HOME CYBER DEFENSE
ARE YOU SAFE FROM CYBER CRIME?
ALERT

Issued 8/25/17

White House Advisors Warn Of Critical Infrastructure Vulnerabilities

A group of advisors to the White House have warned President Donald Trump and his administration of the risk of a cyber attack against critical infrastructure in the United States that could be comparable to the events of September 11, 2001.

The warning came from the National Infrastructure Advisory Council (NIAC), a group commissioned by the National Security Council (NSC) to review more the federal government's capability to secure infrastructure against targeted cyber attacks. In a report published by the NIAC, it called for "direction and leadership to dramatically reduce cyber risks," and warned a failure to take action would leave could result in catastrophic outcomes. "The challenges the NIAC identified are well-known and reflected in study after study," the NIAC wrote. "There is a narrow and fleeting window of opportunity before a watershed, 9/11-level cyber-attack to organize effectively and take bold action. We call on the Administration to use this moment of foresight to take bold, decisive actions."

While the warning from the advisory group was deadly serious, the NIAC presented several recommendations that could help prevent such a disaster from occurring. On the top of the to-do list provided by the council was establishing separate and secure networks for critical infrastructure, including building "dark fiber" networks for traffic from critical control systems, as well as backup communications protocols for emergencies. Such a change would place a gap between the open, public internet and the private communications infrastructure built to allow devices vital to the function of critical infrastructure to communicate. Historically, that is how such systems were built, but as the infrastructure for telecommunications companies changed to meet the demands of the public, it forced utilities companies and other facilities to transfer vital data over the standard wireless protocol used by all data, leaving it potentially vulnerable to interception or attack. Also on the list of suggestions from NIAC was improved information sharing that would allow for quick declassification and improved threat intelligence sharing.

The report also called for improved scanning tools and assessment practices and an exchange program between public and private organizations to strengthen skill sets of IT professionals. To make all of this happen, the NIAC called for the creation of “limited time, outcome-based market incentives” to encourage the owners of critical infrastructure—especially in the private sector—to invest in the necessary technology. While it called for incentivizing the technological advances, the NIAC also made clear such motivations shouldn’t be required. The report found both the government and private sector have “tremendous” resources to invest in cyber defense but have failed to organize, harness or focus them properly. NIAC called for an operational task force comprised of experts from the utilities, finance and communications sectors to team with experts from the government to develop the incentives and bring about the necessary changes as quickly as possible.