring with them. This was difficult with OCIPEP as critical infrastructure protection in general is complex and the opportunity for "easy wins" was really not there.[117]

Identification of National Critical Infrastructure

One of the stated objectives for OCIPEP for part of its lifespan was to identify the critical infrastructure in Canada, not unlike the vital points program with EPC during the cold war, in the sense that once identification of national critical infrastructure (or vital points) had taken place there was no real plan to utilize the information. There were concerns about whether or not this identification would involve the creation of a list of critical infrastructure, due to questions of privacy, commercial confidentiality and potential for such information to fall into terrorist hands, once it was acquired.[118] This linked to another difficulty that OCIPEP had in working with private sector companies: the need to protect information, and the difficulties inherent due to the Access to Information Act, which allows Canadians to request government information.

The act states that such information should be available to the public, that exceptions may occur but should be "…limited and specific, and that decisions on the disclosure of government information should be reviewed independently of

[117] Confidential telephone interview, November 24, 2004.

[118] Confidential telephone interview, November 24, 2004.

government."[119] Considering the sensitive nature of collecting such information, especially because most critical infrastructure is privately owned, there needed the development of a more secure plan for protecting this information. For example, key manufacturers within industry did not want to tell the government about their critical infrastructure for fear that the information would fall into the wrong hands, and also because such specific information might be used to increase regulation, such as environmental regulations. Industries may have felt that they could protect their critical infrastructure better on their own with access to more advanced and up to date technologies than the government had access to, for example, cyber industries.[120]

Without a comprehensive list of critical infrastructure, it made the task of assuring or protecting such infrastructure more difficult, as each owner/operator would have then to be up-to-date on the latest information products. It would also have required a level of trust on the part of the Canadian public that critical infrastructure was being satisfactorily protected by those who owned it, as the Government of Canada would not have a comprehensive list that it could consult to determine the state of readiness or preparation. Although OCIPEP was a small organization there existed significant stove-piping, or a tendency for people not to communicate openly with others outside their division.

Accountability

A serious lack of financial accountability was commented on by the Office of the Auditor General of Canada in their April 2005 report on National Security in Canada. In 2001, roughly $95 million was allocated to OCIPEP as part of a new program for

---

[119] Department of Justice Canada, *Access to Information Act, Chapter A-1* <http://laws.justice.gc.ca/en/A-1/8.html> December 28, 2004.

[120] Confidential telephone interview, July 26, 2004.

emergency preparation and critical infrastructure protection. OCIPEP was to coordinate this program across 12 departments, with the objective to "…expand the capacity of federal agencies to protect the country's critical infrastructure from attack."[121] The report states,

> Officials were unable to say how much money OCIPEP had spent on the critical infrastructure protection program and how much funding had lapsed. We interviewed staff from OCIPEP, National Defence, and PSEPC, and no one was sure whether funding had been deferred to subsequent years or had been absorbed into other programs. Program staff told us that in the first two years they thought they had lapsed $10 million of a $35 million budget, but we were unable to verify this. [122]

The report also states that the team auditing OCIPEP was

> …able to determine that part of the problem in tracking expenditures was the failure of OCIPEP staff to charge their work to the correct financial codes. Management could not correct this problem. In our opinion, basic management controls were missing. We were told that the program may not recover the lapsed funding.[123/124]

This issue of financial mismanagement was also commented on in the Auditor General's report with regards to OCIPEP's funding of CBRN (Chemical, Biological, Radiological and Nuclear) equipment, administered through the Joint Emergency

---

[121] Office of the Auditor General of Canada. *Report of the Auditor General of Canada: National Security in Canada—The 2001 Anti-Terrorism Initiative -- Air Transportation Security, Marine Security and Emergency Preparedness* (Ottawa, Office of the Auditor General of Canada, April 2005) Chapter 2: 35.

[122] Office of the Auditor General of Canada, Chapter 2: 36.

[123] Office of the Auditor General of Canada. Chapter 2: 36.

[124] As with many reports issued by the Office of the Auditor General there were spaces for the department's response, however since OCIPEP as an entity had been subsumed by the time that the report was issued the response was from PSEPC and contained what they were planning to do in the future to meet the suggestions, rather than explanations for why events unfolded as they did.

Preparedness Program (JEPP). JEPP was chosen to administer $10 million in CBRN funding as the program was already in place and thus could distribute the funding quickly. Ultimately, the funding decisions were found to be arbitrary and based on how quickly a particular location sent in its application, rather than on a risk analysis. The choice of what to spend the monies on was left up to the province or municipality. One year into the two-year program, the CBRN steering committee began to use the provincial population percentages to guide the administration of monies, which was done with the intention of proportionately distributing funds across the country.[125]

The report also states that when OCIPEP first announced that it would be distributing funding for CBRN equipment it said that it would help to develop national guidelines as to what should be acquired and how people should be trained, which were subsequently not developed. Some ad hoc advice was offered, but that had ended by the summer of 2004 when officials stated that there was a concern about the government's liability if it recommended specific pieces of equipment. The equipment that was purchased ranged widely in price and quality. An example given in the report states, "…the costs of Level A suits to protect against chemical and biological hazards ranged from $700 to $7200, with no explanation for the cost difference."[126]

Issues with the effectiveness of the Emergency Preparedness College were also identified, in particular connected to the volume of CBRN training. The training was split up into introductory, intermediate and advanced training, and the numbers of people who received the intermediate and advanced training were not sufficient considering the

---

[125] Office of the Auditor General of Canada, Chapter 2: 30.

