

Cyber Security Protecting New York State's Critical Infrastructure

The Cyber Security Task Force

June 2003

Table of Contents

[Executive Summary](#)

[The Need to be Prepared](#)

[Cyber Security Task Force](#)

[Office of Cyber Security & Critical Infrastructure Coordination \(CSCIC\)](#)

[Multi-State Information Sharing and Analysis Center \(ISAC\)](#)

[Public/Private Sector Cyber Security Workgroup](#)

[Public/Private Sector Cyber Security Workgroup - Deliverables](#)

[Conclusion and Recommendations](#)

Executive Summary

The people of New York State have responded heroically to the terrorist events of September 11, 2001. As we respond to the physical nature of terrorism, we cannot lose sight of the realities and threats posed by cyber attacks. Nor can we ignore the devastation natural disasters have on our technology infrastructure. So whether man-made (either intentional or inadvertent) or by acts of nature, cyber incidents on our critical infrastructure can be devastating.

New York State's biggest challenges are preventing-and when necessary, responding to--attacks on public and private critical infrastructure (physical or cyber). Those critical infrastructure assets which are linked together by networks and systems hold additional challenges for us in our efforts to protect them.

As technology continues to evolve, a greater percentage of the primary operations of sensitive utility, transportation, communications, financial services and other critical infrastructures will continue to shift from manual to on-line controls. Accordingly, the threat posed by someone determined to do harm will grow.

New York State is developing a comprehensive approach to cyber security in this new era--to inventory our critical infrastructure assets, and identify the vulnerabilities of and potential threats to these assets through the use of technology. The State's approach will encompass four phases: prevention, detection, response and recovery. In order for us to effectively address these areas, the relationship between the public and private sectors, as well as that between the civil and law enforcement sectors, must be strong and collaborative.

Recognizing the potential threat, Governor George E. Pataki announced on March 8, 2002, the formation of a Cyber Security Task Force, under the leadership of James K. Kallstrom, Senior Advisor to the Governor for Counter Terrorism.

The Task Force was mandated to evaluate the State's critical cyber-infrastructure, identifying potential means of cyber attack, and recommending security practices for private industry, State-operated information systems and the general public. The diversified skills and knowledge embodied in the Cyber Security Task Force, encompassing State agencies, the private sector and academia, is enabling the State to assess and prioritize the critical cyber-infrastructure of greatest concern.

The first meeting of the Cyber Security Task Force was conducted on April 16, 2002 to discuss the mission, objectives, and deliverables of the Task Force. At the following meeting, held on May 30, the Task Force established two separate working groups to further define the deliverables assigned to each workgroup: a public workgroup, charged with advancing public knowledge and responsibility for cyber security; and the Public/Private Sector Cyber Security Workgroup, charged with developing standards of preparedness and methods to inventory and assess critical infrastructure assets contained within industry sectors.

This Report addresses the initiatives of the Public/Private Sector Cyber Security Workgroup and the New York State Office of Cyber Security and Critical Infrastructure Coordination, which coordinates the activities of the Workgroup. The mandates for this Workgroup are on-going - and will continue - in order for New York State to be consistently ready to deal with the new era of cyber threats. Under Governor Pataki's leadership, New York won the race to be prepared for the Y2K date change. This race had a definite end date (January 1, 2000). However, in our on-going effort to be cyber ready, there is no end date. Therefore, the Public/Private Sector Cyber Security Workgroup will continue the valuable work already underway.

New York is a national leader in the ongoing efforts to be prepared. The efforts of the Public/Private Sector Cyber Security Workgroup, which are discussed in this Report, are an important component in keeping the State moving forward toward cyber readiness.

The tragic events of September 11th, 2001 were unlike anything we had experienced before. There will be - and must be - much change as we move into this new, uncharted and unforeseen world. Cyber security and critical infrastructure coordination requires an entity with a single focus dedicated to addressing these highly specialized needs.

The New York State Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) was established in September 2002 as a means to address the State's cyber readiness and resilience. This Office is led by William F. Pelgrin and coordinates closely with the Director of the New York State Office of Homeland Security, James W. McMahon.

CSCIC is responsible for leading and coordinating NYS' efforts regarding cyber readiness and resilience; leading and coordinating geographic information technologies, especially in emergencies, where CSCIC is the single point-of-contact; coordinating the process by which State critical infrastructure data is collected and maintained; expanding the capabilities of the State's cyber incident response team; and monitoring the State's networks for malicious cyber activities.

The efforts of this Office will require tremendous cooperation and input from a variety of entities. This initiative is focusing on building strong relationships between and among the public (federal, state, and local) and the private sectors to best ensure our State's cyber readiness.

The efforts of CSCIC will build on the foundation already established in NYS to help the State prevent, detect, respond to and recover from cyber-based incidents that threaten our State's critical public and private assets.

The Need to be Prepared

The people of New York State have responded heroically to the terrorist events of September 11, 2001. As we respond to the physical nature of terrorism, we cannot lose sight of the realities and threats posed by cyber attacks. Nor can we ignore the devastation natural disasters have on our technology infrastructure. So whether man-made (either intentional or inadvertent) or by acts of nature, cyber incidents on our critical infrastructure can be devastating.

In today's world, we rely on technology and the Internet for a myriad of information, transactions and communication-- at home, in school and at the work place. The number of Internet users worldwide is expected to rise from 445 million in 2001 to 709 million in 2004. [1]

While this ubiquitous technology provides tremendous positive opportunities, there are still a number of vulnerabilities and risks associated with technology systems. According to the Computer Emergency Response Team at Carnegie Mellon University, during 2000, approximately 22,000 cyber incidents were reported. In 2001, more than 52,000 were reported, more than 82,000 were reported in 2002, and more than 42,000 in the first quarter of 2003 were reported to Carnegie Mellon [2]. New York State is experiencing the same high growth in cyber attacks. Code Red I and II worms impacted ten State agencies directly and caused data traffic problems across State networks. During the NIMDA worm crisis, nearly all State agencies were required to temporarily suspend connectivity to their external e-mail systems and five agencies were infected.

