INTRUSION/BREACH

BREACH: This is a successful attempt to get into a system.

INFILTRATION: Means gaining access to a system. Once an infiltration has occurred, a number of things can happen. An intrusion can result in a manipulation of data, exfiltration of data (unauthorized transfer of data from system) or a Denial of Service (DNS).

When the media reports multiple states have experienced attempts against their system, it tells us something positive: The fact that these are attempts and not successful intrusions is a good thing! You are doing your job and your systems have remained protected against malicious attacks.

We have confirmed with DHS that only three instances of actual intrusions have occurred. Illinois' statewide voter registration system was breached earlier this summer with no evidence of manipulation or exfiltration of data. In Arizona, a local jurisdiction experienced a system breach. Again, there was no evidence of manipulation or exfiltration of data, and the state voter registration system was not impacted. Finally, a third party vendor in Florida experienced a breached. This vendor worked with local jurisdictions on their voter registration systems. The state voter registration system was not impacted at all, and this vendor did not work on the state voter registration system.

DHS has assured us that any confirmed breaches will be shared with us immediately. In the meantime, they will continue to share indicators with us. In the weeks before the election, we expect that criminal cyber scanning activity will increase and thus, so will the number of indicators being shared with the states.