[126] Office of the Auditor General of Canada, Chapter 2: 31.

high expenditures towards this program. It also did not take into consideration the need for cyclical refresher training, and staff retraining due to instructor turnover.[127]

One of the biggest challenges that had the potential for a large payoff was the opportunity for people within OCIPEP to spend time and energy building relationships with privately owned companies and the provinces. OCIPEP's method for doing this was two-fold, in meeting with private interests through the NCIAP consultations, and in maintaining regional offices in ten provinces for working with provinces and municipalities. The private business and first responders are the constituents that actually deal with the emergency response in a given situation. This opportunity could have been taken advantage of more concretely, as business-involvement was more through business associations (such as the Canadian Electricity Association) than with specific businesses themselves; and the regional offices had few employees compared to those working in Ottawa. The conclusion can be drawn that OCIPEP was a policy-heavy organization, light on practical application. This was especially unfortunate considering that the policy could only be used to suggest changes for government departments, as OCIPEP did not have the authority to compel action.[128]

Why Horizontal Management?

Why is it that horizontal management is the best, or only, option when dealing with critical infrastructure protection? This is both a simple and a difficult question to answer. At the most basic level, the wide array of organizations that are responsible for the varied aspects of critical infrastructure protection are spread throughout the federal,

---

[127] Office of the Auditor General of Canada, Chapter 2: 33 and 37.

[128] Confidential telephone interview, November 24, 2004.

provincial and municipal governments; over business and industry; and beyond Canada's border. Interdependencies of critical infrastructure indicate that approaches taken by single actors are ultimately less effective and more costly than coordinated actions. The fact that the players are from varied organizations also means that they must work together on a more even playing field—it is less likely that a single "boss" would emerge because that could reduce the feeling of autonomy for each organization. Leadership is then more likely to be shared and democratic.

Another reason for horizontality is that the Government of Canada, having the resources and desire to coordinate information on critical infrastructure protection for internal and external use, does not have the capacity to be the leader. There always will be private organizations that have more resources in specific areas than public organizations will, due to the ability to pay for and receive specialized information and to focus specifically on the areas that affect them. "Best" or "smart" practices cannot be collected by listening to one organization alone, and cooperation can not be legislated. In order for constituents to feel motivated to contribute, they need to feel respected and valued. A forum must be developed which makes space for information sharing, rather than competition. Such an organizational structure is only going to happen in a horizontal model. Vertical organizations are based on a hierarchical model, which may not appeal to outside interests that may feel subjugated due to their location beneath other interests and decision-makers.

The need to build goodwill in industry is another issue. Should the Government of Canada regulate industry when it comes to business continuity or should that be taken care of by industry itself, which will deal directly with the greatest risks in the case that

critical infrastructure be damaged? Presently regulation exists with regard to the safety of people, but not with the resumption of operations. The possibility of increased legislation might be popular on the part of concerned public, but brings with it additional expenses for the businesses, which are rarely popular. The balance of relationship-building with business, in addition to satisfying the need to assure continuity of critical infrastructures, is a delicate one.

In this time of fiscal restraint the benefits of working horizontally are easy to see. The New Public Management model of organization relies on a more team-like approach to public management, working with a more responsive structure than traditional public service models. Reducing the duplication of service helps to identify and close "gaps" that otherwise might not have been noticed, by assuming that some other organization would take care of them. It benefits each of the participants to work with others on issues that are broader than their own, as it is never so simple to deal with one's own critical infrastructure. A business might have back-up power generators, air supply, water and waste water treatment, but still would not have the ability to guarantee roads or information services or any of a number of other services on its own, which demonstrates the value of partnering with others who can take responsibility for the condition of roads, etc.

It is widely recognized that critical infrastructure protection requires horizontality, entities working in partnership, across jurisdictions, and each critical infrastructure protection organization relies on these relationships. Within OCIPEP there was a lack of horizontality, even as it was touted as the answer to the critical infrastructure puzzle. In theory, horizontal management of such an issue would lead to more effective and

efficient plans for critical infrastructure protection, with stakeholders involved the same way that government officials were, working in consultation to achieve the same goals. The National Critical Infrastructure Assurance Plan and the consultations they held in a number of locations throughout Canada best illustrate such horizontality, and they were the most effectively horizontal part of OCIPEP.

