Remarks of Thomas N. Auriemma at the Public Hearing before the Assembly Tourism and Gaming Committee Regarding Homeland Security in the Context of Tourism and Gaming

January 10, 2005

Mr. Chairman, Madam Vice-Chair and Members of the Committee:

As a representative of the Attorney General of New Jersey, and Director of the Division of Gaming Enforcement, one of the state agencies responsible for the regulation of the casino industry in New Jersey, I thank you for the opportunity to appear before you today to address the important issue of homeland security as it relates to Atlantic City.

As you are all aware, the casino industry makes a significant contribution to the State's economy. The 12 casino hotel facilities currently operating in Atlantic City generate over $4 billion in revenues annually, pay more than $300 million in taxes, and provide employment for almost 50,000 people. They also pay approximately 80% of the property taxes in Atlantic City, are serviced and supplied by over 12,000 vendors, and receive more than 30 million visitor trips per year. As is evident, the investment by the casino industry is significant in attracting many tourists to the Atlantic City region.

The economic contributions of the casino industry make it therefore a unique asset which needs to be protected against a terroristic attack. But that protection obviously cannot be achieved by limiting public access to casino facilities. In the wake of 9/11, there has been a lot of discussion

among the Division, the New Jersey State Police, the Atlantic City Police Department and the casino industry as to how best to protect this industry while maintaining its viability.

By way of background, in the immediate aftermath of 9/11, the casinos themselves conducted assessments of their vulnerability to terrorist attack. These assessments attempted to account for the differing levels of security which should be applicable under the color-coded threat assessment levels implemented by the State and federal governments. It was realized that the existing structure of the Casino Control Act, which mandates the existence of casino surveillance and security departments, could be utilized to ensure compliance with the appropriate levels of security based on the color-coded threat assessment system.

Later in 2001, the Domestic Security Preparedness Act of 2001 formally established an Infrastructure Advisory Committee (IAC) as a private-sector component of the Domestic Security Preparedness Task Force. In mandating a public-private partnership, New Jersey recognized that 85 to 90 percent of the infrastructure in the State is privately owned, and that protecting life and property must be undertaken as a joint effort between government and industry. The Task Force has identified a number of key industrial sectors that account for the strength of New Jersey's economy and quality of life. One such sector is sports, entertainment and tourism, with a subsector for casinos and hotel entertainment complexes. Each sector or subsector is paired with one or more state agencies, usually based on prior relationships. The Division has been designated as the liaison to the casino industry.

Since their creation, the Task Force and IAC have been developing "Best Practices" for security. Best Practices for a particular industry represent a baseline security plan that can apply across an entire sector. They focus on prevention, preparation, response to and recovery from terrorist activities. Best Practices include detailed lists of methods, processes, procedures and actions that can be taken to protect the critical infrastructure site. They are developed by IAC private industry sector members, with input from the various state agencies that serve as liaisons to each group, and they include such considerations as:

- Assessing a site's specific vulnerabilities and documenting the methodologies for making these assessments;
- "Hardening," or increasing physical security of the facility, including adding fencing, barriers, and controls for staff and vehicle access;
- Setting up protocols to ensure the continuity of communications;
- Developing and implementing protocols for employee, vendor and delivery person background checks;
- Developing and adopting protocols for adjusting a site's security measures based on changes in the Homeland Security Alert System (HSAS);
- Developing protocols related to cyber-security and the protection of computer content and communications;
- Developing capacity and specific plans to respond to a crisis; and
- Developing contingency and continuity plans to ensure that a site can continue to function or shift functions to another location in the aftermath of a terrorist incident.

The IAC sectors and subsectors submit their Best Practices to the Task Force for review. After its review and approval, the Task Force submits Best Practices to the Governor for his review

and endorsement. When the Governor approves an industry best practice, he or she formally directs the state agency head whose agency is liaison to the sector in question to take certain steps. These include:

- Disseminating the Best Practices to each entity within the sector;
- Encouraging implementation and compliance with the Best Practices by the members of the sector;
- Establishing a capacity to provide training, education and technical assistance for each entity within the sector to ensure implementation and compliance;
- Establishing a capacity to monitor implementation and compliance for each entity within the sector; and
- Reporting back to the Task Force and the Governor regarding the status of implementation and compliance with the Best Practices, with a recommendation whether additional steps are needed.

That brings us to where the Division is now with the casino industry.

The major factors in developing Best Practices for the casino industry involved the protection of the critical assets of the casino industry and the methods for ensuring protection. The critical assets are, first and foremost, the people, along with the hotels, casino equipment and financial assets.

The methods of protecting such assets was made more efficient because of the highly regulated nature of the casino industry. We have in place a system in which casinos are required

to submit internal controls, which set forth in detail how their surveillance and security systems will function. Casinos must adhere to their submitted controls, which are approved by the Casino Control Commission after consultation with the Division. Casinos can be fined for failing to follow their approved controls. Thus, rather than *ad hoc* procedures implemented in response to 9/11, we can use the system of mandated internal controls to implement Best Practices.

The Best Practices for the casino industry were developed by the Division in consultation with casino security directors and State Police assigned to the Division. In determining the Best Practices, which in most cases have been or will be implemented via the internal control process, the Division looked to the existing vulnerabilities of the casino industry and also to appropriate methods to protect against these inherent vulnerabilities.

The vulnerabilities of the industry include the following:

- Casinos are meant to attract the public;
- Employees, contractors and delivery people require back of the house access;
- All the casinos are in a concentrated area and on an island, accessible by boat;
- There are a limited number of egress routes;
- The casinos are located near small airports; and
- Casinos necessarily involve extensive public interaction, including multiple entry points to each casino facility.

Taking into account these vulnerabilities, the Best Practices developed used existing plans which dealt with other types of disasters such as fires, floods and hurricanes, and adapted such plans to deal with the threat or actuality of a terrorist attack. Site vulnerability was addressed by:

- Security and surveillance;
- Monitoring and regulation;
- The training of employees;
- The completion of mandated background checks;
- The formulation of response plans; and
- The creation of back-up systems to continue operations.

Target hardening measures included limitations on parking and deliveries, as well as other access controls appropriate for the color-coded threat level. We also established communications protocols which are required by the internal control submissions. Also mandated are the various levels of licensure and the background checks for employees and vendors. Logical and physical access controls on casino computer systems were instituted to prevent, to the extent practicable, a cyber attack.

The Best Practices for the casino industry were approved by the Task Force and Governor in 2004. Since then, the Division has been working with the casino owners and operators to assist them in implementing the relevant plans. Specifically, we have:

- Taken all appropriate means and made all appropriate contacts to identify all entities which fall within the casino subsector;

- Disseminated the Best Practices to each and every casino hotel facility;

- Made efforts to ensure implementation and compliance with Best Practices throughout the entire casino industry;

- Established a capacity to provide training, education and technical assistance, when appropriate, in the implementation and compliance of Best Practices;

- Established a capacity to monitor implementation and compliance with Best Practices; and

- Reported to the Task Force and the Governor's office on the status of implementation and compliance with Best Practices within the casino industry and made recommendations concerning additional steps needed to ensure compliance or improvement.

I conclude my remarks by expressing my confidences that the work of the Division and the casino industry to ensure effective implementation of the Best Practices will further enhance our goal of protecting New Jersey's citizens, communities, and economy.

Thank you.