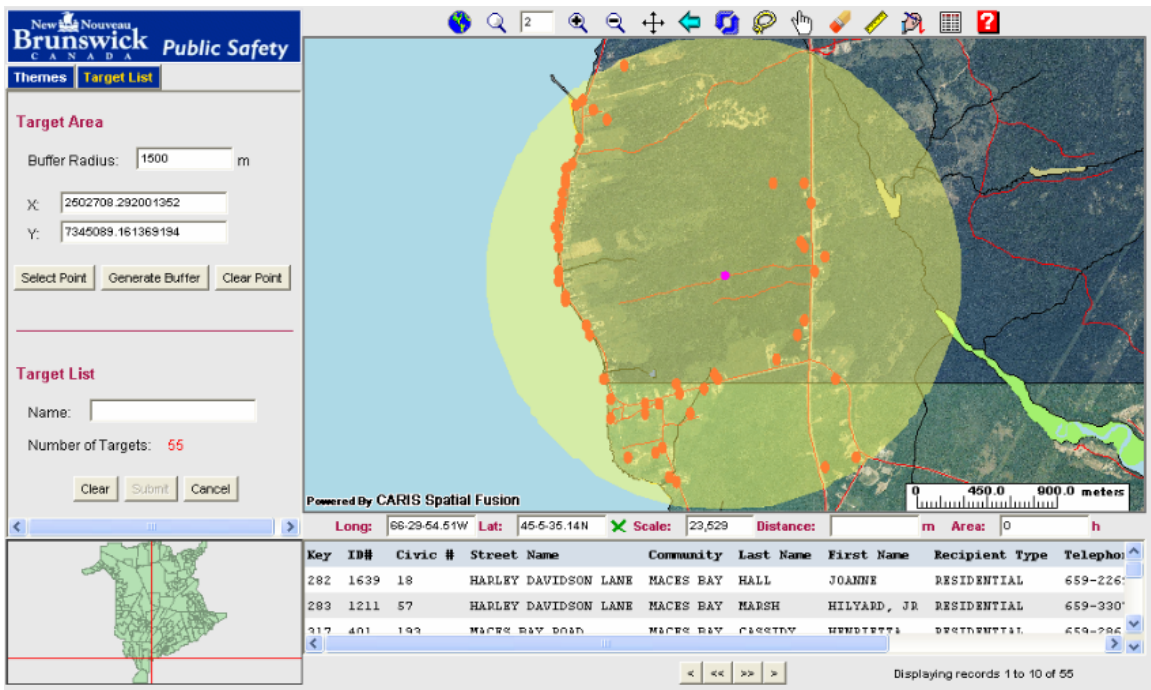


Summary Report

Geographical Public Alerting System



The screenshot displays the 'Public Safety' interface for New Brunswick. It features a map with a green circular target area and a list of targets. The interface includes a 'Target Area' section with a buffer radius of 1500 m and coordinates X: 2602708.292001352 and Y: 7345089.161369194. Below the map is a table of target records.

Key	ID#	Civic #	Street Name	Community	Last Name	First Name	Recipient Type	Telephone
282	1639	18	HARLEY DAVIDSON LANE	MACES BAY	HALL	JOANNE	RESIDENTIAL	659-2261
283	1211	57	HARLEY DAVIDSON LANE	MACES BAY	MARSH	HILYARD, JR	RESIDENTIAL	659-3301
317	401	193	MACES BAY ROAD	MACES BAY	CRESTBY	HENDERSON	RESIDENTIAL	659-2906

Executive Summary

Statement

Our strategy is to provide a basic public warning capability, covering the entire province, and to provide the means for local solutions to address local requirements. This project has contributed significantly to the strategy and has delivered the tools necessary to manage a provincial system.

The only remaining obstacle to deploying a provincial system is access to a reliable source of geo-referenced civic address data; work is ongoing to gain access to 911 data for that purpose.

Project Description

The Geographical Public Alerting System project was developed and managed by the New Brunswick Department of Public Safety, for Industry Canada.

The project was a collaborative effort of the *New Brunswick Department of Public Safety, Aliant Incorporated, Caris Limited* and *Xwave* (An Aliant Company); all parties made significant intellectual and in-kind contributions to the project. Industry Canada provided majority funding.

The intent of the project was to develop and demonstrate, for Industry Canada and the Province of New Brunswick, a single public alerting system capable of creating and sending list-based and geographically-based notifications, by means of a variety of commercial communications channels, with emphasis on interactive-voice response (IVR).

The project vision was to integrate geographical information system (GIS) capabilities into an existing public alerting application, allowing public safety officials to select geographical areas for alerting. A significant feature of the integrated application was that it was to be based on existing commercially available hosted services, remotely accessible over the Internet.

Project Outcomes

The project was successful, in all respects:

- the integrated application worked precisely as designed and performed well in production;
- the integrated application, given appropriate data, provides users with the added capability to alert the public on a geographical basis, without the need for a pre-built contact list;
- the project delivered enhanced capabilities and added value to the existing applications;
- the project proved that public and private sector partners could successfully collaborate on the development of effective tools for emergency management; and
- the project fostered new partnerships and business arrangements that are contributing to commercial success and further product evolution.

<p style="text-align: center;">Geographical Public Alerting System</p>		<p style="text-align: center;">Public Safety Sécurité publique</p>
---	---	---

Opportunities

In addition to satisfying project objectives, the project has resulted in a new business partnership between the Department of Public Safety and Xwave, and a number of significant developments:

- Xwave has acquired the intellectual property from Aliant and assumed responsibility for the production environment; this has facilitated investment in infrastructure and will enable further application development; throughput has been increased to 5000 IVR calls per hour.
- Xwave has made significant enhancements to the Civic Notification application; the system now provides for multiple users and data sets, enhanced call logic supporting multiple organizations, positions and contacts, and supporting additional notification channels; the enhanced feature set and capabilities have attracted new major clients.
- Public Safety has committed to acquire and manage the newly enhanced Civic Notification application for the Province of New Brunswick; the application will support public alerting, security alerting, media alerting and emergency management.

The lessons learned from this project have contributed greatly to the development of an overall strategy for information management, information sharing and situational awareness. Following the success of this project, Public Safety has undertaken a number of related projects to integrate alerting and notification with other hosted services, including web-based information management and collaboration tools.

