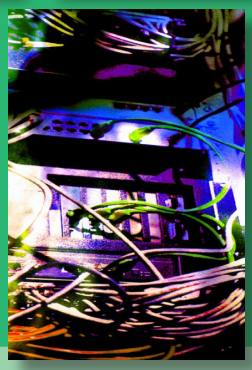
# MARYLAND

## Cyber Security White Paper









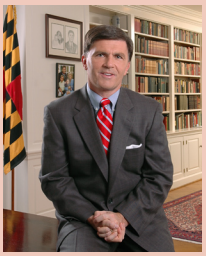
# Defining the Role of State Government to Secure Maryland's Cyber Infrastructure

November 1, 2006

Robert L. Ehrlich, Jr., Governor
Michael S. Steele, Lt. Governor

MARYLAND

## Message from the Governor



My Fellow Marylanders,

Protection of critical infrastructure, which includes both physical and cyber assets, is a component of Maryland's overall homeland security strategy. The State's critical infrastructure resilience program centers upon these four compelling objectives:

- ✔ Prevention Planning
- ✔ Impact of Loss Analysis (Economic/Local)
- ✔ Cycle Time to Recovery
- ✔ Understanding Interdependencies

Our state faces a challenge to protect the technological assets that are essential to its economy, security, and way of life.

Maryland's infrastructure is owned by a diverse set of stakeholders from the public and non-governmental sectors. These stakeholders share a common interest to safeguard cyber assets, and tools such as the Regional Information Sharing Systems – Automated Trusted Information Exchange (RISS-ATIX) help stakeholders share cyber responsibilities and resources. However, the sharing of cyber resources requires trust. Government can promote this trust by facilitating an environment in which stakeholders will benefit by pooling their resources and coordinating their efforts.

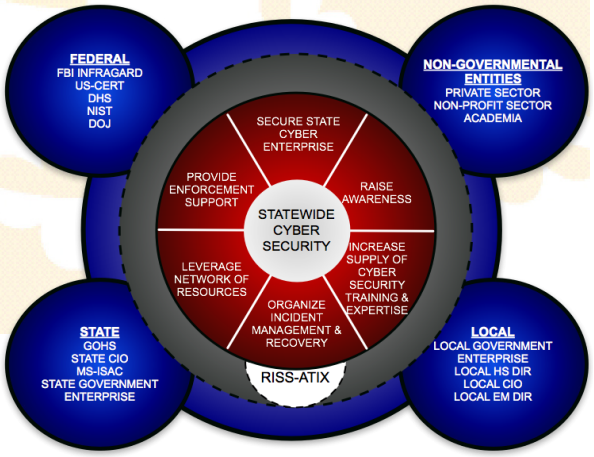
My administration is working hard to bring our private and public partners together to determine the appropriate role of the state in securing our vital cyber assets. I look forward to coming together to find ways to make our cyber assets better and safer for all Marylanders.

Very truly yours,

Robert L. Ehrlich, Jr.
Governor

*The figure at the right depicts the many entities which comprise the Maryland Cyber Security Partnership. It is important to distinguish between the State of Maryland and the State Chief of Information Technology (CIT). For the purposes of this paper, "**State of Maryland**" refers to Maryland cyber security stakeholders and resources. This includes, but is not limited to, the state enterprise, which consists of the State CIT and the information technology teams of state agencies. The term "**non-governmental entities**" as used in this document, includes the academic community, the private sector, and non-profit groups.*

### Maryland's Cyber Security Partnership




### Summary of Objectives

The State's objectives establish a framework for key stakeholders to coordinate their efforts to accomplish cyber security in Maryland.

The following broad objectives and outcomes are proposed:

I. Increase awareness of the cyber security threat in the State and Local Government, Private Sector, and General Public

II. Facilitate a network of resources to leverage cyber capabilities

III. Organize an Incident Management and Recovery Framework

IV. Increase the supply of cyber security expertise within the State of Maryland

V. Provide continued support to statewide law enforcement efforts

VI. Secure the state government's cyber enterprise

The Governor's Office of Homeland Security will provide sponsorship and leadership to key cyber security stakeholders in order to facilitate these objectives.

### Definitions

A ***stakeholder*** is a person or an organization who might affect or be affected by the work or actions of another. Stakeholders most often share a joint interest in the success or completion of a specific task or project. For a listing of Maryland cyber security stakeholders, please see pages 6-7 of this document.

***Cyber security*** runs the gamut from simple physical security steps (e.g., making sure your laptops and other portable media are secured when not in use) to implementing large-scale information technology systems (e.g., firewalls, intrusion detection and prevention systems, anti-virus and anti-spyware software).*

*Definition adopted from *Beginner's Guide to Firewalls*, Published by MS-ISAC.