During our preparation for the Year 2000 date change, New York State was acutely aware that cyber attacks, whether by malicious acts or accident, can seriously disrupt critical information flows in communications, capital movement and allocation, as well as the operation of critical utilities that affect the lives of millions of New Yorkers.

New York State's biggest challenges are preventing-and when necessary responding to--attacks on public and private critical

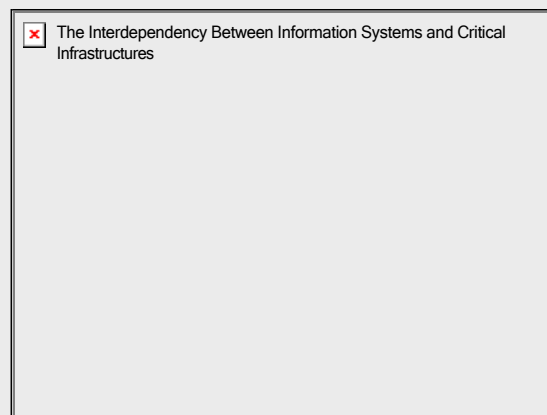
New York State's biggest challenges are preventing and when necessary, responding to attacks on public and private critical infrastructure (physical or cyber). Those critical infrastructure assets which are linked together by networks and systems hold additional challenges for us in our efforts to protect them.

As technology continues to evolve, a greater percentage of the primary operations of sensitive utility, transportation, communications, financial services and other critical infrastructures will continue to shift from manual to on-line controls. Accordingly, the threat posed by someone determined to do harm will grow.

What makes cyber threats so fearful is the fact that:

- Cyber attacks can originate from anywhere as more and more people have access to the Internet and other publicly-connected networks. Connectivity between information systems that are at the heart of cyberspace is spreading worldwide and becoming universal, with millions of new entry points every year; [3]
- The technology to launch such cyber attacks is relatively inexpensive;
- Sophisticated computer expertise is less important since the technology is less complicated to use and the knowledge is readily available;
- There is a shortage of qualified and trained personnel to detect and respond immediately to these attacks; and
- There are no current single formal means of signaling an alert to the rest of the country.

The image below depicts the crucial role that information systems play in the interconnectivity of our critical infrastructure. Additionally, there are many dependencies and interdependencies between and among the different sectors. For example, if an electrical grid goes down, all critical infrastructures within that grid may be negatively impacted--bank ATM machines, "Amber alert systems," elevators, or air-conditioning could be interrupted or cease to function.

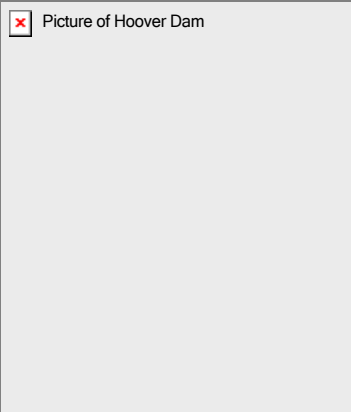


Cyber security threats have tremendous potential to inflict financial disruption as well:

- U.S. companies spent \$12.3 billion to clean up damages from computer viruses in 2001. [4] According to mi2g, economic damages in 2003 by digital attacks is now between \$34.7 billion and \$42.4 billion worldwide.
- 2002 CSI/FBI survey found that 90% of companies surveyed admitted to a successful computer breach in the preceding year, resulting in hundreds of millions of dollars in quantifiable loss. [5]
- Mass cyber-events such as "I Love You" Virus, Melissa Virus, Code Red, and NIMDA caused hundreds of millions of dollars in damage. [6] The SANS Institute reports that more than 86,000 Internet hosts are thought to have been compromised and used to propagate the NIMDA worm on September 18, 2001.
- A Russian hacker in St. Petersburg broke into a major bank's computer system in New York and manipulated millions of dollars by electronically transferring the money to other banks around the world. [7] The majority of the funds were recovered, however, it is important to note the tremendous amount of dollars in losses--that were not recovered--that the bank incurred due to staff time and resources devoted to dealing with this event.

Cyber attacks impact power and energy companies as well, and some experts say that these entities, along with the Financial Services and High Tech sectors, are experiencing increases in computer attacks.

It could be easier to attack a dam by hacking into its command and control computer network than it would be to obtain and deliver the tons of explosives needed to blow it up. [8]



As the world faces the increased possibility of cyber terrorism, the ability of our law enforcement community to respond becomes even more critical. Understanding the latest in forensic analysis capabilities and having the necessary tools and resources to respond is paramount for the law enforcement community in this high-tech era. Law enforcement has, and will continue, to play a pivotal role in incident response. As we go forward, the State must ensure that it has the capability to respond adequately to a cyber attack. We will more fully describe and analyze these activities as we address the Public Safety/Emergency Preparedness Sector.

Our potential threats can come from almost anywhere by anyone -- from sophisticated hackers, to employees, acts of nature, inadvertent incidents, as well as by criminals and terrorists. We don't have to look at the international scene to discover potential sources of cyber attacks; the potential is right here at home. A single individual, operating out of a private residence and using commercially available hardware and software, is capable of perpetrating acts which bring about the economic and social chaos described above.