It should be noted that significant intellectual capital was gained from the project, and this will be of great value to all participating organizations in minimizing the effort and cost of performing future trials or creating/extending future public and private alerting systems.

Background

The project was developed in response to an Industry Canada initiative, intended to accelerate technology development and demonstrate commercially viable public alerting solutions. Given the lack of a business case for public alerting services, the unfavourable regulatory environment and the lack of clients with ability to pay, it is clear that a project of this type would be impossible without the leadership demonstrated by Industry Canada.

1 Scope of the Project

The scope and intent of this project was to successfully demonstrate and measure the results of a trial for a system that could be used to manage, trigger, and track the progress of a public alert. A live audience was intended for the exercise, which would simulate emergencies in a specific geographic area.

The component systems of the public alerting process were assembled to

- Enable pre-incident configuration of specific calling lists, to expedite the completion of the alerting process should an incident arise;
- Construct and save these lists through one of two mechanisms: selecting specific names from a provided population list, or selecting residents that lived within a specifically selected radius of an indicated point on a map;
- Enable rapid creation and triggering of an alert that would automatically be sent to one or more indicated calling lists;
- Measure the performance and quality of the overall alerting process; and
- Assemble lessons learned and other knowledge gained from the conduct of the alerting exercise, and provide this in report format to Industry Canada.

1.1 Participating Organizations

The following partners were involved in the project:

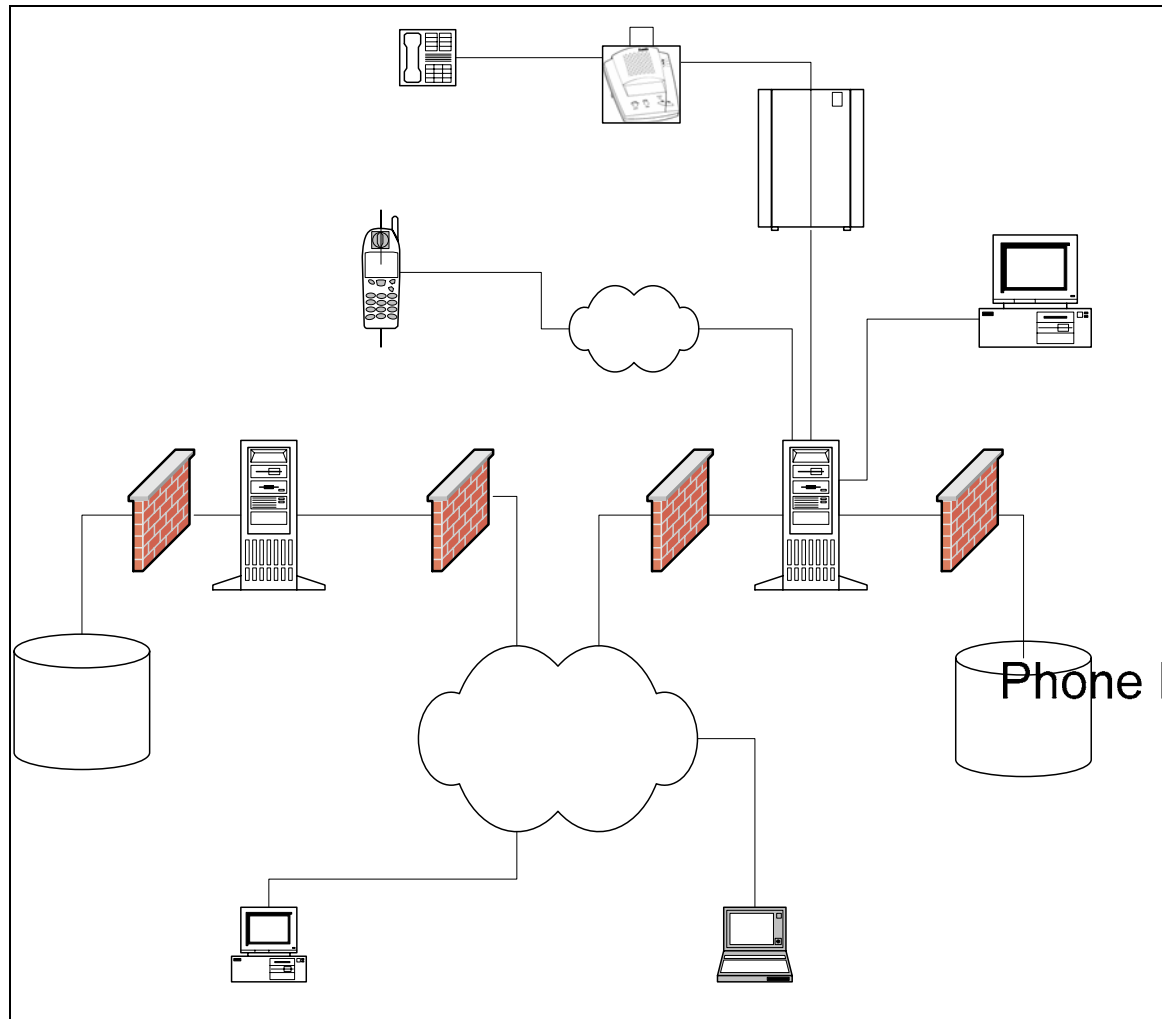
- **Aliant Incorporated.** – Aliant Inc. is the largest telecommunications and information technology services provider in the Atlantic Canadian region. Aliant is the owner of the Multi-Channel Application Service (MCAS), which provides communications and hosting capabilities for applications that are written using the NterWeb platform, including Civic Notification Systems. Aliant is responsible for management, quality assurance, and sustained operations for all production-version applications that are hosted within the MCAS service, and provides front-line support of these applications in the event of any service degradation. Aliant provided significant intellectual capital within the context of these trials, offering consulting services to the partnership and providing planning information for the conversion of these applications to production environments in the future. Aliant also contributed planning information within the context of this report, to assist in understanding the work that would be necessary to convert the product of these field trials to a sustainable “live” environment with sufficient capacity and reliability for public/private use, both within and exterior to the province of New Brunswick.

