

Planning for the Unexpected: Protecting Assets, Securing Services

August 7, 2002

Speaker of the House of Representatives, Walter Freed
President Pro-Tempore of the Senate, Peter Shumlin
Governor Howard Dean, M.D.

Gentlemen:

Today, nearly a year after the tragic events of September 11, it's time to take stock of the progress Vermont has made in planning for the unexpected. And, it's time to assess the challenges that remain to protect the State's assets and secure services for Vermonters.

In the past several months my Office has issued a number of special reviews and bulletins focused on improving the State's safety and security, whether in the event of a radiological emergency at Vermont Yankee or an act of sabotage against the State's computer network.

As a result, we evaluated existing statutes and procedures in place should a catastrophic event disable major services of State government. We believe that prudent planning is the proper approach for Vermont.

I concur with Secretary Hoyt's recent comments that Vermont needs to have an adequate business continuity plan in place to assure its citizens that emergency and basic services will be uninterrupted by disaster. I'd like to offer a few suggestions to achieve this mutual goal.

I believe Vermont would benefit from the following improvements in four key areas:

- Data backup of all key documents and applications;
- Safe and secure storage of all documents;
- Adequate succession of all elected officials to ensure the day-to-day business of the State is not impacted; and,
- Enterprise-wide security protocols over all of its information technology (IT) assets, including better coordination of these activities with public- and private-sector partners.

In the event of an act of war against the United States or Canada, Vermont appears to have appropriate statutory mechanisms in place (20 VSA Ch. 7 §§ 181-192) to allow for an orderly succession of officers within each of the three branches of government.

The statutes also specifically state that municipalities shall create an order of succession in the event of such an emergency (20 VSA Ch. 7 § 186). The statute pertaining to local officials states, in part: “The officer shall designate a sufficient number of persons so that, including deputies, there will not be less than three emergency interim successors.” Copies of these plans are to be placed on file with the County Clerk. When contacted, staff at each of the 14 Superior Courts said no such plans had ever been placed on file.

Vermont’s statute, as currently written, fails to account for additional emergency provisions in the event of a major catastrophic event, either natural or deliberate, that cripples several branches of government at once. The main emergency powers and continuity of government statute (20 V.S.A. Chapter 7) was written in 1959 and updated in the 1960s and early 1970s. At that time, information technology was *not* used to conduct a majority of the State’s business.

My Office’s special review of Vermont’s data security and recovery policies, issued on February 19, 2002, recommended a number of efforts to improve the management and oversight of information and security. I have included some of them below, and have added others to help in the development of steps to improve performance and readiness.

1. Data Backup

Governments of all sizes are re-evaluating their business continuity plans as a result of the tragic events of September 11. While Vermont did undertake such efforts prior to the Year 2000 conversion, many of those plans are incomplete or inadequate, according to a review of several departments by my Office and KPMG’s Risk and Advisory Services Practice.

Vermont’s Chief Information Officer (CIO) should give departments strong guidance on ways to ensure that key information on their main systems are backed up regularly and stored in a secure location away from their central administrative offices. This way, in the event of a major emergency when large portions of the State’s computer network are down, key services could still be provided.

These services include key functions at the Department of Finance and Management, the Department of Health, the Department of Taxes, the Department of Corrections, the Department of Prevention, Health Assistance and Transition, and the Department of Public Safety, the Agency of Administration, the Agency of Transportation, as well as the Secretary of State and Office of the State Treasurer.

Combined, these databases record the birth, marriage, death and health of nearly all Vermonters. These various agencies and departments also track the internal records of State government, including several functions that directly relate to the State’s ability to collect taxes, deposit payments, and issue checks to employees and vendors. I know that Commissioner Torti is already at work on a plan to house data away from the two concentrated areas of government offices – Montpelier and Waterbury.

Recommendation: Vermont should develop enterprise-wide protocols and policies for backing up systems and storing backup data, and protecting the systems and data from unauthorized access.

2. Secure Storage

Currently almost all of the State's public records are stored in a single warehouse in Middlesex. The remaining records are retained by various departments, which provide their own, limited on-site backup.

My Office assessed our current policies to determine where improvements could be made. We have since instituted a stronger policy regarding the electronic storage of key work papers and other Office documents.

Recommendation: The Agency of Administration should develop stronger secure storage policies and protocols that allow for the use of digital technology to store key records electronically. This would save on physical space, and allow for key personnel to retrieve necessary information if the main access point is destroyed or damaged.

The Office of the CIO should provide statewide direction, policies, guidelines and monitoring to ensure each department has adequate IT security. Further, agencies and departments should:

- **Develop and test disaster recovery plans that are communicated to all personnel and tested periodically;**
- **Implement protocols related to data backup, program changes, passwords, and prompts for changing passwords on all systems – including the new VISION accounting software program;**
- **Assess server security, power backup and the risks of not making changes; and,**
- **Examine the cost/benefit of moving critical applications to more secure server platforms.**

3. Succession of Officers

The Statute is clear about the succession of the governor's office, yet it leaves little direction regarding the succession of other Constitutional Officers, and the Legislature - in the case of a catastrophic event in the capital city when lawmakers are in session.

Just as crucial, however, are internal policies at each department regarding appointed Secretaries, Commissioners and Directors. The State would benefit from a uniform

approach to departmental succession in order to ensure the core function of government does not wane during a major emergency.