The particularly unfortunate result of this lack of horizontality overall was that while OCIPEP was uniquely located within the Government of Canada to demonstrate horizontal management, instead they defaulted to the vertical structures common to the rest of government. Subjects interviewed spoke of a lack of information sharing between divisions, frequent changes of directors leading to nearly constant relationship-building within the organization and relearning of personal styles. There was also discussion of a lack of cooperation between divisions, with disappointingly little feedback from other directors when requested, roadblocks put in place from the policy division, and little management support of those actually involved in program delivery.

Considering that leadership is a factor critical to the successful delivery of horizontal programs and that relationship-building and trust take time to develop, the frequent changes of management staff within OCIPEP structurally contributed to failure. Since leaders are needed for retaining corporate memory, to motivate partners, and to increase group cohesion, they require both time and commitment to their role. It is not the same as in vertically organized structures where leaders can be more interchangeable because roles are more rigid and people understand what they entail. Within horizontal projects leaders must be able to mediate between partners, develop group buy-in and a common language, integrate new members and increase commitment, as stated in the

horizontal management chapter. It seems like this was more successful within the divisions themselves, but not within the organization as a whole.

Horizontality as a way of functioning does not come naturally to many people, as most of our training (starting with early childhood education) system has taken place within a vertically-structured system. This does not mean that organizations that try horizontal management are doomed, certainly people are adaptable and can learn new ways of behaving, but that such behaviours must be demonstrated right from the top of management, and this was not successfully demonstrated with OCIPEP. As B. Guy Peters stated in his paper "Managing Horizontal Government," from 1998, structural manipulations on their own will not change behaviour, but must instead be followed up with appropriate budgeting and support from other government leaders. If a horizontal project is horizontal in name only, and structures for accountability, staffing, leadership et al are expected to remain the same government-wide, the horizontality will be greatly challenged, if not a failure entirely.

Another challenge to implementing horizontal management was a failure to effectively involve provinces/territories and private sector owners and operators of critical infrastructure in creating policy around critical infrastructure protection. The NCIAP was having some success with this, but was more involved with industry/sector organizations rather than the specific businesses themselves. In order for OCIPEP to be relevant there needed to be a degree of buy-in from these other groups, and there just was not enough to consider OCIPEP a success. It was not able to offer enough to private organizations in particular to justify the possibilities of increased legislation for them to follow. This contributed to a lack of influence on the part of OCIPEP.

In order for horizontal management to be more than in name only, OCIPEP would have required time to organize before they were expected to produce visibly. It would also have required management who had the vision of a different structure than traditional government structures, as OCIPEP was not a central agency or a line department, but something else entirely. This would have required a unified vision on the part of government as a whole, and significant confidence on the part of those who were to lead the organization, both in the vision itself and in how it was supported by the rest of government. This may have allowed decisions to be made in a more horizontal, collaborative way, thus increasing the impact of undertaken initiatives. To do this may have required an all-parties approach, in order to increase legitimacy and decrease challenges in parliament.

A great deal of study has been done within government through what was the Canadian Centre for Management Development, and now is the Canada School of Public Service, on horizontal management and why it is a positive development to incorporate greater horizontality within the Government of Canada. The arguments boil down to the need for increased fiscal restraint and better use of resources, both monetary and personnel. It is widely accepted that horizontal management is a positive idea yet the government has thus far not put in place supportive systems allowing for horizontality to occur past that of horizontal attitudes and culture, as horizontal coordination and/or collaboration are still not adequately supported. This is the direction that the Government of Canada needs to work towards. OCIPEP was an ideal candidate with which to pilot horizontal management due to the absolute need for horizontality in order to pursue its mandate.

Although horizontal management was not a complete success for OCIPEP, the government has been taking steps towards more thorough horizontal integration, as evidenced in creating the new department that has subsumed OCIPEP: Public Safety and Emergency Preparedness Canada. In bringing together such organizations as the Royal Canadian Mounted Police (RCMP), Canadian Security Intelligence Service (CSIS), Correctional Service of Canada (CSC), National Parole Board (NPB), Canada Firearms Centre, Canada Border Services Agency, along with critical infrastructure protection and emergency preparedness, an interagency horizontality should be more easily attained. Thus rather than horizontality being a threat to one organizations financial and human resources, this co-location of related organizations should reduce such stress and allow better coordination and cooperation.

Summary and Conclusions for Chapter Three

The organization of an office dedicated solely to assembling and clarifying Canada's critical infrastructure protection plans was a necessary step for Canada in order to be able to deal with new threats to infrastructure due to interdependencies and the fact that information technology touches most other infrastructures in some way. Y2K was a strong catalyst for creating and implementing plans, but certainly not the only reason for expanding the area of Emergency Preparedness Canada to include critical infrastructure.

The Government of Canada's all hazards approach is different from the approach taken by other countries, notably the United States, which focuses specifically on terrorism. Considering the variety of disasters that might cause a failure of critical infrastructure, Canada's approach is the best choice. The background reasons behind the

critical infrastructure failure is specific departments to deal with, helping them with emergency preparedness, contingency planning and mitigation is OCIPEP's work.

