IAITAM: "MASSIVE WASTE" IN FEDERAL IT SPENDING MAKING CYBERSECURITY A BIGGER PROBLEM FOR GOVERNMENT AGENCIES

Bad News for Taxpayers: "High Tech Equivalent of $436 Pentagon Hammer" Seen in Tens of Billions of Dollars in Bloated Federal IT-Related Spending; Lack of Focus on "IT Asset Management" Actually Increasing Risks of Lost and Stolen Hard Drives, Outdated Software and Other Risks.

WASHINGTON, D.C. & CANTON, OH.///February 5, 2015///Half or more of the $70-$80 billion the U.S. government spends each year on Information Technology (IT) and 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is wasted and actually leaves federal agencies in greater danger of breaches, lost and stolen hardware, the use of outdated software, missing software patches and other cybersecurity dangers, according to a report issued today by the Canton, OH-based International Association of Information Technology. An example of out-of-control IT spending cited in the report: One federal agency not involved in national security – the US Department of Education -- spends more than 30 times more per employee for IT than the average for American private industry.

The IAITAM report cautions that until the federal government adopts a rigorous approach to IT Asset Management (ITAM), it is unlikely to stem IT-related failures seen recently at the Internal Revenue Service, the White House, State Department, and the Veteran's Administration.

Available online at http://bit.ly/iaitamnews the report titled "*Understanding the Federal Government's 'IT Insecurity' Crisis"* notes that 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. The federal government spends about $70 billion a year on IT purchases and an average of about $10 billion a year on IT security. 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 from those inside and outside of the system.

As the IAITAM report notes, two recent analyses concluded that private industry in the United States spends an average of $4,600-$4,900 per employee on IT – less than $5,000 a head. By contrast, the federal government spends over $36,000 per employee on IT. As the report notes: **"This suggests that the federal government spends an astonishing six times more per employee on IT than does private industry. As if these overall figures were not eye popping enough, the variations by federal agency are even more extreme, including more than $168,000 per U.S. Department of Education employee and more than $109,000 per U.S. State Department employee! It is not comforting to see that the most reasonable (in relative terms) level of spending is at the technology-challenged Veteran's Administration at nearly $11,700 per employee, a level still well over twice what private industry pays in the U.S."**

Report author and IAITAM CEO Dr. Barbara Rembiesa: **"Taxpayers need to understand that simply throwing more dollars at Information Technology (IT) and IT security is not a solution for anything other than mind-boggling waste of public funds. While awareness of the federal IT security problem has grown in recent months, the ability to deal with such threats has improved very little. Right now, we have the high-tech equivalent of the $436 Pentagon hammer and it's just getting worse. Federal IT chiefs often cite inadequate funding as the biggest inhibitor to progress, but a thorough investigation of the overall federal government IT sector reveals that cost savings and IT security would be increased by a comprehensive ITAM program at the national government level in the U.S. Just as importantly, more tightly controlled spending would actually reduce the IT failures now plaguing federal agencies."**

As the IAITAM report notes: **"It is important to understand that in addition to breaches, there is a huge potential for cutting wasteful spending through IT Asset Management that would save taxpayers substantial sums of money. It has been estimated that the Department of Homeland**

Security alone saved $181 million in software licensing in one recent year, and that more than $1 billion could be saved in information technology and telecommunications per year across the federal government if best practices were applied."

Examples of IT failures cited in the report that could be addressed through better ITAM practices include:

- ***Risk of lost or stolen hard drives.*** An October 2014 Inspector General (IG) report of a sample of laptops at the Securities and Exchange Commission (SEC) found that 17 percent of laptops had an incorrect location, 22 percent had incorrect user information, and 5 percent -- 24 of 488 laptops – were missing altogether. Based on the sample reviewed, the IG concluded that more than 200 SEC laptops were totally unaccounted for. A November 2014 IG Report found that mobile device management is poor at the IRS. Nearly three out of five (57 percent) of mobile device inventory records were incorrect at an agency where 94 percent of employees are provided with a mobile device.

- ***Failure to make needed changes.*** In November 2014, the Veteran's Administration (VA) failed its annual cyber security audit for its 16th consecutive year, after having failed to put in place earlier recommendations. Even after a dramatic cyber hack was detected in 2012, the GAO found that the VA has not addressed an underlying vulnerability that allowed the incident to occur. Between fiscal year 2011 and 2013, the IG made 55 recommendations for improving overall IT security. Less than half (21) had been addressed with corrective action at the time of the November 2014 report.

- ***Outdated/mismanaged software.*** According to a Department of Homeland Security IG report, Homeland Security's FEMA and United States Citizenship and Immigration Service (USCIS) were found to still be using the Microsoft Windows XP operating system, which remains vulnerable to attack as Microsoft stopped providing software updates to mitigate security vulnerabilities in April 2014. A November 2014 IG report found that US Department of Agriculture did not have a process for timely and secure installation of software patches, despite requirement. The IG found that an astounding 82.5 percent of correctable vulnerabilities at one USDA agency were not patched when one was available.

- ***Mishandling of device licensees/fee payments.*** The IRS was found in a 2014 IG report to be paying monthly service fees for almost 6,800 devices that were not inventoried (almost 17 percent of total devices, and almost $2 million per year in service fees). For more than 700 employees, the IRS paid for multiple mobile devices (between two and five) despite the prohibition against multiple devices.

- ***Inappropriate system authorization and documentation.*** About one quarter (24 percent) of IT systems in the U.S. Department of Education network were found to be operating on expired security authorizations.

The IAITAM report concludes:

"At the root of much of what ails the federal government bloat in Information Technology (IT) spending and related woes is a lack of meaning IT Asset Management. ITAM is the bridge that links an organization's financial, contractual, and physical IT inventory requirements with the goals and objectives of the operational IT environment.

The Federal Government's approach to ITAM should include two components:

- The first is a rigorous government-wide centralized ITAM program responsible for creating policies, procedures, processes, and metrics for all government agencies.

- The second is an agency level ITAM team, which would include the day-to-day management of all assets within that agency as set forth and required by the centralized program.

Concurrently legislation should be enacted to protect and manage our greatest resource (technology) at the federal level, state level, and in critical infrastructure in the private sector. This legislation should address the areas of procurement, disposal, inventory management to the component level of IT Assets (such as hard drives) , data security, and other mandated policies which would mitigate the risk to the United States and the critical infrastructure that is not owned by the government but is enabled and regulated by legislation."

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: Will Harwood, (703) 276-3255 or wharwood@hastingsgroup.com.

EDITOR'S NOTE: A streaming audio replay of the news event will be available at 5 p.m. EST/ 2 p.m. PST on February 5, 2015 at http://www.iaitam.org.