In fact, one area of high concern is the ability to exploit the vulnerability of commercial software products as a means to spread dangerous viruses. In a survey of 1,000 individuals responsible for their organization's information security, across a variety of industries, virus infection was the single largest cause of serious security breaches (accounting for 33% of the most serious breaches). [9]

The advances in technology enable cyber-crimes to be committed more easily, by less sophisticated users, and can have far-reaching effects. "Cyberspace" has been compared to the Wild West, with unlimited potential for both good and evil. The RAND organization, a non-profit research institution, notes that "in the headlong rush to 'connect,' little attention is being paid to gaping holes in the security of these information networks." [10]

The issue of cyber security is not solely related to recent events. In fact, if September 11th never happened, the issue of cyber security would still be very real and the threat to the Nation's critical infrastructure would still be significant. September 11th highlighted all too sadly the extreme when the convergence of human, physical, and cyber assets are destroyed. In New York, State and City agencies lost over 2,200 telecommunications circuits from a single location when 140 West Street was damaged. Verizon reported that "the terrorist attacks in New York destroyed or disrupted 200,000 voice access lines, 100,000 business lines, 3.6 million data circuits and 10 cellular towers." [11] Clearly, damage to physical assets can impact cyber assets. We must also be aware that not all cyber security events are intentional. There are accidents that can cause major disruptions and even catastrophic failures. RAND notes an instance of a farmer accidentally cutting a fiber-optic cable while burying a dead cow, which resulted in the closure of four major air-traffic control centers for over five hours. [12] So, this physical event-even though unintentional-had a negative impact on the cyber infrastructure.

The potential impact of cyber-related incidents (foreseen and unforeseen, internal and external, intentional or accidental) could cause loss of life, and/or disruption of essential services and critical operations.

New York State is developing a comprehensive approach to information security in this new era--to inventory our critical infrastructure assets, and identify the vulnerabilities of and potential threats to these assets through the use of technology. The State's approach encompasses four phases: prevention, detection, response and recovery. In order for us to effectively address these areas, the relationship between the public and private sectors, as well as that between the civil and law enforcement sectors, must be strong and collaborative.

In order to build strong working relationships that facilitate the free exchange of valuable and timely information between and among these diverse groups, the State needs to ensure that there are strong laws that protect the confidentiality of critical infrastructure data. We must be able to protect this information from unauthorized disclosure. While more needs to be done, one of the steps New York State has taken to address this is through an amendment in 2001 to the New York State Freedom of Information Law to permit agencies to deny access to records that, if disclosed, would jeopardize an agency's capacity to guarantee the security of its information technology assets. [13]

The State's critical infrastructure and assets, public and private, are as vast and diverse as the State's topography. The more prominent sectors include the following:

1. **Telecommunications**: including Signaling System Seven (SS7) and 911 communications;
2. **Utilities**: electric, gas, water, waste, steam, nuclear;
3. **Government**: towns, villages, cities, counties, school districts, state, and federal;
4. **Public Safety/Emergency Preparedness**: police, fire, emergency managers;
5. **Health**: hospitals, nursing homes, pharmacies, health clinics, clinical and environmental laboratories; adult homes;
6. **Financial/Economic**: stock exchange, banks, investment firms, payment and clearing systems;

7. **Transportation**: signal/guidance systems of rail, airline, bus, trucking, shipping/handling companies;
8. **Education and Awareness**: K-12, higher education and general public awareness;
9. **Food**: agriculture and dairy processing industry;
10. **Chemical Manufacturing**: including distribution and storage;
11. **General Manufacturing**: including distribution and storage;
12. **Research and Development**; and
13. **Technology**.

The public and private sector must work together to protect the State's critical infrastructure and assets, as well as the interdependencies, by being cyber-ready.

The State needs to be prepared if one of the following scenarios materializes.

- Air traffic control equipment malfunctions;
- Computer controlled medical life support equipment is altered to function improperly, administering inadequate or excessive doses of critical medicine;
- Patient records are altered, potentially resulting in misdiagnosis and loss of life;
- An orchestrated hoax reporting of disease outbreaks that would mask a true attack by scattering resources across the State;
- Heating, ventilation, and air conditioning systems are modified to circulate harmful gases within a large office complex, containing a population equivalent to a small city;
- 911 telephone communications are interrupted;
- Electrical blackouts occur;
- Power dam water flow is modified to allow downstream flooding incomparable to any previous natural disaster; or
- Financial markets are disrupted.

In order to be prepared, we must employ a coordinated approach, uniting local resources with those at the State and national level. Protection of critical infrastructure has become a top priority nationwide.

On October 16, 2001, President Bush issued an Executive Order to ensure protection of information systems for critical infrastructure. In February 2003, President Bush released the [National Strategy to Secure Cyberspace](#), as a blueprint for how the nation can move forward in protecting its critical cyber infrastructure. New York State must fit into the coordinated national plan, ensuring that staffing, equipment, and training resources are maximized, and providing a mechanism to share vital information in real-time. The magnitude of the impact of potential cyber-attacks is impossible to predict. Because of this resident uncertainty, the State must have mechanisms in place that anticipate likely scenarios and address them in a way that reduces the capabilities of cyber-criminals to endanger the health, welfare and security of our State.

Some of the Fundamentals of Security^[14] that we all must be cognizant of include the following:

- 100% security does not exist;
- Security is as much a management issue as it is a technology issue;
- Implement security in layers; and
- You Are Never Done.