The revision of the original six sectors identified as critical infrastructure into the ten now listed was a positive change, not least because it shows that public consultations have had an impact, that OCIPEP was willing to work with stakeholders other than the federal government. Considering the fact that 85 per cent of critical infrastructure belongs to entities other than the federal government, demonstration of a willingness to work together shows the possibilities for horizontality: working across boundaries and jurisdiction to choose the best solutions.

OCIPEP as an organization was not given the resources it needed to make a successful effort at coordinating the country's critical infrastructure. It could not overcome staffing challenges, the lack of authority to compel action on the part of other government departments, or its location within DND, which all contributed to a lack of legitimacy and an inability to effect noticeable change on the critical infrastructure landscape of Canada. The lack of a Government-wide supported cultural context for horizontality also contributed to OCIPEP's ineffectiveness as the level of cooperation and collaboration needed was not there.

Accomplishments primarily had to do with successful relationship and partnership building, both within Canada and internationally. Barriers to success include the previously mentioned lack of legitimacy, power-struggles within the organization, and an inability to legislatively protect information which prevented sharing of critical infrastructure information by the majority of critical infrastructure owners who belong to others than the federal government. This leads to the most obvious challenge—that only

about 15% of critical infrastructure was owned by the Government of Canada, yet they purport to coordinate plans to protect all of it.

Opportunities include the fact that this was the first organization devoted to critical infrastructure protection in the country, and its dual mandate was the first in the world to incorporate critical infrastructure protection and emergency preparedness. While external events demonstrated to the Canadian public a lack of ability to fulfil its mandate, those events were not entirely understood in relation to what OCIPEP was attempting to do and thus it was unfairly accused of inaction.

Horizontal management is the only way that critical infrastructure protection can effectively be organized and, while OCIPEP failed to exemplify effective horizontality, it led the government to the creation of a new department of Public Safety and Emergency Preparedness Canada that is better positioned to accomplish that goal. Thus OCIPEP has provided a number of lessons for the Government of Canada to learn, and it appears that they have been taken to heart. How well will be determined by time.

Chapter Four: Conclusions and Recommendations

OCIPEP as a stand-alone organization had the potential to be an organization within government that, by using horizontal management, functioned as a bridge between the political parties and the bureaucrats, departments, the public and private sectors, the federal government and the provincial and municipal governments. It did not live up to its potential in part because it was not given the tools it needed that would have allowed it to make a success of its mandate. The challenges inherent in such a quick start-up with so few resources meant that many people within OCIPEP felt insecure in their jobs, that corporate services within the organization itself were not stable, and that unless it had the best of luck it was bound to fail. It did not have the best of luck, but instead had to deal with all the challenges of horizontality, with few of the benefits and a raft of external crises. The decision to dissolve OCIPEP as an organization and to incorporate it into Public Safety and Emergency Preparedness Canada was a move that needed to be made.

New Public Management purports to be a method for increasing government's responsiveness while decreasing costs. Costs do not only mean monetary ones, but those of all types of resources: leadership, staffing, support throughout government, citizen-support, among others. Horizontal management fits within a model that tries to increase responsiveness and decrease costs by allowing all stakeholders to become part of the solution. When stakeholders become part of the team responsible for setting standards and working cooperatively they increase buy-in and commitment to the project. Considering the challenges involved with a government that tries to protect critical infrastructure, much of which does not belong to that government, it is more than beneficial to work cooperatively: it is a requirement. The Government of Canada does not

have the resources that would be needed if it were to set policy for critical infrastructure protection on its own and to require all constituents to follow that policy. Private industry will always have greater resources in that sense simply because they can focus on their own specific interests and not try to cover everything. Working together with huge private industries all the way down to small business and municipalities created space to share knowledge and recognize that these issues were important to all, and all would have to be part of the solution. New frameworks for leadership, accountability and information sharing have needed to be developed, and this need will continue as each horizontal initiative will be unique. As more and more projects are operated with this framework such development will become "normalized," with the partners involved recognizing the nature of their roles and the informal rules of interaction. As with any new enterprise, the initial investment in time, learning and re-learning, and selling the ideas to others is recovered as such methods of working become accepted as they are proven to succeed.

The decision made to consult with the public through the NCIAP consultations was a good one, as making use of the stakeholders' input was necessary to increase the relevance of what OCIPEP was working on. The NCIAP achieved a measure of success in relationship-building with private sector organizations, even though it was run with fewer than 10 people. Likewise, the increase in sectors from six to ten better reflects departmental responsibility (with a few exceptions, unavoidable due to the integration of technology and infrastructures) and makes the sectors easier to comprehend and can let the public and stakeholders see better both the complexity of the task of protecting critical infrastructure, as well as how and where they fit in.