<p>Geographical Public Alerting System</p>		<p>Public Safety Sécurité publique</p>
---	---	---

- **Caris Limited.** – CARIS is a privately held Canadian company, with its head office in Fredericton, New Brunswick. The company has grown to include offices in the Netherlands and United States. CARIS develops and supports rigorous, technologically advanced geomatics software. Their systems give value to spatial data and empower its customers with information that is meaningful. Caris’ product line enables customers to input, create and manage, and deliver consistently reliable spatial data information and products.
- **Department of Public Safety, New Brunswick** – DPS is the provincial lead department for public safety and security. Within DPS are the New Brunswick Emergency Measures Organization (NB EMO) and the Security and Emergencies Directorate (SED). DPS was the prime contractor, sub-contracted the work, provided project governance and managed the field trials.
- **Xwave Solutions Incorporated** – Xwave Solutions Inc. (xwave) is an information technology company based in Atlantic Canada, and with over two thousand employees in several countries. Xwave offers many information technology services, including systems integration (their main contribution to this project), infrastructure services, managed operations, consulting, and fulfillment services. Xwave has an agreement with Aliant to perform all customizations, integration services, and second-level support on the Civic Notification System. Xwave worked with Caris to augment CNS with interfaces to their mapping client, include additional capabilities for target list selection, and modify other elements of the solution to provide enhanced functionality for the original CNS product.

1.2 Technical Environment and Diagram

The following diagram provides a summary of the technical environment for the delivered integrated system.



- **CNS Tenant User** – Because this is a hosted service, several customers, or “tenants”, may share infrastructure. The Civic Notification System tenant user interacts with and configures recipient lists, calling lists, alerts, and histories of contacts through a standard desktop or laptop running Internet Explorer.
- **Internet Recipient** – If a CNS alert is sent with certain activated parameters, recipients have the ability to visit a specific URL and review the information in the alert that they may have received, or acquire further details on this alert if they are provided by the CNS administrator.

- **Firewalls** – Because the contact information for the target audience may be sensitive, all information storage and application services are housed behind appropriately configured firewalls.
- **CARIS Server** – The CARIS Server hosts the geographic component of the system. This component is based on the CARIS Spatial Fusion web mapping technology platform.
- **CARIS Database** – This information asset contains a local copy of contact information, providing persistent storage for geographically created target lists as well as notification update status information.
- **MCAS Server** – Aliant’s Multi-Channel Application Service (MCAS) includes locally hosted applications and services that employ the Civic Notification System. This server acts as the host for the MCAS service.
- **SQL Server 2000** – Configuration data for potential contacts, configured calling lists, alert parameters, and the histories for previous alert runs, are stored within a Microsoft SQL Server 2000 database.
- **Cell Phone Recipient** – CNS has the capability to call both landlines and cellular phones.
- **Aliant Administrator** – As part of the MCAS hosted service, Aliant provides initial configuration and setup activities, ensures the application is running properly at all times, and reacts appropriately to any noted exceptions. Aliant does not configure or invoke alerts – this is the responsibility of appropriate agents within the Department of Public Safety. (Note: for timeline reasons and because this was a trial, all tests were executed on xwave infrastructure, and administrative services were provided by xwave staff. Any future commercial or production implementations of CNS in New Brunswick would see the participation of the Aliant Administrator.)
- **Public Switched Telephone Network** – Each MCAS server has the capability to employ up to 4 T1’s, or 96 phone lines. Of these, one line of every 24 must be reserved for transport of internal data. Thus, a maxed single-server implementation of CNS can be configured to employ up to 92 simultaneous phone lines (or “ports”) when issuing alerts. The configuration used for these trials employed two T1’s, or 46 phone lines.
- **RTMD Device** – Although these devices were not specifically targeted as contact alternatives in this set of trials, the Civic Notification System has the ability to generate and send alerts to Real-Time Messaging Devices (RTMDs). The Department of Public Safety has successfully rolled out these devices in the Point Lepreau area of New Brunswick, to facilitate delivery of emergency messages to individuals living within the risk areas in the event of an emergency at the local nuclear power plant. Further

<p>Geographical Public Alerting System</p>		<p>Public Safety Sécurité publique</p>
---	---	---

information on this technology can be found at ClassCo's website, <http://classco.com/notification.htm> .

- **Phone Recipient** – Two types of phone recipient are noted for this system.
 - **Alert Recipient** – any person that is to be contacted during an alerting or public notification exercise or event. On answering the phone, these individuals receive a message indicating they should hit a key. Doing this plays the public alerting message, and logs the recipient within the system as a successful contact. Options exist to require the recipient to type in a passcode in order to receive the message – this can be useful, for example, when using the notification system to contact officials in the affected area before a general alert is issued.
 - **CNS Administrator** – When configuring an alert, the CNS administrator has the ability to call him or herself and override the selected alerting message with a recording of their own voice. This recording will then play when the alerting message reaches any targeted recipient.

1.3 Telephony Elements

1.3.1 Impact on Telephony Infrastructure

There were no significant impacts, due to the architecture of the hosting environment.

1.3.2 Other Technical Impacts

Technical impacts that are not necessarily associated with telephony are as follows.

- Some hardware and software is required to host the applications. Minimal specifications for a server that is capable of hosting and executing these components are as follows:
 - Civic Notification System – Wintel server (minimum PIII 500MHz CPU; Windows 2000; SQL Server 2000); 128kbps Internet connection; T1-PRI (public switch telephone connection) via Dialogic card; NterWeb software license; Civic Notification System version 2.1.
 - CARIS Spatial Fusion – Wintel Server (minimum PIII 500MHz CPU;Windows 2000;ODBC compliant Database;32 bit True color graphics card); 128kbps Internet connection; CARIS Spatial Fusion software license
- High-speed internet connections are recommended for the principal users of the CNS/Caris system.
Functional Element Overview

This section provides an overview of the functionality of the solution.

1.4 Elements of the Solution

The Caris/CNS supports both list-based and geographical alerting capabilities. The user can elect to create an alert through either of the following options:

- Selecting the “create from screen” option to build a ‘target list’ of potential alert recipients from the general population of identified residents within the database.