[1]eMarketer.com, February 1, 2002

[2]Computer Emergency Response Team at Carnegie Mellon

[3] RAND Research Review, Information War and Cyberspace Security: That Wild, Wild Cyberspace Frontier

[4]Testimony provided to Congress by Stanley R. Jarocki, July 24, 2002

[5]Computer Security Institute, " 2002 Computer Security Issues and Trends," Volume VIII, No. 1, Spring 2002

[6]Testimony provided to Congress by Stanley R. Jarocki, July 24, 2002

[7]RAND Research Review, Information War and Cyberspace Security: That Wild, Wild Cyberspace Frontier

[8]Testimony provided to Congress by Stanley R. Jarocki, July 24, 2002

[9]The Pricewaterhousecoopers "Information Security Breaches Survey 2002 Technical Report"

[10]<http://www.rand.org/publications/randreview/issues/RRR.fall95.cyber/wild.html>

[11]Verizon Press Release, October 3, 2001

[12]RAND Research Review, Information War and Cyberspace Security: That Wild, Wild Cyberspace Frontier

[13]Public Officers Law, Article 6 Freedom of Information Law (§87[2][i])

[14]Adapted from Bill Van Emburg, Quadrix Solutions

Cyber Security Task Force

Recognizing the potential for cyber attacks, Governor George E. Pataki announced on March 8, 2002, the formation of a Cyber Security Task Force, under the leadership of James K. Kallstrom, Senior Advisor to the Governor for Counter Terrorism.

The Task Force is mandated to evaluate the State's critical cyber-infrastructure, identifying potential means of cyber attack, and recommending security practices for private industry, State-operated information systems and the general public. The diversified skills and knowledge embodied in the Cyber Security Task Force, encompassing State agencies, the private sector and academia, is enabling the State to assess and prioritize the critical cyber - infrastructure of greatest concern. The Cyber Security Task Force is performing the following essential functions:

- Assuring a uniform, baseline standard of preparedness for the State's critical-systems infrastructure;
- Examining industry sectors, and appraising their susceptibility to catastrophic cyber-attack;
- Rating and prioritizing potential means of cyber related incidents, such as denial-of-service attacks, intentionally-released computer viruses, and deliberate hacking;
- Minimizing duplication between private-sector and State/Federal government initiatives and investment; and
- Enhancing the ability of New York State to respond to cyber incidents.

The first meeting of the Cyber Security Task Force was conducted on April 16, 2002 to discuss the mission, objectives, and deliverables of the Task Force. At the next meeting, held on May 30, the Task Force established two separate working groups to further define the deliverables assigned to each workgroup: a public workgroup, charged with advancing public knowledge and responsibility for cyber security; and a Public/Private Sector Cyber Security Workgroup, charged with developing standards of preparedness and methods to inventory and assess critical infrastructure assets contained within industry sectors.

This Report addresses the initiatives of the Public/Private Sector Cyber Security Workgroup and the New York State Office of Cyber Security and Critical Infrastructure Coordination, which coordinates the activities of the Workgroup.

Office of Cyber Security & Critical Infrastructure Coordination (CSCIC)

Governor Pataki established this new initiative in September 2002 to address New York State's cyber security readiness, and critical infrastructure and geographic information systems coordination. The Governor has directed CSCIC to continue New York State's efforts to be vigilant and resilient regarding information assurance. This Office is led by William F. Pelgrin and coordinates closely with the Director of the New York State Office of Homeland Security, James W. McMahon.

It is important to note that this Office is about cyber security and geographic information systems coordination in New York State - for both public and private sectors.

CSCIC is performing the following essential functions:

- Reducing redundancy between private sector and State/Federal government initiatives and investment;
- Developing a uniform, baseline standard of cyber preparedness for the State's critical systems infrastructure;
- Coordinating with critical industry sectors to examine potential vulnerabilities to catastrophic cyber attack;
- Rating and prioritizing potential means of cyber related incidents, such as denial-of-service attacks, intentionally released computer viruses, and deliberate hacking;
- Developing New York State teams to respond to cyber incidents;
- Improving geographic information analysis capabilities for emergency response;
- Coordinating and managing the statewide GIS Coordination Program, including digital base maps, the Digital Ortho Program, the GIS Clearinghouse and the Data Sharing Cooperative.
- Establishing agreements with counties and municipal government for emergency response data sharing;
- Developing emergency response remote sensing capabilities;
- Establishing a mobile emergency response geographic information team;
- Establishing a critical infrastructure and asset management tool to improve the State's ability to provide an efficient coordinated response to emergencies; and
- Performing intrusion detection services to monitor for potential cyber attacks on critical segments of the State's networks.
- Additionally, CSCIC has developed a website to be a central source of information and will include the following:
 - Best practices;
 - Real time alerts/warnings; and
 - A resource library.
- CSCIC has conducted six simulation exercises since 9/11, including one with local government.

Multi-State Information Sharing and Analysis Center (ISAC)

CSCIC participated, through the Office of Homeland Security, in a ten State Northeast Regional Consortium for sharing information. On October 22, 2002, James Kallstrom, Senior Advisor to the Governor for Counter Terrorism and John Scanlon, Director of New York State's Office of Homeland Security (OHS), held the first Northeast States Regional Homeland Security Consortium. Directors of ten States' Homeland Security Offices, including New York State, have agreed to participate in a Northeast Consortium to further the collective security interest of these states. William Pelgrin, Director of CSCIC, presented an overview of what New York State is doing to fight the war against cyber attacks and protect its critical infrastructure. It was clear from the response of those in attendance at the meeting, that New York State is a leader in addressing this new and challenging cyber era. New York State offered its services to coordinate a Multi-State Information Sharing and Analysis Center (ISAC), focusing on facilitating communication among States regarding cyber and/or critical infrastructure readiness and response efforts. This proposal was quickly embraced and a Multi-State ISAC was formed, chaired by CSCIC Director Pelgrin, in collaboration with OHS Director McMahon.

The goal is to have this ISAC include all fifty states, which would provide a valuable centrally-coordinated mechanism for sharing important security intelligence and information between the States. The ISAC can serve as a critical point of contact between the States and the Federal government. A primary goal of the ISAC is to eliminate duplicative efforts.

The kick-off meeting of the ISAC was held on January 30, 2003. The ISAC meets monthly via teleconference, and those meetings have been scheduled for the remainder of 2003.