Partnering was recognized as one of the more successful initiatives, both within Canada and internationally. International partnerships were widely recognized as an area of strength, and other countries looked to OCIPEP as a leader and as an example of what could be done to work with such a difficult subject. Greater acceptance of critical infrastructure protection as a necessary concept was more or less agreed to by stakeholders, and this recognition was achieved through many meetings and consultations with involved parties. This was and will remain critical to much of the success of critical infrastructure protection, because it is not a task that one organization can do successfully on its own. The world of technology, and increasingly the world of economics, no longer recognizes borders and in order to protect critical infrastructure from new threats that may initiate anywhere the solutions need to go beyond borders as well.

Perhaps the most unique aspect of OCIPEP was that it was charged with the Government's preparation and response to critical infrastructure threats, but it was not given the authority to require other departments or agencies to take specific actions. Of course this was a barrier to its success, and is why it cannot be compared directly with central agencies, though each had in common a location outside of line departments. This confusion of roles between those of a central agency and those of a traditional line department contributed to trouble in understanding how OCIPEP was pursuing its mandate, and the roles needed to be clarified.

Other difficulties included the yet unsolved problem of protecting private information through legislation, as private companies will continue to keep their information private until there is proof that it is protected if they share it with the Government. Even if it is possible to protect that information it will be a difficult job to

convince private organizations that it is in their interest to share such data with the Government of Canada. This may result in a comprehensive list of critical infrastructure never being made. As long as all stakeholders share and use “smart practices,” such a list may not be required.

The Government of Canada must create plans that include the Government of Canada as victim, an exercise that was embarrassingly demonstrated as a need during the August 2003 power outage. Such a situation proved the requirement for all departments to have their own plans for continuous operation in the case of an emergency, and how important redundancy is. The loss of public confidence during that particular situation will only be restored as Canadians learn how the Government is improving their own planning, not just encouraging Canadians to be ready for emergencies personally. It will take a great deal of public education to help average Canadians to understand the Government’s role in critical infrastructure protection, though it seems as if stakeholders both inside Canada and outside have become more knowledgeable of OCIPEP (and now PSEPC) and willing to partner.

The researcher was surprised and delighted with the ease of obtaining interview subjects as it is well known that this is often a difficult process for research. Subjects were all very helpful both in providing information and in suggesting further avenues for investigation. It was a pleasure to work with this sample of people.

Recommendations

The incorporation of OCIPEP into PSEPC has already been demonstrated to be a beneficial choice both in increased profile, due to being in a department that correlates more closely with the aims of critical infrastructure protection than did DND, and

because PSEPC has emerged as a high-profile department. The Auditor General's report that was so critical of how OCIPEP's operations took place made recommendations that are in line with many of the initiatives that PSEPC already had underway at the time the report was written. This bodes well for the future of the department and for critical infrastructure protection in Canada.

This departmental integration should also improve communication with the former Solicitor General's department, which was responsible for any terrorism arising on Canadian soil; which obviously overlapped with parts of OCIPEP's mandate. Issues of communication between these offices and the RCMP and CSIS will need to be worked out, but should increase the information available on all areas of responsibility which ideally will make the department more responsive than the components previously were.

In order to improve "buy-in" on the part of partners who are not compelled to work with the Government (e.g. private industry) consultations with parties who have a vested interest in protecting critical infrastructure are suggested with the purpose of developing a strategic set of goals. This could result in greater obligation on behalf of the partners as they contributed to the creation of the strategic plan, and the Government would be situated as a more relevant organization that is committed to taking the partners' concerns seriously. This carries with it the risk of the Government losing some control over the process, but the potential gain of more committed partners could make the risk worthwhile.

A further recommendation is that OCIPEP take on the responsibility for managing interdependencies, and to let the industry/sectoral associations (such as the Canadian Telecommunications Emergency Preparedness Association, the Canadian Electricity

Association) be responsible for the critical infrastructure plans on the part of the private sector. This way the associations, which have the best knowledge of what is possible and desirable in their sectors, can regulate their member associations without the perception of increased governmental interference, which is a risk if the Government of Canada increases the regulation of these industries. There certainly is a role for the Government of Canada in helping communication and information-sharing to happen cross-sectors and between levels of government.

The need for better information-sharing, and a more organized approach to lessons learned was demonstrated in the communications sector between the 1998 ice storm and the 2003 blackout. One of the lessons learned from the ice storm was that telecommunications required fuel in order to run emergency generators, and that sector was a low priority for emergency fuel. This was an issue again during the power outage, and considering that it affected some of the same telecom businesses there was no reason why this was not followed up on. If organizations do not follow up on their own lessons learned how much more difficult is it for one sector to learn from the challenges to another sector? If there was a specific project that allocated time to compiling lessons and disseminating it to other organizations, with a follow up to help increase the practical use of the information, it might help the coherence of practical applications of critical infrastructure protection and improve its implementation.

If further research into this area is undertaken, interviews should be conducted with a greater number of subjects, and the sample should be chosen more systematically than the snowball sample used for this case study. There is always a risk in using a sample where the subjects are referred by other subjects that the group will self-select to

the point that only a narrow range of viewpoints are apparent, especially considering the small sample size. A more systematically chosen subject-set would decrease this possibility and widen the range of opinions and experiences.

