IAITAM: WIDESPREAD FAILURE OF FEDERAL AGENCIES TO INSTALL ANTI-SPOOFING EMAIL TOOL SHOULD HAVE TAXPAYERS "UP IN ARMS"

"No question here about what needs to be done; the only mystery is why the federal government can't get its act together and start looking out for the interests of taxpayers."

CANTON, OH – January 18, 2018 – With an estimated one out of eight emails that appear to come from federal government accounts actually being fraudulent, it is "totally unacceptable and a complete dereliction of duty to taxpayers" that almost half (45 percent) of federal agency email domains have failed to meet a deadline to install anti-spoofing software, according to Dr. Barbara Rembiesa, president and CEO of the International Association of IT Asset Managers (IAITAM).

IAITAM has long been critical of the failure of federal agencies to maintain proper Information Technology Asset Management (ITAM) procedures, including the proper accounting for all hardware and rigorous maintenance of software, with timely installation of patches and upgrades. See: http://ws.iaitam.org/Misc/IT_Government_Insecurity_Report_v2.5.15.8.pdf and http://iaitam.org/iaitam-new-release-tax-dollars-not-work-plan-ending-massive-waste-tech-insecurity-irs/.

A new review by ValiMail (http://www.nextgov.com/cybersecurity/2018/01/45-percent-federal-email-domains-miss-security-deadline/145220/) found that 45 percent of federal agencies missed a Homeland Security Department deadline to install a new anti-spoofing email security tool. Ironically, the Homeland Security Department was among the worst offenders with 85 percent of its own email domains not protected. The new tool is designed to eliminate or substantially reduced phony (or "spoofed") email that appears to be coming from U.S. government agencies.

According to NextGov: "DMARC, which stands for Domain-based Message Authentication, Reporting and Conformance, essentially pings a sender's email domain—irs.gov, for example—and asks if the sender — say, martha.stewart@irs.gov — is legitimate. If the domain says the sender is illegitimate, DMARC can send the email to the recipient's spam folder or decline to deliver it entirely."

IAITAM President and CEO Barbara Rembiesa said: **"What is it going to take for the federal government to start taking its email situation seriously? You would think that the Clinton email scandal would have caused people to sit up and start flying right when it comes to managing federal email systems, but here we see new evidence of something that is totally unacceptable and a complete dereliction of duty to taxpayers."**

Rembiesa added: **"Where is the focus on Information Technology Asset Management in federal agencies? Heads would roll at private sector companies that allowed a deadline like this to be missed at half of all domains targeted for a major software upgrade or addition like this. It is astonishing to me that a need could be identified, a solution chosen, and a deadline set, and then have this much failure result. The federal government is never going to clean up its IT-related waste and inefficiency until it streamlines federal technology purchasing and oversight and imposes consistent rules with real consequences for non-compliance."**

Rembiesa concluded: **“There is no question here about what needs to be done; the only mystery is why the federal government can’t get its act together and start looking out for the interests — and dollars — of taxpayers.”**

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: Alex Frank, (703) 276-3264 or afrank@hastingsgroup.com.