At the kick-off meeting in January, the group agreed upon the ISAC mission and objectives as follows:

Mission

- ISAC will provide a focal point for gathering information on cyber and physical threats to critical infrastructures.
- Its mission includes the following:
 - Two-way sharing of information on critical infrastructure cyber incidents and threats;
 - Providing timely warnings of cyber and physical threats and attacks;
 - Producing comprehensive information and intelligence analyses to support federal, state and local first responders and law enforcement readiness and response efforts.

Definition of Critical Infrastructure Asset

A Critical Infrastructure Asset is an asset (both physical and logical) which is so vital that its disruption, infiltration, incapacitation, destruction or misuse would have a debilitating impact on the health, safety, welfare or economic security of citizens and businesses. Critical Infrastructures shall include human, physical and cyber assets.

Objectives of the ISAC

- Disseminate early warnings of physical and cyber system threats
- Share security incident information between Sectors
- Provide trending and other analysis for security planning
- Distribute current proven security practices and suggestions

What needs to be reported?

- Major Alerts, Incidents and Viruses
- Current Issues for the State
 - Would include any relevant reports, statements, etc made relating to this state*
- Upcoming Major Events for the State

How often should the States report in?

- The states agreed that reporting will be minimally on a monthly basis via conference calls with the NYS Office of Homeland Security and the NYS Office of Cyber Security and Critical Infrastructure Coordination—but could occur more frequently if warranted due to a significant event or incident.
- Face-to-face meetings will occur on an annual basis--and will be hosted by a different state for each occurrence.
- Reporting will be from a physical and cyber perspective.

Members

Please see the [Multi-State Information Sharing and Analysis Website](#) for full listing of ISAC Members.

Additionally, we are also reaching out internationally, and have started with Australia. (Australia is the farthest time zone which would see potentially harmful activities before the US.)

Reporting Exercise

We conducted our first test reporting exercise, where each of the states reported into New York on a daily basis over the Presidents' Day weekend in February as to the status of their state—from a cyber and physical perspective. The reporting went extremely well--with all states reporting--and the exercise was a good test run in how we can communicate.

Common Procedures

The ISAC members are working toward the adoption of a common Cyber Alert Indicator Protocol process, modeled after the federal government's color-coded alert system. Thus, when any ISAC member state is at a "blue level" for cyber, all of the other ISAC member states will know the specific criteria used to arrive at that level.

Additionally, the ISAC members are working toward the adoption of a common Incident Reporting process, whereby states can call into a toll-free number to report cyber incidents to the Multi-State ISAC.

The following section of this Report will focus on the Public/Private Sector Cyber Security Workgroup, a primary initiative underway in New York State to help ensure the State's cyber readiness.

Public/Private Sector Cyber Security Workgroup

The Public/Private Sector Cyber Security Workgroup (Workgroup) chaired by CSCIC Director Pelgrin, comprises a talented cadre of representatives from government, academia and the private sector.

Those individuals are listed below alphabetically by organization. Special thanks and recognition are deserved by all of these Workgroup members for their dedication and commitment to this important effort.

Name	Agency/Company
Nathan Rudgers	NYS Department of Agriculture and Markets
Ruth Moore	NYS Department of Agriculture and Markets
Margaret Becker	NYS Department of Agriculture and Markets
Edward Amoroso	AT&T
Diana Taylor	NYS Banking Department
Barbara Kent	NYS Banking Department
David Fredsall	NYS Banking Department
Cathy Weintraub	NYS Banking Department
Stephen Rosario	New York State Chemical Alliance
Luther Tai	Con Edison
Bob Mullen	Con Edison
William Pelgrin	NYS Office of Cyber Security & Critical Infrastructure Coordination (CSCIC)
Laura Iwan	NYS Office of Cyber Security & Critical Infrastructure Coordination (CSCIC)
Krista Montie	NYS Office of Cyber Security & Critical Infrastructure Coordination (CSCIC)
Chauncey Parker	NYS Division of Criminal Justice Services
Erin Crotty	NYS Department of Environmental Conservation
James Tuffey	NYS Department of Environmental Conservation
Susan Waltman	Greater New York Hospital Association
Susan Stuard	Greater New York Hospital Association
Ray Sweeney	Health Care Association of New York State
Louise Marks	Health Care Association of New York State
Dennis Whalen	NYS Department of Health
Gregory Serio	NYS Insurance Department
Ron Minafri	NYS Insurance Department
Phyllis Linker	NYS Insurance Department
Mike Calimano	New York Independent System Operator
Tony Elacqua	New York Independent System Operator
Jack Schwartz	New York University
Patty Noonan	NYC Partnership
John Otero	NYC Police Department
Steven Donahoo	NYC Police Department
Dennis Eccleston	New York Power Authority
James McMahan	NYS Office of Homeland Security
Mark Cohen	NYS Office of Homeland Security
Russell Bessette	NYS Office of Science, Technology, and Academic Research

William Flynn	NYS Public Service Commission
John Sennett	NYS Department of Public Service
Howard Tarler	NYS Department of Public Service
Steven Sokal	NYS Department of Public Service
Dennis Taratus	NYS Department of Public Service
Suzanne Gorman	Securities Industry Automation Corporation
Steve Cumoletti	New York State Police
Ted Phelps	State University of New York
Donald Sullivan	New York State Sheriff's Association
William Grau	Verizon
Alan Aront	Wakefern Food Corp.

One of the initial tasks of this Workgroup was to prioritize a list of critical industry sectors to determine which would be the immediate focus of the Workgroup. The Workgroup identified thirteen critical sectors (listed on page 9). We have prioritized those sectors to initially focus our efforts as follows: Chemical, Financial and Economic, Food, Health, Telecommunications, Utilities, Government**, Transportation**, Education and Awareness and Public Safety.