TargetListFilter: Display All Lists Display Screen Lists Display Map Lists

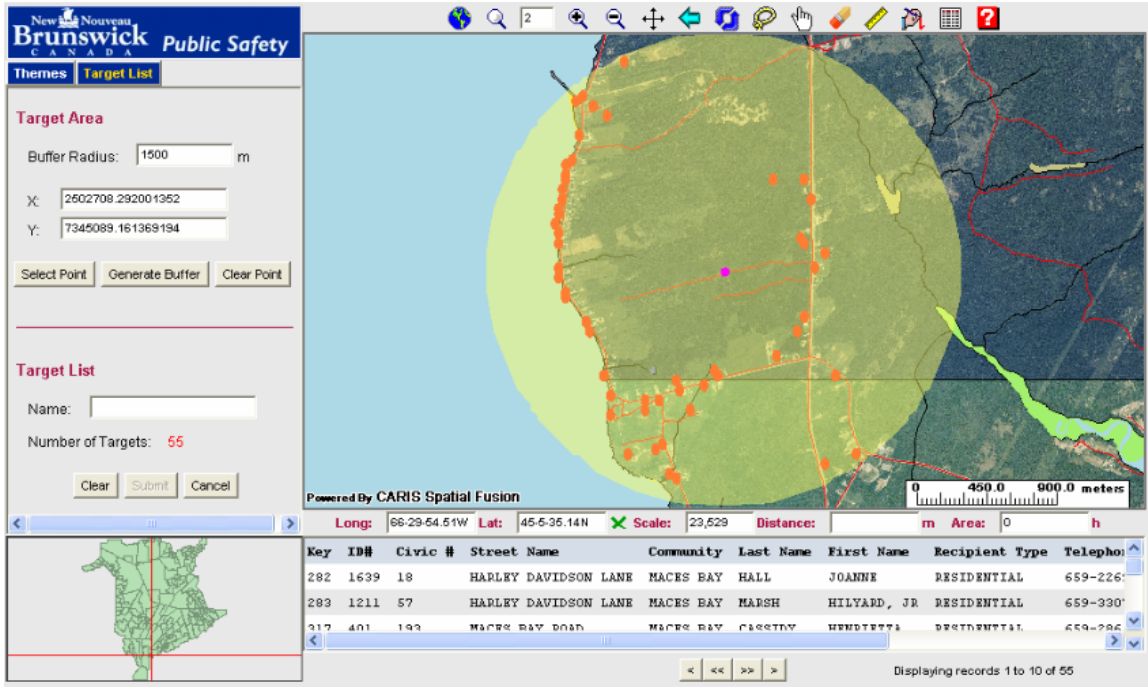
Update Interval:

Target List Name:

Maximum Target List Size:

<p>Select Recipient</p> <p>Name (Type)</p> <div style="border: 1px solid gray; padding: 2px;"> BELDING, DORIS (Business) ▲ BELDING, DAVID (Business) ▼ BELLIVEAU, DORA (Business) BELLIVEAU, JAMES (Business) BELMORE, DONALD (Business) ▼ </div> <div style="text-align: center; margin: 5px 0;"> <input type="button" value=">>"/> <input type="button" value="<<"/> </div> <p><input type="button" value="Sort Recipient By Type"/></p>	<p>Target List Members</p> <div style="border: 1px solid gray; padding: 2px;"> ALLABY, WINDSOR ▲ ALLEN, MARY ARCHILLES, RICHARD AUSTIN, DONALD BAWN, KATHY ▼ </div>
---	--

- Selecting the “create from map” option, which causes a specific geographic region to display in an on-screen map, and selecting a specific region within this map that will create a list of all the residents within the selected area.



Key	ID#	Civic #	Street Name	Community	Last Name	First Name	Recipient Type	Telephone
282	1639	18	HARLEY DAVIDSON LANE	MACES BAY	HALL	JOANNE	RESIDENTIAL	659-226
283	1211	57	HARLEY DAVIDSON LANE	MACES BAY	MARSH	HILYARD, JR	RESIDENTIAL	659-330
317	401	193	MACES BAY ROAD	MACES BAY	CLESTY	HEDETTA	RESIDENTIAL	659-796

- Using the geographic component of the system a buffer with a user-generated diameter can be created around a specific location.
- The potential contacts that fall within this buffer are automatically selected by the system
- A target list of contacts can then be created and passed back to the CNS system
 - During a notification the current status of the individual calls made by the CNS system will be displayed graphically on the map.

1.4.1 Geographic Information Systems

The GIS component of this system provides the following capabilities:

- Create target lists by selecting regions on maps, and automatically capturing into the target list all of the known residents within the selected region;
- Edit an existing target list by displaying it in the map and redefining the selection region;
- Monitor an in-progress notification by displaying the successful, unsuccessful, and untried attempts to target contacts with color-coded symbols;
- Zoom and pan the map to refine the region of selection; and
- Add and/or remove various display layers to the map to facilitate recognition and interaction, including but not limited to roads, hydrology, political regions and orthographic photographs.
- Query Spatial features on the map and retrieve attribute information; and
- Perform distance and area calculations

1.4.2 Integration Methods

A key component of this system’s functionality lies in the methods of integration that enable requests and responses for information to pass from the GIS server component to the alerting engine component. Facets of this integration are described here:

- To enable the Caris and Civic Notification System elements to be hosted on geographically separated servers if desired, the integration method must support the ability to pass information through the firewalls that protect these servers. A SOAP (simple object access protocol) message, which contains information in XML (eXtensible Markup Language) format, is used to pass information between the CNS and Caris hosted servers. SOAP messages contain only informational, not instructional, content and the firewalls can be configured to pass them through to the applications with minimal increased security risks.
- The following table summarizes the message classifications and direction that are used within the integration of the two systems.

Message Name	Originated by	Description
Add Target List	Map Client	Creates a new target list in CNS when a user creates a target area in Spatial Fusion.
Add Target List Response	CNS	Used to identify possible errors during the previous message send
Update Target List	Map Client	Update a target list that was originally created using Spatial Fusion
Update Target List Response	CNS	Used to identify possible errors during the previous message send
Update Incremental Contact Status	CNS	Notifies Caris of incremental changes of a contact status on a target list which is currently being broad casted.
Update Incremental Contact Status Response	CNS	Used to identify possible errors during the previous message send
Update Full Contact Status	Caris	Requests a full status update from CNS
Update Full Contact Status Response	CNS	Used to identify possible errors during the previous message send

1.5 Advantages of this Approach

- **Preservation of system security** – Due to the potentially sensitive nature of the population information that can be used to invoke public notifications, a secure environment is essential. By employing a SOAP interface, a high level of security can be ensured on the participating servers without impacting the ability to communicate vital

<p>Geographical Public Alerting System</p>		<p>Public Safety Sécurité publique</p>
---	---	---

information back and forth. Strong firewall policies can be enforced that still enable SOAP information to reach the applications and servers that they protect.