It would also be interesting to carry out the interviews in person rather than over the telephone, due to the additional information that can be garnered by observing the subject's body language and other non-verbal cues.

Canada's horizontal approach to critical infrastructure protection was and continues to be a topic worthy of study and analysis. The view that Canada is a world leader in critical infrastructure protection can continue with an uninterrupted emphasis on partnering and sharing information globally. This requires a commitment to longitudinal funding, regardless of the political party in power. With such an emphasis on the desirability of horizontal critical infrastructure protection, Canada will continue to improve and build on OCIPEP's success, and mitigate weakness.

Bibliography

Aucoin, Peter. *The New Public Management: Canada in Comparative Perspective* Montréal: The Institute for Research on Public Policy, 1995.

Bakvis, Herman, and Luc Juillet. *The Horizontal Challenge: Line Departments, Central Agencies and Leadership.* Ottawa: Canada School of Public Service, 2004.

Bakvis, Herman. "Pulling Against Gravity? Horizontal Management in the Canadian Government." *Proceedings of the conference'Knowledge, Networks and Joined-Up Government.'* Centre for Public Policy, University of Melbourne, June 3 –5, 2002.

Barzelay, M. and C. Campbell. *Preparing for the Future: Strategic Planning in the US Air Force.* Washington: Brookings, 2003.

Bourgault, Jacques. *Accountability and Horizontal Management: an Approach for the Quebec Federal Council.* Report to Marlynn Briseboise. Ottawa: Treasury Board of Canada Secretariat, 16 May 2002.

Bourgault, Jacques and René Lapierre. *Horizontality and Public Management*. Ottawa: Canadian Centre for Management Development, 2000.

Canada, Canadian Centre for Management Development. *Moving from the Heroic to the Everyday: Lessons learned from Leading Horizontal Projects.* Ottawa: Canadian Centre for Management Development, 2001.

---, Department of Justice. *Access to Information Act, Chapter A-1*. Department of Justice Canada, August 31, 2004, <http://laws.justice.gc.ca/en/A-1/8.html> December 28, 2004.

---, Environment Canada and the Synthesis Workshop on Horizontality for the Canadian Centre for Management Development's Action-Roundtable on the Management of Horizontal Issues. *Guide to Building Dialogues on Horizontality: Discussion Paper.* Ottawa: Canadian Centre for Management Development, November 8, 2000.

---. Joint Canada-US Task Force Releases Power Outage Sequence of Events. 2003-72, September 12, 2003. <www.nrcan-rncan.gc.ca/media/newsreleases/2003/200373_e.htm>

---, Office of Critical Infrastructure Protection and Emergency Preparedness. *Fact Sheets: National Critical Infrastructure Assurance Program*. <www.ocipep-bpiepc.gc.ca/info_pro/fact_sheets/general/CIP_NCIAP_e.asp>. April 25, 2004.

---, ---. Home page, <www.ocipep-bpiepc.gc.ca> January 17, 2003.

---, ---. "National Critical Infrastructure Protection Program." *Emergency Preparedness Digest* January-March 2002.

---, ---. National Critical Infrastructure Assurance Program, *An Assessment of Canada's National Critical Infrastructure Sectors* July 2003. <www.ocipep-bpeipc.gc.ca/critical/nciap/nci_sector1_e.asp>. April 25, 2004.

---, ---. *National Critical Infrastructure Assurance Program Synopsis*. <www.ocipep-bpiepc.gc.ca/critical/nciap/synopsis_e.asp>. September 3, 2004.

---, ---. *National Critical Infrastructure Assurance Program, Update No. 1*. <www.ocipep-bpiepc.gc.ca/critical/nciap/update1_e.asp>. September 4, 2004.

---, ---. *National Critical Infrastructure Assurance Program, Update No. 3*. <www.ocipep-bpiepc.gc.ca/critical/nciap/update3_e.asp>. January 31, 2004.

---, ---, News Release. *Government of Canada Launches Consultations on the Development of a National Disaster Mitigation Strategy*. Ottawa: Office of Critical Infrastructure Protection and Emergency Preparedness, June 26, 2001.

---, ---. *Slides-Presentation to DSAB Asymmetric Threats Study Team*. Ottawa: January 15, 2002.

---, Office of the Auditor General of Canada. *Report of the Auditor General of Canada: National Security in Canada—The 2001 Anti-Terrorism Initiative – Air Transportation Security, Maritime Security and Emergency Preparedness* April 2005.

---, Public Safety and Emergency Preparedness Canada. *National Critical Infrastructure Assurance Program Selection Criteria to Identify and Rank Critical Infrastructure Assets,* January 20, 2004. <www.ocipep_bpiepc.gc.ca/critical/nciap/nci_criteria_e.asp>. May 4, 2005.

---, Standing Senate Committee on National Security and Defence. *Canada's Fragile Front Lines.* 48.