To date, Sector Leads from both public and private entities have been identified for eight out of the thirteen sectors as follows:

Chemical Sector Leads:

Erin Crotty, Commissioner, New York State Department of Environmental Conservation
~Alternate: James Tuffey
Stephen Rosario, New York State Chemical Alliance

Education and Awareness Sector Leads:

Ted Phelps, Information Security Officer, State University of New York
Jack Schwartz, Professor, New York University
Russell Bessette, Executive Director, New York State Office of Science, Technology, and Academic Research

Financial and Economic Sector Leads:

Diana Taylor, Superintendent, New York State Banking Department
~ Alternates: Barbara Kent, David Fredsall, Cathy Weintraub
Gregory Serio, Superintendent, New York State Insurance Department
~Alternates: Ron Minafri, and Phyllis Linker
Suzanne Gorman, Managing Director, Corporate Information Security Awareness and Investigations, Securities Industries Automation Corporation

Food Sector Lead:

Nathan Rudgers, Commissioner, New York State Department of Agriculture and Markets
~Alternates: Ruth Moore and Margaret Becker
Alan Aront, Vice President, Communications and Information Services Division, Wakefern Food Corp.

Health Sector Leads:

Dennis Whalen, Executive Deputy Commissioner, New York State Department of Health
Ray Sweeney, Executive Vice President, Health Care Association of New York State
~Alternate: Louise Marks
Susan Waltman, General Counsel, Greater New York Hospital Association
~Alternate: Susan Stuard

Public Safety Sector Leads:

Chauncey Parker, Commissioner, New York State Division of Criminal Justice Services
James McMahan, NYS Office of Homeland Security
John Otero, Commanding Officer, Computer Investigation and Technology Unit, NYPD
Donald Sullivan, New York State Sheriff's Association

Telecommunications Sector Leads:

William Flynn, Chairman, New York State Public Service Commission
~Alternates: John Sennett and Steven Sokal
Edward Amoroso, Chief Information Security Officer, AT&T

Utilities Sector Leads:

William Flynn, Chairman, New York State Public Service Commission

William Flynn, Chairman, New York State Public Service Commission

~Alternates: John Sennett and Howard Tarler

Dennis Eccleston, Chief Information Officer, New York Power Authority

~Alternate: John Hahn

Luther Tai, Senior Vice President, Central Services, Con Edison

~Alternate: Bob Mullen

**Sector Leads for the Government and Transportation Sectors will be identified at a later date. Government Sector Leads will include representatives from the local government, including New York City and upstate New York.



October 2002 Workgroup Meeting

Public/Private Sector Cyber Security Workgroup - Deliverables

The Workgroup is focusing on a number of deliverables in its efforts to assess the current state-of-readiness against cyber incidents on our critical infrastructure and provide recommendations to the entities within each of the sectors above. (Note that the remainder of this report focuses on the outreach activities of the following four sectors: Financial, Health, Telecommunications and Utilities. Subsequent reports will include information from the other sectors.)

Definition of Critical Infrastructure

The Workgroup adopted the following as its general definition of critical infrastructure:

"Cyber assets (technology-based physical and/or logical) which are so vital that their infiltration, incapacitation, destruction or misuse would have a debilitating impact on the health, safety, welfare or economic security of the citizens and businesses of New York State."

Each sector has supplemented this generic definition, as appropriate, to apply to the specific nature of the sector.

- **Financial and Economic Sector:**

Cyber assets (technology-based physical and/or logical) which are so vital that their infiltration, incapacitation, destruction or misuse would have a debilitating impact on the health, safety, welfare or economic security of the citizens and businesses of New York State.

Critical assets for the Financial and Economic sector would be those systems in which there would be a potential for broad systemic impact to the banking, payments or securities and capital market systems.

- **Health Sector:**

Cyber assets (technology-based physical and/or logical) which are so vital that their infiltration, incapacitation, destruction or misuse would have a debilitating impact on the health, safety, welfare or economic security of the citizens and businesses of New York State.

Critical assets for the Public Health Sector include those where there would be the potential for a broad system attack and the system compromised or used to broadcast hoax alerts. With the Public Health focus on use of the Internet as a new communications tool, misuse would be much more devastating than a denial of service, at least at this time.

- **Telecommunications Sector:**

Cyber assets (technology-based physical and/or logical) which are so vital that their infiltration, incapacitation, destruction or misuse would have a debilitating impact on the health, safety, welfare or economic security of the citizens and businesses of New York State.

Critical assets for the Telecommunications sector include the following:

- Facilities housing significant critical network switching, routing, transport or restoration equipment along with operations support systems and business applications;
- Work Centers with active surveillance, analysis and notification capabilities for network equipment performance and utilization trends;
- Data Table Repository Facilities for signaling, routing, directories, recording, and managing the network; and
- E911 Systems.

- **Utilities Sector:**

Cyber assets (technology-based physical and/or logical) which are so vital that their infiltration, incapacitation, destruction or misuse would have a debilitating impact on the health, safety, welfare or economic security of the citizens and businesses of New York State.

Critical assets for the Utilities sector include any computer system, hardware or software that if severely damaged, destroyed, infiltrated or

compromised would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact to the reliability or operability of the energy grid, or would cause significant risk to public health and safety. This includes those components under the direct control of your organization, as well as those controlled by other organizations upon which you are dependent.

Inventory, Vulnerability and Risk Assessment

In order to protect the critical infrastructure assets as defined above, there is a need to know where they are located; whether they are vulnerable to a cyber attack; and what is the risk associated with the vulnerability.

