IAITAM: TIME FOR WASHINGTON TO “BUILD THE WALL” SEPARATING TAXPAYERS FROM CYBERATTACKS AND WASTEFUL IT/IT SECURITY SPENDING

“Don’t Build This Wall with Dollars Frittered Away on More Federal IT & IT Security Spending; We Need Best ITAM Practices Now Across the Board”; IAITAM Echoes Call Made in 2015 “IT Insecurity” Report.

CANTON, OH – August 1, 2019 -- Responding to the “Federal Cybersecurity: America’s Data at Risk” report released this month by U.S. Senators Tom Carper (D-Del.) and Rob Portman (R-Ohio), the International Association of IT Asset Management (IAITAM) said today that no further delays are acceptable and that Washington should proceed now to “build the wall that will protect taxpayers from cyberattacks from outside and billions of dollars in wasteful federal spending on Information Technology (IT) and IT security on the inside.”

The new Carper/Portman analysis echoes the February 2015 IAITAM report, "Understanding the Federal Government's 'IT Insecurity' Crisis," which concluded that half or more of the $70-$80 billion the U.S. government spends each year on IT/IT security is wasted and actually leaves federal agencies in greater danger of breaches, lost and stolen hardware, the use of outdated software, missing software patches and other cybersecurity dangers.

2015 report author and IAITAM CEO Dr. Barbara Rembiesa said: **“You can’t build the wall we need to protect taxpayers and sensitive federal data by wasting billions more dollars on random IT spending and cybersecurity measures that vary wildly from federal agency to federal agency. By focusing largely on hacks and other breaches, elected officials and agency administrators are failing to take a bottom-up approach to the purchase, control, inventory, and proper destruction of such IT assets as software, computer hard drives and mobile devices. With no meaningful standards and controls in place across and even within federal agencies, the result is massive waste, inefficiency, and huge vulnerabilities that can easily be exploited by bad actors inside and outside of the system.”**

The 100-page Carper/Portman report gauges the strength of information security standards at eight federal agencies: The Department of Homeland Security, Department of State, Department of Transportation, Department of Housing & Urban Development, Department of Agriculture, Department of Health & Human Services, Department of Education, and the Social Security Administration.

The findings demonstrated a wide range of pervasive cybersecurity failures, all of which jeopardize to varying degrees the privacy and well-being of American citizens. The executive summary of the Carper/Portman report flatly states that the eight “agencies currently fail to comply with basic cybersecurity standards.”

The years 2006-2015 saw an increase in reported cybersecurity events by over 1,300 percent. Federal agencies reported 35,277 cyber incidents in 2017 alone.

Some of the most notable screwups cited by Carper/Portman include outdated systems and lapses in routine maintenance of IT equipment, all of which can be addressed through the Information Technology Asset Management (ITAM) recommendations outlined in 2015 by IAITAM. For example, the Department of Transportation hosted a system that was approaching its semicentennial (or half-century) anniversary. Six agencies failed to act on security vulnerabilities within a timely fashion.   Proper use of ITAM procedures would have required that these and other deficiencies be addressed before harm could be done.

Untracked hardware and software were discovered at five of the eight agencies. This issue falls under the core of ITAM best practices, which operate on the rule that you can't manage what you can't count. Having an up-to-date IT asset inventory is essential for any organization, regardless of size.

The authors of the Carper/Portman report concluded: "Despite major data breaches. the federal government remains unprepared to confront the dynamic cyber threats of today. The longstanding cyber vulnerabilities illustrate the federal government's failure to meet basic cybersecurity standards to protect sensitive data."

In May 2019, IAITAM backed calls by the Trump Administration to bolster IT security infrastructure through a cybersecurity initiative to move the U.S. in that direction.

In December 2018, IAITAM predicted that 2019 would be the "breakthrough" year for IT Asset Management and related cybersecurity initiatives.

Following ITAM best practices is a roadmap for organizations to protect and get the most out of their IT assets. IAITAM offers courses and training opportunities throughout the year for agencies and businesses seeking to strengthen their cybersecurity and IT management.

ABOUT IAITAM
The International Association of Information Technology Asset Managers, Inc., is the professional association for individuals and organizations involved in any aspect of IT Asset Management, Software Asset Management (SAM), Hardware Asset Management, Mobile Asset Management, IT Asset Disposition and the lifecycle processes supporting IT Asset Management in organizations and industry across the globe. IAITAM certifications are the only IT Asset Management certifications that are recognized worldwide. For more information, visit www.iaitam.org, or the IAITAM mobile app on Google Play or the iTunes App Store.

MEDIA CONTACT: Whitney Dunlap, (703) 229-1489 or wdunlap@hastingsgroup.com