## Objective I

### Increase Awareness of the Cyber Security Threat in the State and Local Government, Private Sector, and General Public

*Stakeholders' awareness of the potential risks to cyberspace and potential security solutions is an important first step to engaging them in the cyber security effort.*

*To elevate awareness, the stakeholders will:*

- ✔ **Engage** the business community, local emergency managers, and chief information officers (CIOs) by suggesting they perform a sufficiency check of their existing cyber security plans. They will be encouraged to perform this self-assessment by responding to a comprehensive questionnaire which addresses four key areas of their security plan: policy, training, technology deployment, and vulnerability assessment.*
- ✔ **Focus** efforts on local chambers of commerce, local technology councils, and similar organizations of business leaders. This outreach will emphasize the importance of cyber security to small and midsize companies and local government.
- ✔ **Provide a forum** where government and non-government sectors can meet together to discuss and raise awareness of cyber security issues. The Anti-Terrorism Advisory Council Private Sector Workgroup (ATAC PSWG), in coordination with InfraGard, has taken preliminary steps to form a Cyber Security Community of Interest that will serve this outreach goal.
- ✔ **Encourage the adoption** of effective technology solutions and promising practices by partnering with National Centers of Academic Excellence in Information Assurance Education (CAEIAE), United States Computer Emergency Readiness Team (US-CERT), the Computer Security Resource Center (www.csrc.nist.gov) of the National Institute of Standards and Technology (NIST), InfraGard, the non-governmental sector, and CyberWATCH. Through these partnerships, stakeholders will organize an on-line, comprehensive directory of common terms, definitions, promising practices, and resources.
- ✔ **Promote private-sector development** of a cyber security business case as an economic justification for small and mid-sized businesses.

* The template of questions can be found in the Cyber Security section (Appendix I) of the 2006 Homeland Security Grant Program Guidance and Application Kit published by the United States Department of Homeland Security. A copy of this document is also available on the Maryland Cyber Security Community of Interest website, www.mdcyber.info.

## Objective II

### Facilitate a Network of Resources to Leverage Cyber Security Capabilities

*The private sector owns a significant majority of the cyber assets in Maryland. A comprehensive cyber security strategy requires coordination between both the public and private sectors. By building consensus, the State will provide structural leadership and guidance by facilitating a series of workshops, workgroups, and interactive forums.*

*Relationships between stakeholders are a valuable part of enhancing the State's cyber security capabilities. This series of relationship building exercises and events serves to:*

- ✔ **Sponsor and/or promote opportunities** for stakeholders to convene and exchange innovative ideas and solutions. At the Cyber Security Consensus Symposium on September 15, 2006, stakeholders from academia, law enforcement, the private sector, and state and local government met and provided feedback on the objectives and action-items of the White Paper.
- ✔ **Facilitate sector-to-sector communication** between various public and private agencies and organizations. For example, the ATAC PSWG Cyber Security Community of Interest will convene regularly to share ideas and discussions between the public and private sectors regarding cyber security priority projects and initiatives.
- ✔ **Explore additional public and private partnerships** that link state and federal resources. For example, the Governor's Office has designated a representative to serve on the FBI's InfraGard of Maryland Programs Committee.
- ✔ **Encourage** federal, state, local government, academia, and the private sector to participate in the Mid-Atlantic All Hazards Consortium. The Consortium provides an opportunity to promote regional cyber security partnerships with other states in the Mid-Atlantic Region.
- ✔ **Share critical cyber security information**. Through the Multi State Information Sharing and Analysis Center (MS-ISAC), the State of Maryland will benchmark other state programs and coordinate with the NGA Best-Practices Center.

## Objective III

### Organize Incident Management and Recovery Framework

*The State of Maryland will develop and exercise a series of cyber security continuity and contingency plans to coordinate response and remediation to cyber incidents. It is essential that stakeholders engage non-government volunteers from groups like InfraGard to actively participate in the development of these plans and the exercises that test them. To increase cyber resilience, stakeholders will:*

✔ **Sponsor and promote** a series of exercises to convene and exchange strategies for enhancing the ability to respond to cyber incidents. Through these exercises, stakeholders will:

1. Emphasize the importance of coordinating interdependent resources following an attack on information systems *(ATAC PSWG Interdependencies Workshop—October 2006).*
2. Test Supervisory Control and Data Acquisition (SCADA) systems that control electric power, gas, and water production and distribution *(Maryland SCADA Exercise—February 2007).*
3. Incorporate cyber continuity of operations planning into the State's critical infrastructure protection program *(Blue Chesapeake Regional Exercise—April 2007).*

✔ **Build cyber preparedness and response** into the State Emergency Operation Plan. Stakeholders will work with the Maryland Emergency Management Agency (MEMA) to:

1. Develop a comprehensive on-line resource and handbook of standardized operating procedures.
2. Utilize the Maryland Joint Operations Center (MJOC) as a centralized repository for up-to-date information on the consequences of a cyber attack.

