JB Pritzker, Governor
Sanjay Gupta, Actng Secretary and State CIO

**FOR IMMEDIATE RELEASE:**
June 9, 2023

**FOR MORE INFORMATION:**
Jennifer Jennings
Jennifer.Jennings2@illinois.gov

# Illinois Department of Innovation & Technology offers technical details associated with global ransomware attack

**SPRINGFIELD –** The Illinois Department of Innovation & Technology (DoIT) announced Friday that it is investigating the impact to Illinois after a network of cyber criminals attacked private companies and governments around the world. According to the FBI and the federal Cybersecurity & Infrastructure Security Agency, the attack is believed to have originated when the cyber criminals exploited a vulnerability in a widely used third party file transfer system.

"We all need to be extremely vigilant against cyber attacks – whether we work in the government or private sector," **said Illinois Department of Innovation & Technology Acting Secretary & State CIO Sanjay Gupta.** "DoIT's Infrastructure and Security teams moved quickly to respond to the attack affecting Illinois' network, evicting the attacker within three hours and verifying that the vulnerability could no longer be exploited in our system. We are working with all relevant authorities and will provide regular updates to the people of Illinois."

CISA and the FBI released an alert attributing the worldwide attack to the CL0P Ransomware Gang, which exploited a vulnerability in the third party MoveIT file transfer system. Within minutes of the attack on May 31, DoIT took immediate action, disconnected all associated systems that utilized the third-party software, and engaged its security incident response team to conduct a forensic analysis. In the following days, the worldwide cyber community began to identify the attackers' "fingerprints," and state security officials were able to begin mapping the extent of the attack on Illinois' systems.

DoIT's investigation is ongoing and the full extent of this incident is still being determined, but DoIT believes a large number of individuals could be impacted. DoIT is currently advising impacted agencies and will issue public notice of the incident as expeditiously as possible once DoIT finalizes a determination of all people impacted. At that time, DoIT will also stand up a call center for impacted parties to answer any outstanding questions and provide assistance.

To maintain security, DoIT urges the State to remain vigilant about potential threats and continue to equip staff with the necessary resources to prevent future attacks.

###