PRESS RELEASE

FOR IMMEDIATE RELEASE
May 11, 2017
Larry Clinton
President and CEO, Internet Security Alliance
(202) 236-0001
lclinton@isalliance.org

ISA APPLAUDS TRUMP ADMINISTRATION'S NEW CYBERSECURITY EXECUTIVE ORDER

(WASHINGTON, D.C.) – The Internet Security Alliance (ISA) has come out in support President Trump's new executive order (EO) on cybersecurity. The ISA is also releasing a series of memoranda to the Committees of jurisdiction in the Congress with recommendations for the implementation of the EO.

"This is an EO, not legislation," noted ISA President Larry Clinton, "and it does several things that can be accomplished at this level. For example, we are strongly supportive of having agency heads – not the IT departments – become responsible for cybersecurity. We are also very supportive of switching from the current 'policy-based' approach to cyber practiced in most government agencies to an enterprise risk management approach."

Clinton noted that Agency heads are much like corporate boards who, while expert in their field, may not know much about cybersecurity. "Agency heads are the government equivalent of board members. Just like we have been training corporate boards about how to do cyber risk management, we need similar high level training for the Agency heads. PricewaterhouseCoopers has documented that when boards take this type of training we get bigger budgets, better risk management, better alignment of cyber with organizational goals and a culture of security throughout the organization. That's what we are looking for here too."

Clinton also noted that while risk management has become a buzz word, implementing it at the federal level would have major implications. "GAO has pointed out that most agencies don't follow the risk management model of cybersecurity. They follow the 'policy model' which means check the box on previous policies/standards. The private sector does that too but also does forward looking risk management – anticipating likely attacks, triaging data, etc. As a result, when federal agencies are measured against private organizations, they often come out last in actual cyber measures such as use of best practices and fixing inadequate systems. Actually, doing risk management could go a long way toward improving federal systems," Clinton said.

ISA also pointed to several of its long-standing proposals that seem to be reflected in the EO. "We have long been calling for greater urgency to be applied to cybersecurity and frankly the need to spend more on cyber defense is critical. We are delighted to see that these issues are going to be reviewed and hopefully acted on very short time lines," Clinton said.

"We also are anxious to assist in the required investigation of how the government can assist critical infrastructure more. When this analysis is done, as called for in the EO, we hope that the Agencies follow the wisdom of both the House GOP Task Force on Cybersecurity and Executive Order 13636, both of which advocated the development of market incentives for cybersecurity in critical infrastructure."

"Cyber-attacks are becoming much more sophisticated. Not only do we have nation states robbing banks, but some of the criminal enterprises are becoming as sophisticated as the nation states. Even sophisticated companies are at times fighting above their weight and the problem is even worse for smaller companies. We need to finally address the economic imbalance of cybersecurity, work in a stronger partnership, and build a sustainably strong cyber ecosystem. The EO is one step in that direction."

###