CISA, MS-ISAC, NGA & NASCIO RECOMMEND IMMEDIATE ACTION TO SAFEGUARD AGAINST RANSOMWARE ATTACKS

Take the First Three Steps to Resilience Against Ransomware for State and Local Partners

WASHINGTON – July 29, 2019 – The recent ransomware attacks targeting systems across the country are the latest in a string of attacks affecting State and local government partners. The growing number of such attacks highlights the critical importance of making cyber preparedness a priority and taking the necessary steps to secure our networks against adversaries. Prevention is the most effective defense against ransomware.

The Cybersecurity and Infrastructure Security Agency (CISA), Multi-State Information Sharing and Analysis Center (MS-ISAC), National Governors Association (NGA), and the National Association of State Chief Information Officers (NASCIO) are committed to supporting ransomware victims and encouraging all levels of government to proactively protect their networks against the threat of a ransomware attack. Today, we call on our State, local, territorial and tribal government partners, along with the wider cyber community, to take the following essential actions to enhance their defensive posture against ransomware. Through this collective action, we can better protect ourselves and our communities, and further advance the cyber preparedness and resilience of the Nation.

Three Steps to Resilience Against Ransomware:

1. **Back-Up Your Systems – *Now* (and Daily)**
   Immediately and regularly back up all critical agency and system configuration information on a separate device and store the back-ups offline, verifying their integrity and restoration process. If recovering after an attack, restore a stronger system than you lost, fully patched and updated to the latest version.

2. **Reinforce Basic Cybersecurity Awareness and Education**
   Ransomware attacks often require the human element to succeed. Refresh employee training on recognizing cyber threats, phishing and suspicious links – the most common vectors for ransomware attacks. Remind employees of how to report incidents to appropriate IT staff in a timely manner, which should include out-of-band communication paths.

3. **Revisit and Refine Cyber Incident Response Plans**
   Agencies must have a clear plan to address attacks when they occur, including when internal capabilities are overwhelmed. Make sure response plans include how to request assistance from external cyber first responders, such as state agencies, CISA and the MS-ISAC, in the event of an attack.

Additional Resources

- MS-ISAC Security Primer on Ransomware
- CISA Tip Sheet on Ransomware
- NGA Disruption Response Planning Memo
- NASCIO Cyber Disruption Planning Guide

After implementing these recommendations, refer to the ransomware best practices published by CISA, MS-ISAC, NGA, and NASCIO for additional steps to protect your organization.

###