NEWS from New York State
OFFICE OF CYBER SECURITY

NYS Division of Homeland Security & Emergency Services

David A. Paterson, Governor **Thomas D. Smith, Director**

Media Contact:
Dennis Michalski
(518) 292-2310
dmichalski@dhses.ny.gov

FOR RELEASE:
Thursday
October 14, 2010

NEW YORK STATE PARTICIPATES IN NATIONAL CYBER SECURITY EXERCISE

The New York State Office of Cyber Security (OCS), Office of the NYS Chief Information Officer and Office for Technology (OFT) participated in the national exercise called Cyber Storm III, the largest information security exercise of its kind. New York State has been participating in the Cyber Storm series since its inception three years ago. Cyber Storm III is sponsored by the U.S. Department of Homeland Security.

"Taking advantage of opportunities like Cyber Storm III to test the processes and procedures that must be implemented during large scale events and to evaluate the skills and training of staff is an important component in the effort to maintain the State's cyber security posture," said Thomas D. Smith, OCS Director. "Exercises like this one help to ensure that New York State is prepared for an effective response to attacks against our critical systems and networks."

"With 19 million New York citizens to support, CIO/OFT provides centralized IT services to more than 95 state agencies, and 60 local government entities. In the event of a major disaster or incident, we must ensure processes are in place to restore and recover the State's mission-critical applications quickly. New York's participation in the Cyber Storm III exercise enables us to strengthen our planning, information sharing and response time to keep our government operating smoothly and without disruption." said Dr. Melodie Mayberry-Stewart, NYS Chief Information Officer and Director of the Office for Technology.

The Cyber Storm series simulates large-scale cyber events and attacks on the government and the nation's critical infrastructure and key resources — so that collective cyber preparedness and response capabilities can be measured against realistic and credible national-level events. DHS's National Cybersecurity Division sponsored the latest installment of the series — Cyber Storm III, which included thousands of players across government and industry and more than 1,500 injects of data to challenge participants.

The scenario incorporated known, credible technical capabilities of adversaries and the exploitation of real cyber infrastructure vulnerabilities, resulting in a range of potential consequences – including the crippling of critical government and private sector functions.

-more-

The participants examined incident response plans and activities as they responded to the large-scale cyber events and attacks on government and national computer systems. The adversary in the exercise launched simulated coordinated cyber and physical attacks on critical infrastructures within selected sectors to meet political and economic goals.

National Participants Included:

- Seven Cabinet-Level Departments: Homeland Security, Defense, Commerce, Energy, Justice, Treasury and Transportation, as well as representatives from the intelligence and law enforcement communities.
- 11 States: California, Delaware, Illinois, Iowa, Michigan, Minnesota, North Carolina, New York, Pennsylvania, Texas, Washington, as well as the Multi-State Information Sharing and Analysis Center.
- 12 International Partners: Australia, Canada, France, Germany, Hungary, Japan, Italy, the Netherlands, New Zealand, Sweden, Switzerland, the United Kingdom. There were only four international partners in Cyber Storm II.
- More than 60 private sector companies: DHS worked with Banking and Finance, Chemical, Communications, Dams, Defense Industrial Base, Information Technology, Nuclear, Transportation, and Water Sectors as well as the corresponding Sector Coordinating Councils and ISACs to identify private sector participants.

For more information on Cyber Storm III, please visit:

- http://www.dhs.gov/files/training/gc_1204738275985.shtm
- http://www.dhs.gov/xlibrary/assets/cyber-storm-3-media-fact-sheet.pdf
- http://www.nationalterroralert.com/updates/2010/09/28/cyber-storm-iii-drill-to-assess-nations-cyber-incident-response-capabilities/
- http://www.networkworld.com/news/2010/092910-cyber-storm-iii-simulates-large-scale.html?source=nww_rss
- http://www.washingtontimes.com/news/2010/sep/28/cyber-storm-iii-aims-protect-against-real-thing/
- http://homelandsecuritynewswire.com/us-battling-simulated-cyber-attack-cyber-storm-iii-exercise
- http://www.dailytech.com/US+to+Kick+Off+Cyber+Storm+III+Exercise+Today/article19742.htm

OCS Website: www.cscic.state.ny.us

###