- **Information security without encryption** – Because both the Caris mapping client and the CNS system rely on local information stores for their tasks, only the elements that link together the individual records within these separated data stores (i.e. the primary key for the data records that are affected by the transaction) are required to be transmitted between the applications. This information, if intercepted during transmission, would not be meaningful to any third party because there is no externally accessible resource that can link the message information to an individual. The message is only useful to applications or persons with the ability to directly access the data stores within the Caris or CNS systems.
- **Servers are platform-independent** – The platform-independent SOAP protocol is able to pass messages between different architectures, which increases the flexibility of this approach when configuring future alerting implementations that may share information with external partners or systems. The information-sharing mechanism used in the CNS/Caris system would not require substantial changes to communicate with other operating systems or platforms.
- **Extensibility** – The SOAP message-handling subsystem was deliberately constructed to be extensible to new message formats if required. If additional future types of communication are required between these elements, such as if the applications are extended to include new functionality, adding new messages to the communications mechanism is not complex.
- **Flexibility for third-party data integration** - The use of CARIS' Spatial Fusion technology provided a great deal of flexibility on the mapping data formats. This was important in leveraging data provided by DPS' own agents together with alternative sources, such as Service New Brunswick, other government departments and the private sector.

1.6 Emergency Measures Organization Reaction

- **7x24 availability with little to no lead time required to create alerts** – The CNS/Caris system can be incurred from any remote web connection, without the requirement to be attached to a network. In the event of a midnight emergency, for example, the administrator can use a home internet connection to create and distribute a notification within moments of receiving word of the situation.
- **Supports multiple channels for alerting** – In addition to standard outbound calling, the CNS/Caris application provides the ability for the notification creator to use email, pagers, cell phones, alternate contact numbers, and Real-Time Messaging Devices (RTMD's). The system also provides a configurable internet site that recipients may visit

to determine further details on the message if required. This combination of alerting mechanisms enables the Civic/CNS solution to reach a greater percentage of the population than a single-channel alerting mechanism. In addition, target lists can be created to immediately notify owners of other possible channels for public alerting, such as media and community television channels, in the event of an emergency. Note that the CNS application can also be customized to extend alerting capabilities to include other electronic delivery systems, potentially including faxing and wireless-based messaging.

- **Avoids delays and management efforts that would be required for running a calling team** – Because the systematic approach of the CNS/Caris application will ensure that all members of a calling list are attempted, little management during the process is required. If the process were to be attempted by a human team, considerable energies would be required to assemble the calling personnel, coordinate the calling lists, and reassign idle callers. In addition, the contacted individuals would more than likely tie up the caller with further questions and requests for instruction, further delaying the process.
- **Minimal effort required to ensure alerting staff are trained** – If a public alerting process is to be used for relatively rare and unpredictable events, there is a strong possibility that it may remain idle for extended periods of time. Risk can be created if the notification process is manually managed and conducted, because the knowledge required to perform the required tasks can slip away unless training programs are instituted to periodically refresh the participants, and special considerations must be made when employee churn becomes a factor. However, with a comprehensive and simple instruction guide, very little training is required to invoke and monitor an ongoing alert for automated systems, provided they are not too complex. (This is one of the reasons why the Caris/CNS system employs a webpage interface and has been made as user-friendly as possible.)
- **Automatic and comprehensive status reporting** – For manual notification processes that would potentially require the participation of a number of people calling contact lists, the process of distributing the lists, organizing the effort, and reporting on the progress of the calls is not trivial. The CNS/Caris solution provides automated tools that, at a glance, can inform the administrator of the status of any outbound contact effort, including the number and locations of successful contacts, number and locations of failed contacts (and information on these individuals), and number and locations of contacts that have not yet been attempted. In addition to in-progress reporting, this information is retained after the completion of the notification process, to enable the administrator to view a history of the tool's effectiveness or use alternate means to reach the list of failed contact attempts. This information could also be imported into other toolsets such as Microsoft Excel, to enable trending and long-term historical studies, if required.

- **Externally hosted services may be able to avoid necessity for “maximum contingency” infrastructure investment** – Hosted environments can be configured to support one or more clients of alerting systems, and the alerting technology used in this trial is no exception. Although this exercise did not concentrate on the construction of a shared infrastructure, it may be possible to create a business model around a shared environment that includes a combination of private enterprise notification applications and governmental systems for alerting. In the event of a critical event that could impact a significant population, the full capacity of the alerting infrastructure, including that which is normally reserved for the private enterprise, might be dedicated to the needs of the public notification system. This would ensure maximum throughput of alerting attempts without a dedicated infrastructure, and is being considered for future versions of the Civic Notification Systems product.

The Department of Public Safety is working with partners to develop a compatible database and a favourable regulatory environment that will enable the use of the Geographical Public Alerting System province-wide.

2 Deployment and Other Future Considerations

2.1 *Remaining Requirements to Provide Production Alerting System*

2.1.1 Resolution of Policy Issues

The following policy issues are expected in a provincial deployment. Comments on resolution approaches and suggestions are noted.

- Applicability of the Protection of Personal Information Act.
- Authority from CRTC to employ 911 data for public alerting.
- Approval of a tariff by CRTC for Aliant Telecomm to enable a public alerting application, employing 911 data.

2.1.2 Technical Issues for Deployment

Deployment of the alerting system is expected to have the following technical implications.

- **Ensuring availability in the event of power outage** – In some cases, circumstances where public notification is desirable may occur when power is not available either at the alert origination point, or within the residences and buildings of the alert’s target audience. For the former, it is important to ensure the alerting solution supports failover/recovery technology, through both the availability of an uninterruptible power supply, and through scheduling and completion of effective backups to enable rapid rebuilding of the notification system. Technical considerations when deploying a production CNS/Caris system may wish to consider “hot spares” or similar methods that maximize the continuity and minimize any down-time for the hosting environment.
- **Readiness and availability of a parallel diagnostic/development environment** – In the event of technical issues with a production solution, support channels should be available in as short a timeframe as possible, and a diagnostic environment should be immediately available to these resources to facilitate their detection and resolution of any problems.
- **Quality of shared data** – Long-term data viability is certainly an issue with any public alerting process or system. Residents within New Brunswick are mobile, and a static list of addresses and contacts will significantly decline in accuracy over time. Thus, a technical requirement of the repository of contacts is the presence of a mechanism to refresh the information it contains. This may take the form of screens accept manually entered corrections (provided for CNS), or, more likely, a complete refresh of residential descriptive information from an external source that replaces all existing information with fresh content. Since the CNS/Caris solution employs to distinct repositories of information for security

<p style="text-align: center;">Geographical Public Alerting System</p>		<p style="text-align: center;">Public Safety Sécurité publique</p>
---	---	---

purposes, the update process must ensure that both the geositional and contact information are refreshed simultaneously.

