State of New Hampshire Department of Safety
Robert L. Quinn, Commissioner
Richard C. Bailey, Jr., Assistant Commissioner
Perry E. Plummer, Assistant Commissioner

Homeland Security and Emergency Management
Jennifer L. Harper, Director
Kevin P. LaChapelle, Assistant Director

FOR IMMEDIATE RELEASE
Wednesday, January 08, 2020
Paul D. Raymond, Jr.
Community Outreach Coordinator
C: (603) 892-5804

PRESS RELEASE

OFFICIALS RECOMMEND BEING CYBER SAFE

CONCORD, N.H. – The U.S. Department of Homeland Security recently advised that increased geopolitical tensions and threats of aggression may result in cyber-attacks against the United States.

"There is no known credible threat – cyber, physical or otherwise – to New Hampshire and we remain actively engaged with our federal intelligence partners for emerging threats," NH Homeland Security and Emergency Management Director Jennifer Harper said. "Cyber-attacks have unfortunately become more common as technology has evolved. It is important to understand that everyone is a potential target for cyber criminals."

"Our best line of defense against cyber-attacks is raising awareness among users," said NH Chief Information Officer and Commissioner of the Department of Information Technology Denis Goulet. "Every day, cyber criminals find new and improved ways to access valuable and personal information."

State Executive Branch agency personnel are reminded to follow approved computer and internet policies and procedures, and to report all cyber suspicious activity to the help desk.

Harper and Goulet provide these recommendations for individuals and families:

- Use a strong password that is unique for each device or account. Longer passwords are more secure. To create strong passwords, use simple, long, and memorable passwords or passphrases.
- Use multi-factor authentication, if available. Multi-factor authentication is a more secure method of authorizing access.
- Use internet connections you trust, such as your home service or a connection through your wireless carrier. Public networks are not very secure, which makes it easy for others to intercept your data.
- Keep all of your personal electronic device software current. Manufactures issue updates as they discover vulnerabilities in their products.
- Be suspicious of unexpected emails and do not click on links from unknown or untrusted sources.
- "If You See Something, Say Something®" – Report suspicious activity to 9-1-1 or your local law enforcement agency.

The U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) makes the following recommendations to businesses and organizations:

- Prepare your organization for rapid response by adopting a state or heightened awareness. This ranges from reviewing your security and emergency preparedness plans, consuming relevant threat intelligence, minimizing coverage gaps in personnel availability, and making sure your emergency call tree is up to date.
- Increase organizational vigilance. Ensure your security personnel are monitoring key internal security capabilities and that they know how to identify anomalous behavior. Assess your access control protocols. Flag any known Iranian indicators of compromise and tactics, techniques, and procedures for immediate response.
- Confirm reporting processes. Ensure your personnel know how and when to report an incident. The well-being of your workforce and cyber infrastructure depends on awareness of threat activity. Consider reporting your cyber incidents to CISA as part of an early warning system.
- Exercise your incident response plan. Ensure your personnel are familiar with the key steps they need to take during an incident. Do they have the accesses they need? Do they know the processes? Are your various data sources logging as expected? Make sure personnel are positioned to act in a measured, calm, and unified manner.
- Confirm offline backup. Ensure you have an offline backup of information critical to operations.

Director Harper reminds residents and visitors of New Hampshire to remain vigilant and "If you See Something, Say Something®." Anyone who sees suspicious activity is urged to call 9-1-1; if you are unable to call, you can text 9-1-1 in New Hampshire.

Learn more at ReadyNH.gov, stopthinkconnect.org, and CISA.gov.

###