Opening Remarks:
Partnerships for Combating Terrorism Forum

4 March 2002

I'm Mike Hayden, Director of the National Security Agency. NSA is the nation's cryptologic organization, the world's best at making and breaking codes. We protect the security of the U.S. government's classified and sensitive communications and provide intelligence information derived from foreign communications and signals.

Intelligence and information assurance have always complemented each other. Intelligence gives us an information advantage over our adversaries. Information assurance prevents others from gaining a comparable advantage over us. The two functions serve as the offensive and defensive squads of a team dedicated to a single goal -- information superiority for the United States and its allies.

Intelligence is, of course, vital to combating terrorism. The ultimate weapon against terrorists is information regarding their identity and intent. Terrorists depend upon absolute secrecy in conducting their operations, and pose no match for security forces when their activities are compromised. Given our many points of vulnerability and the near-impossibility of defending them all adequately, our homeland security program must include intelligence capabilities that take the initiative away from our adversaries.

But intelligence is useless if it doesn't get to the people who need it. It must be shared, and this is where the defensive team – information assurance – has a key role to play. As we discuss federal, state, and local partnerships here today, I expect that much of the discussion will focus on protecting the networks and information systems that will make these partnerships possible.

Before we get into the details, I'd like to make three larger points about the role of information assurance in building partnerships for homeland security. First, our partnerships, like much of our national enterprise, will depend critically on the trustworthiness and availability of our information infrastructure. Second, this infrastructure constitutes a high-value target. And third, protecting the information infrastructure will require partnership not only across the various levels of government but with the private sector, as well.

In recent years, the nation has become highly dependent on networked information systems to conduct essential activities, including military operations and government business. This technology has become simultaneously one of our most important sources of competitive advantage and one of our most serious strategic vulnerabilities.

Our ability to network has far outpaced our ability to protect networks. The efficiency that networking has made possible has come at the price of increased vulnerability of data and systems to attack. Information in unprotected or poorly protected networks can be accessed, changed, or destroyed. Unprotected systems can be controlled, damaged, or shut down, and critical services denied.

In a world where information systems control key functions and critical infrastructures, logic bombs rival iron bombs in their power to bring operations to a standstill. The emergence of cyberspace has opened a path over which an attacker could strike powerfully against our homeland – and our efforts to protect our homeland -- through cyber attacks against the data and systems on which we depend.

The attacks of September 11th have generated a tremendous amount of cooperative effort to defend the country in physical space. We need a comparable sense of urgency and an even greater level of partnership to defend the country in cyberspace.

All of us rely on an interdependent web of networked infrastructure for the energy and other services we require. We are mutually vulnerable if that infrastructure fails. At some level of damage, the protections and back-ups we have put in place to deal with the normal risks encountered in our individual enterprises will be overwhelmed. No one can go it alone.

Our information infrastructure encompasses a wide range of activities extending over vast reaches of physical and virtual space. No single entity in government or industry directly controls more than a small fraction of it. The problem of infrastructure security will require shared effort across organizational boundaries. No one can solve it alone.

The vulnerability of our infrastructure is thus neither an entirely public nor an entirely private problem. The risk it poses is common to government, business, and citizen alike. Reducing that risk will require coordinated effort within and between the private and public sectors. The need for infrastructure protection creates a zone of shared responsibility and potential cooperation for industry and government.

New forms of information sharing between government and the private sector are needed both to improve the effectiveness of the measures put in place to protect the infrastructure and to provide the earliest possible warning of attack. State and local law enforcement have key roles to play in the national defensive information operations effort as primary channels for communication with businesses and communities.

That's the big picture. Our focus today is how we can optimize information sharing within government. Again, assuring our information is key to our success.

On January 18th a ten-state coalition of state and local law enforcement organizations met to discuss homeland security, and identified the following challenges:

- Develop a secure system for information exchange.

- Standardize protocols and access to critical information.

- Implement a standard notification system to alert officers if persons of interest to intelligence agencies or INS are encountered.

- Develop data integration systems.

The solutions to each of these challenges require confidentiality through encryption, verification of data integrity, authentication of originators, proof of participation by parties to a transaction, and availability of service on demand – that is, the full range of information assurance services.

NSA has served for decades as the national security community's center of excellence for information assurance, as well as one of the nation's most important sources of intelligence. I look forward today to exploring ways in which the benefits of both aspects of my Agency's mission – providing and protecting vital information – can be made available to all levels of government.