2.2 Security Measures

To ensure the system remains protected and secure from accidental or deliberate tampering, the following security-related features are noted:

- **User name and password protection** – All users of the CNS/Caris system must log on using a defined user name and non-visible password before being able to address any functionality. To prevent unauthorized use, the user name and password is also required if there is no interaction for a short period, such as if a user steps away from their computer.
- **Different security roles** – The application supports several roles to enable different user classes to access different areas of functionality. These roles include Service Centre Administrator (with the ability to manage all clients ('tenants') that are configured to use the system server), Tenant User (with the ability to invoke alerts, create calling lists, and act as a general user of the system), Administrator (with access to all functionality within the system for a specific tenant).
- **Use of SOAP protocol for messaging between servers** – As previously mentioned within this document, the SOAP message process that is used for communicating between the CNS and Caris applications contains no information that would be meaningful in any context that is external to these applications. In other words, intercepted messages traversing the internet would contain no usable information.
- **Database and telephony server are isolated from the outside world with firewalls**
 - This protection ensures that unauthorized users are limited to the application server component of the architecture, and cannot view or change the database or its information directly.
- **New Brunswick's Provincial Security Program (PSP) is federally compliant.**
 - Provincial policy makes provision for the safeguarding of personal, sensitive and classified information, in accordance with federal standards. All personnel with access to the data are security cleared to federal standards.

2.3 Approach for System Roll-Out

To introduce the system into a public environment with live data, the following steps were employed.

2.3.1 Testing

To ensure the joint application functioned as required, the following testing elements were considered:

- **Assignment of dedicated testers to the project team.** These individuals had the following responsibilities to ensure the application was performing acceptably
 - author a testing approach and test cases to verify all elements of the proposed solution worked properly and according to the approved design;
 - conduct simulations of the application's use;
 - record all encountered problems and forward them to the development teams for resolution; and
 - maintain a log of all encountered issues, problems, and discrepancies between the design specifications and the alerting application.
- **Creation of an appropriate testing "simulation" environment.** Much of the required effort to deliver this solution centred on the construction and handling of the messages that are passed between CNS and the Caris hosted environment. To facilitate the construction of a functioning gateway that could pass this information, xwave and Caris assembled and tested a prototype message handler application.
- **Capacity monitoring while testing.** Technical personnel watched various performance characteristics of the affected servers during the exercises and testing processes to ensure that the system could handle the processing and message loads that simulated a real emergency. In addition, simulation runs were conducted that dialled lists of 'artificial' phone numbers to ensure that large numbers of contacts could be handled.

2.3.2 Public Policy and Communication

By mutual agreement of the partners, it was decided to forego any public announcements, until the system was deemed successful. Now that the project is complete, public communications are permitted and encouraged. Wherever possible, partners will coordinate their messaging concerning the project.

Provincial senior officials, including the Deputy Minister and Minister of Public Safety, have publicly commented on the project and promoted the Civic Notification application to partners.

2.3.3 Deployment

The following general steps would be required for a production rollout of the CNS/Caris system:

- 1) Document and acquire approval on the parameters of the production rollout, to enable appropriate configuration and capacity set-up for the system. Distribution and quantity of contacts within the area of coverage, expectations on the most effective way to reach these contacts with a public notice, and other factors will be considered.

<p>Geographical Public Alerting System</p>		<p>Public Safety Sécurité publique</p>
---	---	---

- 2) Acquire a source of geo-referenced data that represents the population within the area of influence. Review this information for accuracy and timeliness.
- 3) Establish a hosting agreement for the service. This agreement details the telecommunications and application environments that will be provided to the agency administering the service.
- 4) Identify the stakeholders and users of the purchased system, and train the main system user in the functionality of the product, issue reporting processes, and a recurring process to test the application on a periodic basis to ensure it is ready for their use. Verify user systems are capable of running the notification system.
- 5) Review all operational aspects of the existing trial system to ensure that any additional causes for concern for a full production system are mitigated. Review all outstanding issues that were encountered during the conduct of the trial, and resolve those that would be considered undesirable or unacceptable by the system users.
- 6) If required, “clean” the production information that will populate the hosted system, including geo-referenced data. This step includes removing cases where letters appear in numeric fields, verifying the geo-referencing ranges are within acceptable limits, and so on. Author and test the process that will bulk-load this information into the CNS and geo-referenced databases.
- 7) Configure the production hosting environments with the new service, upgrading or enhancing any hosting infrastructure in order to do so. Execute the bulk-load process to move the population data into the system.
- 8) Run a trial with a simulated alert that will hit a preselected “friendly” user in the target audience, to verify all elements of the alerting solution are functional. Create an iterative requirement to test this aspect of the system on a frequent and periodic basis.
- 9) “Turn on” the service.

2.4 Process Steps for Other Communities

This section responds to the following clause in the proposal.