✔ **Support** the Maryland Coordination and Analysis Center (MCAC) and the MJOC in their respective roles pertaining to cyber security. Specifically:

1. To collect, analyze, and disseminate credible cyber-threat information to stakeholders (MCAC).
2. To coordinate response to cyber incidents by federal, state, and local law enforcement.
3. To verify that law enforcement personnel hold clearances to view sensitive cyber threat information.

✔ **Facilitate the development** of an online resource and handbook that will help individuals determine which law enforcement personnel to contact to report cyber crime and incidents.

> "If there is a cyber disaster, there is no emergency number to call and no one in place to respond because our nation simply doesn't have the kind of coordinated plan in place that we need..."
>
> *--Edward Rust Jr., Chairman and CEO, State Farm Insurance Companies*

## Objective IV

### Increase the Supply of Cyber Security Expertise Within the State of Maryland

*The State will encourage the use of existing training resources and curricula to increase the supply of qualified IT professionals available to government, law enforcement, and small to midsize private sector companies. To further this objective, the stakeholders will:*

✔ **Develop and maintain** partnerships which will further this objective. Specifically, stakeholders will:

1. Pursue relationships with academic institutions such as the Centers of Academic Excellence and CyberWATCH that offer training and courses in cyber security that enhance the credentials of IT professionals. To increase the supply of highly qualified IT professionals, the State of Maryland will foster the connections among these academic institutions, non-governmental entities, and local jurisdictions.
2. Develop on-line learning as a resource for cyber security training.
3. Encourage non-governmental stakeholders to provide support to local government and law enforcement for the purpose of improving cyber security training and evidence collection.

✔ **Facilitate opportunities for students** to learn about promising career paths in information technology. Toward this end, the stakeholders will:

1. Provide internship programs that will allow students to gain experience and interest in IT positions with government, law enforcement, and small to midsize private sector companies.
2. Continue to nurture and support educational programs such as the homeland security curriculum established by the Harford County Public Schools.
3. Publicize and communicate cyber-related career paths through stakeholders' newsletters and informational websites.

## Objective V

### Provide Continued Support to Statewide Law Enforcement Efforts

*The State seeks to clearly define the role of law enforcement stakeholders in the prevention of and response to cyber security events. The State will engage law enforcement at the federal, state and local levels in a series of discussions to develop the nature of their role in the State's cyber protection strategy.*

*To further this objective, the stakeholders will:*

- ✔ **Increase coordination** between state and local law enforcement, the threat information collection and sharing components of US-CERT and the Federal Bureau of Investigation (FBI).
- ✔ **Increase utilization of the ISACs and RISS-ATIX** as key resources for gathering information and intelligence on cyber threats. RISS-ATIX, a secure intranet website, will serve as the conduit for cyber threat information between the private sector, federal government, and law enforcement at the federal, state and local levels.
- ✔ **Develop MCAC as a clearinghouse** for all state cyber threat information and intelligence through assignment of dedicated cyber crime analysts. MCAC is structured to disseminate cyber threat information to appropriate federal, state and local agencies, as well as non-governmental entities.
- ✔ **Utilize** non-governmental entities, the Electronic Crimes Task Force of the U.S. Secret Service, US-CERT, and the Department of Justice to provide resources to improve and increase cyber crime training programs.

### QUESTIONS?

For answers to questions or more information on Maryland's cyber security strategy, please visit the Maryland Cyber Security Community of Interest website at www.mdcyber.info or contact:

Dennis R. Schrader, ***Director***
Leigh B. Middleditch, ***Criminal Justice Programs Director***

Governor's Office of Homeland Security
16 Francis Street 4th Floor
Annapolis, MD 21401
(410) 974-2389 • gohs@gov.state.md.us

## Objective VI

### Secure the State Government's Cyber Enterprise

*The National Strategy to Secure Cyberspace encourages state and local government to establish appropriate information technology security programs and participate in information sharing and analysis.*

*The State Chief of Information Technology (CIT) focuses on protecting the cyber welfare of State agencies in Maryland. State agencies currently participate in or work with a wide-range of cyber security resources. The State of Maryland will share information about resources with the CIT to help secure the state government's cyber enterprise.*

"Preparedness for a cyber attack requires partnership and coordination between all levels of government and the private sector..."

*-- George Foresman, Under Secretary for Preparedness, U.S. Department of Homeland Security*

## Maryland Cyber Security Stakeholders

### The Anti-Terrorism Advisory Council of Maryland Private Sector Workgroup

The Private Sector Work Group represents a nexus of public and private sector organizations in Maryland dedicated to the protection of critical infrastructure assets. The Workgroup meets every fourth Wednesday of even-numbered months.