Two of the principles adopted by the Workgroup are as follows:

- We would not duplicate efforts. If a credible entity (e.g., U.S. Department of Energy) is, or will be, doing an inventory, vulnerability and risk assessment, this Workgroup will not duplicate their effort, as long as we are able to receive the necessary information from the other entity.
- We would only request a high level summary to be reported. While the Workgroup recognized the need to have entities within each sector perform a detailed inventory and analysis, the granular information would remain with the entity unless otherwise required by law to be reported. Therefore, entities within each sector are being asked to report only high-level information to the Workgroup; other, more detailed and sensitive information will remain within the entities. Some of the sectors have already begun this process, while others are still in the preliminary stages. A draft inventory and assessment template form has been developed which the Sectors may distribute to the entities.

Below is the status of this effort, by Sector.

Financial and Economic Sector:

The New York State Banking Department is reaching out to its largest institutions for inventory and vulnerability and risk assessment information. Those institutions include JP Morgan Chase, Bank of New York, HSBC, Deutsche Bank, Depository Trust Company, Manufacturers and Traders, North Fork Bank and GreenPoint Bank. These comprise the bulk of banking assets under the Banking Department's jurisdiction, and are the institutions where a systemic impact could occur, given a successful cyber attack.

Outreach has been made to the Insurance Department to develop a strategy to assess the insurance industry.

Additionally, the Workgroup will reach out to all of the Self Regulatory Organizations (SROs.) An SRO is a nongovernmental agency formed in accordance with the Securities Exchange Act of 1934. SROs are charged with regulating the conduct and activities of its own members, but are subject to oversight by a government regulatory agency. SROs include securities and commodities exchanges, as well as clearing organizations. Examples include Security Industries Automation Corporation (SIAC), The New York Stock Exchange, NASDAQ, and the American Stock Exchange, which are overseen by the Securities Exchange Commission (SEC).

The Financial and Economic Sector is continuing to have discussions with the Federal Reserve Board to coordinate identifying key elements and critical operational components. The Financial Industry Summit on Business Continuity sponsored by the Banking Department, federal bank regulators and the SEC provides a forum for a public/private discussion of business continuity issues, including cyber-vulnerabilities.

Health Sector:

The New York State Department of Health (NYSDOH) is surveying hospitals, nursing homes, pharmacies and other critical infrastructures as follows: Hospitals: 255 (100%); Nursing Homes: 685 (100%); Clinics: 470 (100% of major clinics); Clinical Labs: 934 (100% of permitted labs); Environmental Labs: 712 (100% of permitted labs); Adult Homes: 539 (100%); Pharmacies: 18 major chains (representing 2200 pharmacies); Intermediate Care Facility/Mental Retardation (ICF/MRs): 14 (100%); Public Water Supplies: Top 30 systems

A major focus will be on requiring third party vulnerability and risk assessments of the health communications systems. This includes interface with the Department's hospital capacity system, hospital response systems, disease reporting systems, environmental reporting systems and public health communications systems.

In addition, the Department of Health will survey the thirty largest public water supplies. Out of the 18,976,457 New York State census 2000 population data, approximately 16.6 million people are served by 3,274 community water systems in their residence. The NYSDOH Top 30 Emergency Notification list includes the largest thirty of these systems, listed in order of population served, as follows:

1. NY City	16. Albany, City
2. Suffolk Co Water Authority	17. New York Water Service
3. Onondaga Co Water Authority	18. United Water of New Rochelle
4. Monroe County Water Authority	19. Upper Mohawk Valley Reg WB
5. Erie Co Water Authority	20. Town of Hempstead WD
6. Syracuse, City	21. Westchester Joint Water Works
7. Metropolitan Water Board	22. Binghamton, City
8. Rochester, City	23. Latham WD
9. Buffalo Water Authority	24. Troy City PWS
10. Westchester Co WD #1	25. Schenectady City Water Works
11. Niagara County Water District	26. WA of Western Nassau
12. United Water of New York	27. South Huntington WD
13. Long Island Water Corp	28. Tonawanda, Town WD
14. Yonkers, City	29. Elmira Water Board
15. Monticello, City	30. Cortland, City

The thirty systems listed provide water service to more than 12 million people. This is roughly 72% of the population whose residence is served by a public water system or approximately 63% of the State's census 2000 population.

The New York State Public Service Commission is conducting outreach to the six major water utilities in the State as follows:

- Aquarion - Sea Cliff
- Aquarion - New York
- Long Island Water Works
- New York Water Service
- United Water of New Rochelle
- United Water New York

The Federal EPA is doing an assessment of water supplies. The Health sector is attempting to determine the details of the assessment and results to date.

Telecommunications Sector:

The Public Service Commission (PSC) is requiring major telecommunications providers that PSC regulates to conduct third party vulnerability and risk assessments, as follows:

- AT&T Communications of New York, Inc.
- Teleport Communications Group of New York
- ACC Long Distance Corporation
- ACC National Telecommunications of NY
- ACC Telecommunicatons, LLC
- Citizens Telecommunications Company of New York, Inc.
- Citizens Long Distance, Inc.
- Electric Lightwave, Inc.
- Ogden Telephone Company
- Ogden Long Distance Company
- Frontier Telephone of Rochester, Inc.
- Frontier Communications of Rochester, Inc.
- Frontier Communications New York, Inc.
- Frontier Communications Sylvan Lake, Inc.
- Frontier Communications Seneca Gorham, Inc.
- Frontier Communications of Ausable Valley, Inc.
- Frontier Communications of America, Inc.
- Bell Atlantic Communications, Inc.
- NYNEX Long Distance Company
- Verizon New York, Inc.
- Verizon Select Services, Inc.
- MCI WorldCom Network Services, Inc
- MCImetro Access Transmission Services, Inc.
- Brooks Fiber Communications of New York, Inc
- Intermedia Communications, Inc

PSC is also conducting discussions with major cable television companies (Time Warner, Adelphia and Cablevision) to discuss security.