2.4.1 Lessons Learned From This Trial

In addition to proofing the technology and processes for public alerting, this exercise yielded several important “lessons learned”, which are summarized below:

- It is not trivial to gain access to information sources for alerting target areas – It is essential to identify an appropriate source of data and to develop a data maintenance strategy that will satisfy the business requirements of public alerting.
- *An effort is required to prepare/convert data sources for public alerting* – Once the clearance is received to employ a specific information source that describes a target population, there may be a significant amount of work to “sanitize” this data, and convert it to the format used by the loading mechanism for the Civic Notification System and the Caris geospatial engine. The following points will factor into the necessary work to both initially create, and recurrently maintain, this information:
 - *How the information is provided:* Can the necessary records be extracted by directly connecting the application to a privileged source? Is direct access prohibited, and a source-provided “comma-separated value” file is the only way to get the information?
 - *How accurate the data source must be:* How reliable is the original information that is being merged? How old is this information?
 - *How often reloading/updating will be required:* What percentage of the information changes on an annual basis? A monthly basis?
 - *Repeatability of the information source:* Can access to the latest data be assured, or is this a one-time load, with maintenance expected to be performed manually afterward?
 - *Access to the system:* Is there an expectation that the system must provide the ability for the original information’s custodians to access the system and make direct updates?
 - *Consistency of the information:* Is there a potential for bad data within the original information (e.g. letters in numeric fields; phone numbers typed in with separator “-” characters that must be removed; date/time formats that vary according to source geography; fields that are too long and must be truncated)?
 - *Completeness of the information:* For residences without any known contact information whatsoever, how will their records be handled within the alerting system?
 - *Variance in standards within the information:* Do some fields represent different types of data (e.g. postal code / zip-code for cross-border alerting joint efforts)?
- *Time of day has a significant impact on success rate of calls* – Some provision should be made for alternate contact numbers, day / night options or an alternate means of notification for after-hours; Civic Notification does provide for a variety of notification options; ideally this should be addressed through self-subscription.
- *Alerting technologies at the residence can be abandoned if not frequently tested* – Regular testing is required to ensure that alerting appliances are installed; if not regularly used, they are often disconnected.

<p style="text-align: center;">Geographical Public Alerting System</p>		<p style="text-align: center;">Public Safety Sécurité publique</p>
---	---	---

- *Solutions should be designed to attempt the fastest contacting methods first* – CNS/Caris is a multiple-channel application, and can support alternate ways of contacting residents. In those cases where some of the contacts within a calling list have acquired an early warning device such as an RTMD, systems should be designed to attempt to hit these devices first to accelerate overall throughput of alerting messages. An RTMD requires only a single, very fast outbound message and will automatically answer on the first ring. However, a telephone call to a resident will usually take several rings and the duration of the message in order to complete the notification – which can be upwards of one minute. If RTMD’s are preferentially contacted before trying to reach residents on the phone, the number of successful alerts will be substantially higher in the first minutes of the event, which is a desirable outcome.
- *When invoking an alert, separate options should be provided for full-featured use and for first-time-user alert creation* – Although the CNS/Caris system was designed to be user friendly and remotely accessible, circumstances can occur where the system’s principal trained user may not be able to reach the internet and can’t invoke an alert. Generation of a public alert is a relatively complex process, and it is important that any user is prepared to perform the necessary steps as rapidly as possible, particularly if they are an ‘emergency’ designate when the responsible user is unavailable. For this reason, one of two alternatives is recommended to enable alternate users to create alerts without substantially slowing down the process.
 - *Provide CNS/Caris with a “lite” front end, with minimal functionality.* To minimize the requirement for supervision and refresher training, providing a system with a very intuitive, stepwise approach that informs the user of the exact steps to create and release an alert is desirable.
 - *Provide a very simple, stepwise documented process for creating an alert.* As with any flexible system, CNS/Caris supports some features and screen options that are not necessary to interact with when the user is performing a minimal process. To remove these from consideration, it is recommended to ensure the “guest” user has access to a very simple set of step-wise documentation that describes the most critical processes in brief and very clear terms.

2.4.2 Business Model Alternatives for Public Alerting

It is important to realize that the mechanisms employed to provide public alerting differ considerably with geographic area, telecommunications infrastructure, and jurisdiction. For this reason, different business models should be considered when developing an alerting solution. Depending on the circumstances, one or more of these potential business models may be viable:

- Employing a corporate solution that uses 911 data

<p>Geographical Public Alerting System</p>		<p>Public Safety Sécurité publique</p>
---	---	---

- Employing a corporate solution that uses GCADB (Geo-referenced Civic Address DataBase) data
- Employing a self-subscription model that solicits personal data from the subscribers. This could potentially be tied in with other processes that collect personal data.
- Employing a local solution based on public/private partnerships (e.g. partnership for safer communities sponsored by the Canadian Fire Chief’s association) using locally gathered information (e.g. Point Lepreau)

Note that different techniques may be used to collect information that can generate residence or calling lists. For example, Service New Brunswick solicits certain personal information when residents apply to renew their driver’s licenses. An alerting service could be configured to verify collected information at that time, and to populate the information necessary to reach the individual with alerts of interest.

2.4.3 Implementation Steps for Other Communities

The following process is suggested for other communities within New Brunswick to adopt the Public Alerting system and process:

1. *Evaluate information sources.* Due diligence must be conducted to determine if population and geospatial information is available for the potential target regions. If so, the alerting initiative must determine if this information can be shared for this purpose. Various factors that must be resolved include agreement with the supplier/maintainer to protect the privacy of those named in the data, compensation for use to those who assemble and maintain this information, and schedules for complete information refreshes and/or incremental changes.
2. *Evaluate alerting conditions and parameters.* It is essential when planning and configuring an alerting system to understand the capacity and throughput requirements for the solution. These should be looked at from a “worst case” scenario basis – for example, how many contacts must be made in the first hour after a situation is declared where a river is rising rapidly. This will help determine the costs for the minimal stand-by infrastructure that will be required to service this capacity.
3. *Acquire sources of financing for the deployment and maintenance of the system –* Economics of maintenance may be a challenge when throughput requirements are high for an alerting solution. Creative financing, subscription models, private/public participation, shared infrastructure, and other ways to drive the cost per contact down for both idle and utilized capacity should all be examined.
4. *Determine stakeholders and user teams –* To guarantee success in delivery, the implementation of the solution MUST be looked at as a full project composed of discrete,

time-sensitive tasks. As a result, it is essential to select an extended project team with stakeholder representation from each involved agency - the information providers, the system maintainers/deployers, and the user community all must assign members to the project with a clear understanding of the value the system will provide. Strong project management and communication coordination is essential to ensure the solution meets the requirements of all of these agencies.