### Centers for Academic Excellence in Information Assurance Education

The National Centers of Academic Excellence in Information Assurance Education (CAEIAE) Program is jointly sponsored by the NSA and the Department of Homeland Security (DHS) in support of the President's National Strategy to Secure Cyberspace, February 2003. The goal of the program is to reduce vulnerability in our national information infrastructure by promoting higher education in information assurance (IA), and producing a growing number of professionals with IA expertise in various disciplines.

### CyberWATCH

CyberWATCH is an institutional academic partnership representing seven regional community colleges and eight universities. CyberWATCH includes the six Centers for Academic Excellence. The overarching goal of CyberWATCH is to improve the quantity and quality of the security workforce on the associate degree, baccalaureate, and advance degree levels.

### United States Department of Defense Cyber Crime Center

DC3 is the U.S. Department of Defense's center of excellence for digital forensics analysis, research and development, and training to support the Defense criminal investigative, counterintelligence, and security organizations, as well as other customers both within and outside DoD.

### Governor's Office of Homeland Security

GOHS serves as the direct liaison to the U.S. Department of Homeland Security, as well as coordinating State departments, agencies, counties, and municipalities in matters of homeland security and emergency preparedness.

### FBI's InfraGard of Maryland

The FBI's InfraGard is a partnership of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States.

### Maryland Coordination and Analysis Center

The Anti-Terrorism Advisory Council oversees the Maryland Coordination and Analysis Center (MCAC) to ensure that information regarding terrorism is disseminated to appropriate federal, state and local agencies, as well as private sector entities, in a timely manner.

### State of Maryland Chief of Information Technology

Located within the Department of Budget and Management, the CIT guides Maryland State government's information technology initiatives. The State CIT serves as the primary advisor for all aspects of information technology including the development and implementation of the State's Information Technology Master Plan.

### U.S. Secret Service Electronic Crimes Task Force

As part of a national network of electronic crimes task forces, the U.S. Secret Service's ECTF seeks to prevent, detect, and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems. Its role includes conducting computer/telecommunications investigations, and preparing search warrants on electronic storage devices.

## Maryland Cyber Security Stakeholders Continued

### Mid-Atlantic All-Hazards Consortium

The All-Hazards Consortium organizes the All-Hazards Forum, a grassroots, public-private partnership of Mid-Atlantic States and private corporations to solve emergency management and homeland security issues at the local, county, and state levels in the Mid-Atlantic region.

### Multi-State Information Sharing and Analysis Center (MS-ISAC)

The MS-ISAC is a voluntary and collaborative organization with participation from all 50 states and the District of Columbia. The MS-ISAC provides a central resource for gathering information on cyber threats to critical infrastructure from the states and providing two-way sharing of information between and among the states and with local government. The mission of the MS-ISAC is to provide a common mechanism for raising the level of cyber security readiness and response in each state and with local governments.

### National Governors Association

The National Governors Association (NGA) is the collective voice of the nation's governors and one of Washington, D.C.'s most respected public policy organizations. NGA provides governors and their senior staff members with services that range from representing states on Capitol Hill and before the Administration on key federal issues to developing policy reports on innovative state programs and hosting networking seminars for state government executive branch officials. The NGA Center for Best Practices focuses on state innovations and best practices and issues that range from education and health to technology, welfare reform, and the environment.

### National Institute for Standards and Technology

The National Institute for Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life.

### Regional Critical Infrastructure Interdependencies Workshop

On October 10, 2006, this workshop marked the first step in a government and private sector initiative to identify critical infrastructure interdependencies—complex interconnections among the critical infrastructures that underpin information networks, public health and safety and national security.

### Regional Information Sharing Systems - Automated Trusted Information Exchange (RISS-ATIX)

RISS-ATIX is a secure intranet website that will serve as the channel of cyber threat information among the private and public sector, to include law enforcement and local, state and federal government officials. Funded by the Department of Justice, RISS-ATIX is a secure communications channel that allows for the timely exchange of information pertaining to homeland security and serves as an interface for the private and public sectors.

### U.S. Computer Emergency Readiness Team (US-CERT)

US-CERT, in partnership with the Department of Homeland Security (DHS), is charged with protecting the nation's Internet infrastructure by coordinating defense against and response to cyber attacks.

### U.S. Department of Justice Office of Justice Programs – Information Sharing

Since 1984, the Office of Justice Programs has provided federal leadership in developing the nation's capacity to prevent and control crime, improve the criminal and juvenile justice systems, increase knowledge about crime and related issues, and assist crime victims.

Robert L. Ehrlich, Jr., Governor
Michael S. Steele, Lt. Governor