For example, Florida has an explicit “continuity of government” or COG plan that outlines the chain of command during an emergency. This state’s plan covers everything from the succession of officers in each of the three branches of government to the safeguarding of essential records and the protection of government resources. The outline of Florida’s COG plan is available online at www.dca.state.fl.us.

The key function of any COG plan is to offer reassurance to citizens that essential services will be available and delivered during a true emergency. Measuring the success of these plans is critical. According to RAND, a non-profit think tank that specializes in COG plans, the main test of any such plan is “the degree to which the consequences of emergencies can be mitigated and the speed with which government functions and services can be restored.”

In addition, our Office noted that 20 V.S.A. Ch. 7 § 186 provides guidance for municipalities to develop succession plans for elected and appointed officials. These plans are to be updated annually and kept on file with the County Clerk. Our testwork, which included on-site visits and telephone surveys, revealed that no such plans are on file at State’s 14 Superior Courts.

Recommendation: The General Assembly should adopt legislation that clearly articulates a uniform approach to the succession of Constitutional officers and departmental heads.

The Agency of Administration should establish measurable goals to evaluate the performance of these security plans annually, as well as incorporate a spot security inspection program.

Municipalities should comply with statutory guidance that provides for the creation of plans detailing the orderly succession of officers in the event of an emergency. These plans should be kept on file with the County Clerk.

4. Guarding IT Networks from Sabotage

The events of September 11 have made public and private sector managers re-examine the tools they need to assure their information systems are safe from sabotage.

In Vermont, a chapter of the national InfraGuard organization has formed a collaboration between the public and private sector to help monitor the type and volume of visitors to their individual organization’s websites. In short, it acts like a Web-based Neighborhood Watch. This chapter originated as, and continues to be, an organization and resource for the Vermont information security community and affiliated with the [Vermont Information Technology Center](http://www.vtinfotech.org) at Champlain College (www.vtinfotech.org).

According to its website, “All InfraGard participants are committed to the proposition that a robust exchange of information about threats to and actual attacks on these critical infrastructures is an important element for successful infrastructure protection efforts.

The goal of InfraGard is to enable that information flow so that the owners and operators of infrastructure assets can better protect themselves and so that the United States government can better discharge its law enforcement and national security responsibilities.”

Vermont InfraGard Charter and Mission Statement: “The Vermont InfraGard chapter comprises working professionals and others interested in the field of information security in the state of Vermont. The group is committed to acting as a communications coordination facilitator and information resource within the state. We are organized under the FBI InfraGard program in order to participate with other similar groups on a national basis, but our activities are not limited to InfraGard ‘members.’ Our goal is to facilitate communication and share expertise amongst our peers.”

State government should become an active partner of this organization, and use it to conduct an Information Assurance Training/Awareness. For more information about Vermont’s InfraGard chapter, visit its website at www.vtinfragard.org.

As part of the national InfraGard program, the U.S. Department of Defense has identified several steps to succeed in information assurance planning.

Those steps are to:

- Implement detailed information assurance policies and plans to provide automated detection, differentiation, warning, response and recovery against intrusion, malicious activity, or information warfare attacks;
- Perform comprehensive risk assessments of critical information infrastructures to determine the level of vulnerabilities, susceptibilities, and risks that exist within those infrastructures; and,
- Develop an incident reporting system to coordinate detailed incident information to and from the lowest echelons of government.

A recent report conducted for the National Association of State Chief Information Officers (NASCIO) outlined a similar framework to ensure that States are prepared to not only defend their own infrastructures, but are part of a greater web to gird up the nation’s telecommunications and information technology infrastructure.

In its report, *Public Sector Information Security: A Call to Action for Public-Sector CIOs* available to be downloaded at www.nascio.org, the authors outline 10 main steps that States can take to initiate improvements that allow for better coordination and cross-state tracking of information.

They include:

- Develop security metrics that accurately measure unwanted intrusions, security breaches, penetrations, and vulnerabilities;
- Deploy automated and manual security technologies based on asset inventories and application criticality, including security levels derived from the enterprise architecture for IT;
- Develop a state security portal that integrates with emerging technologies for emergency response such as intelligent roads and radio-frequency infrastructure; and,
- Develop and model state legislation that allows local, state and federal entities to confidentially share security incident reports.

Recommendation: The Agency of Administration should, together with the Vermont InfraGard chapter, develop a blueprint to ensure that Vermont's security infrastructure protects the State's IT assets. The NASCIO report may serve as an important resource.

The Agency of Administration should implement IT security measures that are designed with specific outcomes so they can be evaluated for performance. Security policies should be independently tested on a frequent basis.

I know that Secretary Hoyt and Commissioner Torti are making progress on these important issues and I hope our Office's suggestions prove useful.

Sincerely,

Elizabeth M. Ready
State Auditor

cc: Sen. William Doyle, Chair, Senate Government Operations Committee
Rep. Cola Hudson, Chair, House Government Operations Committee
Kathy Hoyt, Secretary, Agency of Administration
Tom Torti, Commissioner, Department of Buildings and General Services
Howard Rice, Jr., Director, Division of Emergency Management
B. Michael Gilbar, Director of Administrative Services, Vt. League of Cities and Towns