In addition, the Workgroup will request assessments from the major wireless carriers and major Internet backbone and service providers.

Utilities Sector:

The Public Service Commission (PSC) is requiring the larger utilities that PSC regulates to conduct third party vulnerability and risk assessments as follows:

Energy Companies

- Central Hudson Gas & Electric Corporation
- Consolidated Edison Company of New York, Inc.
- Keyspan Corporation:
 - Brooklyn Union Gas Company/dba/Keyspan Energy Delivery New York
 - Keyspan Gas East Corporation/dba/Keyspan Energy Delivery Long Island
- National Fuel Gas Distribution Corporation
- Niagara Mohawk Power Corporation
- Orange and Rockland Utilities, Inc.
- New York State Electric and Gas Corporation
- Rochester Gas and Electric Corporation

The PSC does not have security authority over nuclear facilities. The Nuclear Regulatory Commission (NRC) is responsible for all matters related to nuclear plant security.

Gold Standards for Cyber Security Readiness

The Workgroup is finalizing a set of "gold standard" guidelines by which entities within each sector may use to measure their state-of-readiness. The gold standard, in conjunction with the inventory and assessment forms, will provide entities with a much clearer picture of how ready they are, and what areas may need to be strengthened. These gold standards will be weighted in determination of importance, so that if an entity "fails" to meet the gold standards in a certain number of the highly-weighted categories, we would not consider them to be in an acceptable state-of-readiness.

Technology Vendor Contact Database

During the attacks on the World Trade Center, the out-pouring of assistance from vendors and citizens was overwhelming. We needed a comprehensive way to collect this information, and by September 13, 2001, we had a functioning web-based database application to collect and search information regarding donations.

Building on that model, and using our lessons learned from that experience, a database application is being developed in which technology vendors can participate on a voluntary basis, providing emergency contact information for high-level staff within their company. They can also indicate what types of resources, both physical and human, they could provide in the event of any kind of emergency.

Authorized users at the State's emergency operations center will be able to search quickly and efficiently during an emergency to call upon necessary resources available from the private sector.

We will start by soliciting almost seventy companies for participation; this list will be expanded in the future to include data from other Northeast states.

Conclusion

The Workgroup has made significant strides in fulfilling the mission of the Task Force. However, the mandates for the Workgroup are on-going -- and will continue - in order for New York State to be consistently ready to deal with this new era of cyber threats. Under Governor Pataki's leadership, New York won the race to be prepared for the Y2K date change. This race had a definite end date (January 1, 2000). In this on-going challenge to be cyber ready, there is no end date. Therefore, the Workgroup must continue its valuable work underway. We are proud of what New York State has already accomplished in such a short amount of time. We firmly believe New York is on the right course in this critical effort to be prepared. The following are fundamental principles that when followed will provide strong building blocks to support this cyber initiative.

- Operational aspects of cyber security readiness and response are critical to address the long-term viability and stability of New York State's Critical Infrastructure. The State plays a major role in the efforts to prevent cyber attacks from occurring, via early detection of such threats and through a comprehensive response when such attacks occur.
- Collaborations among and between local, federal and other state partners are essential to a successful solution of improving our cyber security and readiness.
- Solid policies, procedures, and practices are important to achieving our overall goal for improving the health, welfare and safety of the Critical Infrastructure and the Citizens of New York State.

It is clear that issues related to people, policies, procedures, practices, training, and education are a critical adjunct to any successful cyber security strategy.

Recommendations

The following are the Workgroup's recommendations for implementation in order for New York State to become cyber ready:

Immediate Actions for Implementation

- **"Inventory, Vulnerability and Risk Assessments"** Request-through the Workgroup--that Assessments are conducted minimally on an annual basis.
- **"Gold Standard"** Request-through the Workgroup--that entities within each Sector rate themselves against the Gold Standard periodically.
- **"Red Teams"** Encourage testing of key critical information infrastructure systems' defenses through the use of tiger teams or ethical hacking. Entities need to be proactive in testing their systems in order to identify vulnerabilities.
- **"Information and Sharing Analysis Center"** Establish the State's ISAC to receive and distribute cyber warnings and alerts with the private sector's ISACs.
- **"Emergency Response Teams"** Create partnerships with the private and public sectors to respond to major cyber incidents.
- **"Legal and Technical Advisory Subcommittees"** Create two subcommittees to advise and provide recommendations to the Workgroup regarding emerging legal and technical issues.
- **"Development of Dos and Don'ts One-Pager"** Develop a high-level document designed for CEOs and Executive Staff in both the public and private sectors to provide them with a quick, handy reference guide on security basics.
- **"Development of a One-Pager on Cyber Ethics for Kids"** This would be an awareness document on the issues of cyber ethics designed for K-12.

Additional Recommendations

- **"Inventory of Modems/Remote Computing Capabilities"**
Recommend as a Best Practice that all governments and private entities:
 - Conduct inventories of their remote access systems such as modems that are in place within their networks;

- o Determine if these remote access points are authorized, create a vulnerability or are unnecessary or inactive and could be removed; and
- o Government entities (State agencies and authorities) would report this information back to the CSCIC for inclusion in future reports to the Governor.

- ***"Hosting of a Multi-State Cyber Summit in New York State"***

The Summit would bring together government and industry leaders to discuss cyber issues. New York has been recognized by President Bush's Advisor on Cyberspace Security and his Critical Infrastructure Protection Board as a model for the country. This summit will not only help promote NYS it will also be a tremendous benefit to other states that wish to participate.

[CSCIC Home](#) | [About CSCIC](#) | [Cyber Security](#) | [Cyber Security Alerts](#)
[Cyber Security Advisories](#) | [Related Sites](#) | [Policies](#) | [Reports](#) | [Calendar](#) | [Contact Us](#)

[Privacy Policy](#)