---, ---. *Evidence* (Ottawa, October 20, 2003) online, Parliamentary Search Engine, Internet, April 20, 2004.

---, Standing Senate Committee on National Finance. *Evidence* (Ottawa, October 23, 2001) online, Parliamentary Search Engine, Internet, April 21, 2004.

---, Statistics Canada. *2001 Canadian Census: A Profile of the Canadian Population*. <http://geodepot.statcan.ca/diss/highlights/Page9/Page9_e.cfm>.

Caro, Denis. "Integrated Emergency Support Systems: Governance and Leadership Challenges," *Optimum Online: The Journal of Public Management*. 31 (2) December 2001.

Charih, Mohamed and Lucie Rouillard. "The New Public Management and Public Administration in Canada." *New Public Management and Public Administration in Canada.* Toronto: The Institute of Public Administration of Canada, 1997.

"CIAO: An Integrated Approach to Counter-Threats of a 'New Era' (An Interview with Dr. Jeffrey A. Hunker Director of the Critical Infrastructure Assurance Office)." *USIA Electronic Journal.* 3(4) November 1998.

Confidential telephone interview, July 26, 2004.

Confidential telephone interview, November 10, 2004.

Confidential telephone interview, November 16, 2004.

Confidential telephone interview, November 24, 2004.

Confidential telephone interview, December 1, 2004.

Confidential telephone interview, December 15, 2004.

Confidential telephone interview, December 17, 2004.

Confidential telephone interview, January 5, 2005.

Denhardt, Robert B. and Janet Vinzant Denhardt. "The New Public Service: Serving Rather than Steering." *Public Administration Review* 60(6) November/December 2000: 549 – 559.

Dexter, Lewis Anthony. *Elite and Specialized Interviewing*. Evanston: Northwestern University Press, 1970.

Ditchburn, Jennifer. "Business, Government Reap Rewards of Y2K Planning in Wake of Sept. 11." *Canadian Press Newswire*. October 10, 2001.

Eckstein, Harry. "Case Study and Theory in Political Science." *Handbook of Political Science Volume 7: Strategies of Inquiry.* Ed. Fred I. Greenstein and Nelson W. Polsby. Don Mills: Addison-Wesley Publishing Company, 1975. 79-137.

Eggleton, Art (Hon), Minister of National Defence. *Address: 11th World Conference on Disaster Management*. Hamilton, Ontario, June 26, 2001.

Emergency Measures Organization Debriefing for Hurricane Juan. Dartmouth NS: October 29, 2003.

Fitzpatrick, Tom. *Horizontal Management: Trends in Governance and Accountability*. For CCMD's Action-Research Roundtable on the Management of Horizontal Issues. Ottawa: Canadian Centre for Management Development, 2000.

Gibaldi, Joseph. *MLA Handbook for Writers of Research Papers*. 4th Ed. New York: The Modern Language Association of America, 1995.

Harlick, James. *Standing Senate Committee on Defence and Security: Evidence* (Ottawa, July 19, 2001) online, Parliamentary Search Engine, Internet, 20 April 2004.

---, *Standing Senate Committee on Social Affairs, Science and Technology, Issue 20 Evidence*. (Ottawa, 17 September 2003) online, Parliamentary Search Engine, Internet, 20 April 2004.

Juillet, Luc. *The Federal Councils and Horizontal Governance: A Report Prepared for the Regional Federal Councils and Treasury Board Secretariat*. Ottawa: University of Ottawa, 2000.

Kernaghan, Kenneth, and David Siegel. *Public Administration in Canada, 3rd Edition*. Toronto: Nelson Canada, 1995.

Lahey, James (Chair). *Moving from the Heroic to the Everyday: Lessons Learned from Leading Horizontal Projects.* Ottawa: Canadian Centre for Management Development, 2001.

Mussington, David. *Concepts for Enhancing Critical Infrastructure Protection: Relating Y2K to CIP Research and Development.* Santa Monica, CA: RAND, 2002.

Nuutilainen, Janet. *OCIPEP: Leading the Way*. On-line: OCIPEP. <www.epc-pcc.gc.ca/whoweare/firstyear_e.asp>

O'Connor, Dennis R. *Part One, A Summary. Report of the Walkerton Inquiry: the Events of May 2000 and Related Issues.* Toronto: Ontario Ministry of the Attorney General, 2000.

O'Toole, Lawrence J., Jr. "Different Public Managements? Implications of Structural Context in Hierarchies and Networks." *Advancing Public Management: New Developments in Theory, Methods and Practice.* ed. Jeffrey L. Brudney et al. Washington DC: Georgetown University Press, 2000.

Peters, B. Guy. *Managing Horizontal Government: the Politics of Coordination*. Research Paper #21. Ottawa: Canadian Centre for Management Development, January 1998.

Purdy, Margaret (Associate Deputy Minister, National Defence). *Address to The Partnership for Critical Infrastructure Security, Annual Meeting and Public Policy Briefing*. Washington D.C, May 20-22, 2001.

