PRESS RELEASE

FOR IMMEDIATE RELEASE December 5, 2016
Larry Clinton
President and CEO, Internet Security Alliance
(202) 236-0001
lclinton@isalliance.org

ISA PRAISES EFFORT TO REFORM CYBER SECURITY AUDITING PRACTICES

(WASHINGTON, D.C.) – "The reality is that in most companies they are more afraid of the cyber auditor than they are the cyber attacker," said Internet Security Alliance (ISA) President, Larry Clinton. "That is why the efforts of the AICPA to make the cyber auditing system more effective and efficient are so important. ISA is delighted to work with the AICPA and the Center for Audit Quality (CAQ) on this effort and congratulates them for their outreach for input."

Clinton, who along with ISA board chairman Jeff Brown of Raytheon, sits on CAQ's Cyber Security Advisory panel and has been working with the two organizations to reform cyber auditing for nearly a year. ISA suggested several fundamental changes to the cyber security auditing process in response to AICPA's detailed proposals on cyber auditing reform in comments filed with AICPA December 5. ISA's full comments can be found at www.isalliance.org

Among the key recommendations made is to stop calling enterprise cyber assessments, audits. "The reality is that these so called cyber security audits are really not audits in the same sense of a financial audit," said Clinton. "A financial audit is really a backward looking, standards based pass-fail proposition – you are either in compliance or you are not. We need an entirely different model for cyber security assessments. We need a forward-looking, risk management model. In addition, if you get a positive a cyber assessment it doesn't mean you are secure. Security is more a question of where you stand on a continuum. Calling these assessments audits is a misnomer, and it is especially critical for government and regulators to understand these assessments are not the same as financial audits."

Consistent with the notion that cyber assessments need to be thought of differently than audits is the recommendation that the method of scoring these assessments also needs to be changed. According to ISA, the current check the box – pass fail system should be replaced with a maturity model including a multi-tiered scoring system that would better reflect an organization's relative degree of security.

"By switching to a maturity model for scoring cyber assessments, organizations will get a better picture of where they stand with respect to their security posture. This will also recognize that not all organizations can meet, or need to meet, the same level of cyber security. For example, using a maturity model would allow smaller organizations within the supply chain to realize and achieve appropriate levels of security consistent with their unique risk perspective. This will make cyber investments more affordable, appropriate and effective," said Clinton.

ISA's recommendations also urge AICPA to broaden the focus of assessments beyond just IT, to base their measurements on proven cost effective security practices and to undertake increased training of cyber assessors to assure quality of the assessments.

About ISA: *The Internet Security Alliance (ISA) is a trade association with members from virtually every critical industry sector. ISA's mission is to integrate advanced technology with economics and public policy to create a sustainable system of cybersecurity. ISA pursues three goals: thought leadership, policy advocacy and promoting sound security practices. ISA's "Cybersecurity Social Contract" has been embraced as the model for government policy by both Republicans and Democrats. ISA also developed the Cyber Risk Handbook for the National Association of Corporate Directors. For more information about ISA, please visit www.isalliance.org or 703-907-7090.*

###