# GROUP: TRUMP CAN TAKE NEEDED NEXT STEP TO END MAJOR FEDERAL PRIVACY THREATS TO U.S. AND EU CITIZENS

***In Wake of Recent Executive Order on Privacy, President Has Big Opening to Address Wider Problems Posed by Government Agencies Hit by Hacking, Data Breaches and Wasteful Spending.***

**WASHINGTON, D.C. & CANTON, OH.**///**February 14, 2017**///President Trump issued a major privacy-related executive order on January 25th and now is positioned to take the needed additional steps to crack down on the inadequate internal controls, wasteful spending, and data breaches that "puts at risk the personal data of every individual processed" by federal agencies, according to an analysis by the International Association of Information Technology Asset Managers, Inc. (IAITAM). The organization also indicated that the danger posed to personal data could be remedied by the federal government adopting needed IT Asset Management (ITAM) controls.

On January 25th, 2017, President Donald Trump signed an executive order titled Enhancing Public Safety in the Interior of the United States. This Executive Order states, in part: *"Sec. 14. Privacy Act. Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information."*

While initial concerns about the Trump executive order focused on a potential threat to the EU-US Privacy Shield, IAITAM said the reality is that EU citizens are now being dealt with by the federal agencies subject to the executive order in the same way that US citizens are.

IAITAM CEO Dr. Barbara Rembiesa said**: "President Trump should seize the initiative here and take the necessary next steps. The real problem here is putting the federal government in charge of privacy. Unfortunately, the US government has shown it is not equipped to successfully process privacy data. What is at risk here is the personal data of every individual processed by federal agencies. The privacy threats are widespread and include the IRS, the White House, the State Department, and the Veteran's Administration."**

Focusing on the needed solution, Rembiesa said: **"At the root of much of what ails the federal government bloat in IT spending and related woes is a lack of meaningful 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."**

How bad is the problem?

Every year, there are tens of thousands of cybersecurity and data integrity incidents involving federal agencies, including the following recent cases:

1. Social media hack within the Department of Defense/ U.S. Central Command.
2. China-linked state-sponsored cybersecurity attack on personnel information within the U.S. Postal Service.
3. A State-sponsored Russian intrusion into unclassified networks within the White House.
4. State-sponsored Chinese hacker entered into the Department of Defense/ U.S. Transportation Command.
5. Inspector-General reports of the Nuclear Regulatory Commission being hacked three times in three years.
6. A primary US security clearance contractor being compromised within the U.S. Investigation Services.
7. An unclassified email network hacked into within the U.S. State Department.

How would ITAM address these problems and others?

According to the IAITAM analysis: “With so many federal agencies being compromised on a regular basis it becomes readily apparent that granting personal data processing to these federal agencies puts the data and the people at risk. The historical precedent shows that the US Government is not currently prepared to handle the responsibilities necessary to process data as well as protect it. There needs to be a stop-gap between the processing of the data and the inability to protect it. The only way to successfully do that is to institute and enforce a mature and robust ITAM Program …”

“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. “

The IAITAM analysis concludes: “… 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. (IAITAM) 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 of every size 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:** Natalie Watson, (703) 276-3256 or nwatson@hastingsgroup.com.