---, *Critical Infrastructure Protection and Public Safety* Address at Strategies for Public Transformation 2002 Conference: Terrorism and Technology: Prevention, Protection and Pursuit. Whistler, B.C. April 29, 2002.

Scott, William G. et al, *Organization Theory: A Structural and Behavioural Analysis, 4th Ed*. Illinois: Richard D. Irvine Inc. 1981.

Sproule-Jones, Mark. "Horizontal Management: Implementing Programs Across Interdependent Organizations." *Canadian Public Administration* 43.1 (2000) 93-109.

Stock, Bruce. "Emergency Preparedness in Quebec: the Position After the Great Ice Storm," *Emergency Preparedness Digest* (October – December 1998); online, Public Safety and Emergency Preparedness Canada, Internet, 20 June 2005.

Tapscott, Don. "The Digital Media and the Reinvention of Government." *Canadian Public Administration*. 40(2) Summer. pp. 328-345.

Thomas, Paul. "Accountability Introduction," in *Handbook of Public Administration*, Ed. B. Guy Peters and Jon Pierre. London: Sage Publications, 2003.

---, *Performance Management, Reporting and Accountability: Recent Trends and Future Directions*. Regina: The Saskatchewan Institute of Public Policy, February 2004.

---, "The Changing Nature of Accountability." *Taking Stock: Assessing Public Sector Reforms* ed. B. Guy Peters and Donald J. Savoie. Montréal: Canadian Centre for Management Development, 1998.

---, "The Role of Central Agencies: Making a Mesh of Things." *Canadian Politics, 3rd Edition*. Ed. James Bickerton and Alain G. Gagnon. Peterborough: Broadview Press, 1999. 129-147.

Verschuren, Piet J. M. "Case Study as a Research Strategy: Some Ambiguities and Opportunities." *International Journal of Social Research Methodology*. 6:2 (2003): 121-139.

Ward, John. "Government Buildings Vulnerable to Terrorist Attacks, Experts Say." *Canadian Press Newswire*. October 7, 2001.

Appendix A.

E-mail inviting subjects to participate in this research

Sender: Marina Rountree (umrountr@cc.umanitoba.ca)

Subject: OCIPEP and horizontality research

My name is Marina Rountree, a graduate student in the Department of Political Studies at the University of Manitoba. As a requirement of my degree I am conducting research on the organization and management for the Office of Critical Infrastructure Protection and Emergency Preparedness. Part of my research includes phone interviews with a number of individuals connected to this organization. This letter is to invite you to participate in this research.

Research Goal: My research explores the nature of the Government of Canada's Critical Infrastructure Protection system, and its management from the time the office was established until until 2003, when OCIPEP was subsumed into the new Department for Public Safety and Emergency Preparedness.

I am hoping to interview you to discuss your views on OCIPEP and your experiences within the organization during the years outlined above. Each interview will be set up via e-mail to take place on the telephone at a time convenient for you. Anticipated timeframe of interviews is from 30 minutes to one hour, depending on the length of your responses, and the time that you have available. It is possible to continue the interview at another time convenient to each respondent, if necessary. After the information collected through interviews is assembled into a chapter format, I will send it to you for your review. You are not obligated in any way to provide further comment, however if you wish to clarify or change information that you have provided, it can be done at that time.

By proceeding to answer this e-mail, you are giving free and voluntary consent to participate in this project. Note, however, that you are free to withdraw at any point in time from the research project, without penalty, by simply advising me of your desire to withdraw. The information collected would at that point be destroyed, and no copies retained. Simply contact me via e-mail at umrountr@cc.umanitoba.ca, and any information collected up to that point would be destroyed.

Privacy:
If you choose to participate, please know that all records will be maintained in strict confidence at all times. All personal information collected is confidential and to be used for contact purposes only by the researcher. Information collected during the interview will be collected both through audio cassette connected to the telephone and via hand-written notes. If you prefer to be recorded in only one way, either audio or on paper, this can certainly be accommodated. Please state your request at the beginning of the

interview.

All audio cassettes and handwritten notes will be stored in a locked filing cabinet at my personal residence. Information will also be stored on my personal computer, which is password protected and not networked to any other computer. Also note that direct quotes, if used, will appear in an anonymous format (non-attributable) in the body of the final research paper. When the research is completed, the audio cassettes, notes and electronic files will be destroyed.

Final Paper:
The completed paper will be housed at the University of Manitoba library and Political Studies office. It can be sent to you upon completion via e-mail, either in its entirety or in summary if you would like.

For further information or clarification, please contact me at:
Marina Rountree (204) 284-8075 or <umrountr@cc.umanitoba.ca>.

Thank you for your time and I look forward to your response,

Marina Rountree
Graduate Student, Master of Arts

This research has been approved by the Joint-Faculty Research Ethics Board at the University of Manitoba If you have any concerns or complaints about this project you may contact any of the above-named persons or the Human Ethics Secretariat at 474-7122.