5. *Determine infrastructure arrangements* – One of the first steps in the actual construction of the solution is to understand the impacts on the existing telecommunications and hosting environments that will house the completed system. Again, capacity planning is an important component of this phase, and senior technical participation should be actively sought to ensure the costs, expectations, and timeframes for the deployment are accurately estimated.
6. *Initiate the adaptation project* – A formal project is conducted to implement the alerting solution. Note that the complexity of this project depends entirely on a combination of the expected capacity/throughput of the solution, quality of the target population data, list of extensions or additional functionality that is sought for the new implementation, and availability and involvement of the project stakeholders.
7. *Train staff and provide documentation* – The implementation project should also address training needs for the staff that will be interacting with the solution, delivery of appropriate documentation, and announcements of the service once it is complete.
8. *Establish a maintenance agreement with all affected parties* – To ensure the system remains at the desired state of readiness, agreements should be defined that assign specific responsibilities to participating organizations in the event of outages, failed data refreshes, requirements for business process change in the future, or downgraded performance repairs. Terms should be decided on a maintenance agreement with those responsible for the system and its component applications, well in advance of any live deployment.
9. *Test the system* – If possible, the system should be tested with live data. It is understood that this might not be appropriate for certain communities, but at minimum, it is strongly recommended that a “friendly” test bed of target recipients be contacted under realistic conditions (such as through a simulation exercise) to ensure the system is operational and performing as per expectation of throughput and functionality.
10. *Initiate a Public Education Program* - It is necessary to have a formal program that explains the system and how it fits into the home and community emergency plan.

11. *Establish Governance* - An operational system must be competently managed, with appropriate governance and accountability; establish program ownership and develop the operational policy, before deployment.

12. *Deploy the system* – The decision to turn the system on should not be automatic. It is recommended that a formal evaluation of the system be conducted before electing to ‘go live’. This is usually performed as a high-level stakeholder meeting that checks the readiness of each project participant, ensures all necessary communications have been performed, and reviews the results of quality and functional testing. From this, a “go / no-go” decision is reached to convert the alerting system to production status.

2.5 Implementing Public Alerting System in Other Provinces

2.5.1 Steps Required to Implement in Other Provinces

Should other geographies within Canada elect to pursue public alerting technologies, the following additional factors should be considered:

- Policy Framework (Privacy Legislation; Regulatory Environment; Policy)
- Program Management (Ownership; Governance; Operational Policy)
- Telco Partner (Service Agreement; Business Agreement)
- Data (Sources; Authorities; Quality Assurance; Maintenance)
- Friendly Test Environment (Trusted Agents; Sample Population; Early Adopters)

2.5.2 Hosting vs. Licensing Approaches

This section describes the business models that can potentially be used to provide a Public Alerting service with the Caris/CNS solution.

Two alternatives are available – a hosted service, and a customer premise model that involves the purchase of licenses and possibly maintenance agreements.

Alternative	Description	Advantages
Hosted Service Model	Customer (tenant) enters into a hosting agreement with an external partner, who provides hosting, support, and configuration services on behalf of the tenant.	<ul style="list-style-type: none"> • No infrastructure required • Significantly less expensive over time – includes all costs for application, hardware and telecommunications. • 7x24 experienced support is available • Changes are incurred through a rigorous, quality controlled process.

		<ul style="list-style-type: none"> • Possibility exists for upgrades of software to be supported through a migration path. • Shared service models, where separate customers bundle their changes, may be considered to further reduce costs compared to the self-hosting alternative
Customer Premise Model	Customer owns infrastructure and runs the Caris/CNS system themselves	<ul style="list-style-type: none"> • Customer may be able to reuse some of the customer's existing infrastructure to reduce hosting cost. • Customer has exclusive control over infrastructure.

3 Noted Issues of Concern

Miscellaneous other observations and findings are discussed in this section of the report.

- **Interest in regional Public Alerting is high** – There have been a number of events that have occurred in the summer and autumn of 2003 that have increased the prevalence of emergency and alerting communications mechanisms in the minds of the general public. Recent events include the impact of Hurricane Juan on the Halifax region, the blackout in Ontario and the United States, and intense flooding and forest fire dangers within the interior of British Columbia. As a result, interest is significant in technologies that can facilitate public alerting and response. Organizations with mature solutions to the problem of timely public alerting have significant opportunities to either produce revenues as a service provider, or defer costs for their own solutions, by transferring their intellectual capital to those in need of such solutions. This trial has significantly increased the capability of the participants to operate in the field of public alerting.
- **Proponents must be capable of linking public alerting to governmental priorities** - In the absence of an obvious need or regulated requirement, governments will not likely view public warning as a policy priority. By linking public warning to public safety or public security policy objectives (Amber Alert, for example), it may be possible to engage senior government officials and secure the necessary support.
- **Strategic partnerships between Government and Industry are required to advance the cause of public alerting** – In any venture with a diversity of business and public interests, it is vital to find the common ground that provides a solution of mutual benefit. No one party can do this alone. Lack of capital is another factor, this can be mitigated through clever financial models such as revenue sharing and strategic investment funds.
- **A favourable regulatory environment is a predecessor for success** – Broadcast alerting is not specific to the areas at risk. The advantage of geographical alerting is that it targets those at immediate risk from an event. The challenge is to know who is at risk, where they are and what number to call. The best solution is to employ 911 data; regulatory approval and a tariff for the use of 911 data are necessary pre-requisites. Tariff must be affordable, or no party will be able to deploy such as system.
- **Protection of privacy is a significant factor in the perception of public alerting** - Public confidence and government approval are dependent on the Program Owner's ability to comply with privacy legislation and regulated requirements with regard to privacy. Proponents must be prepared to demonstrate that they are compliant. Governments must be prepared to demonstrate that they have adequate oversight.
- **Mitigating risk is a strategic element of public alerting**- Risks apply to both the public and private sector. There is a requirement for a degree of indemnity in the event that an

<p>Geographical Public Alerting System</p>		<p>Public Safety Sécurité publique</p>
--	---	--

alert is not received by part of the target audience. These risks can be of particular concern for the private sector. For the government partner, it's what happens if you do NOT call your citizens.

- Public Alerting must be a long-term viable business to attract the private sector as partners** The cost/benefit analysis must show public alerting as a profitable long-term venture in order to attract the attention of corporate elements that may be interested in investing in, and creating, a reusable practice. Essentially, champions of the technology and process are required, with a demonstrated sustained commitment to making the process succeed in the long term. The recommended business strategy is to consider *public warning* as a sub-set of *communications*, which includes related business requirements, such as media alerting, security alerting, information sharing, notification of officials and so on. A single strategy, and application, addressing all of these has a better business case and more paying partners than a solution for public alerting alone. This is in fact the New Brunswick Model.