NEW TRUMP MOVE WILL BOOST CYBERSECURITY WITH ITAM PROTECTIONS, ENCOURAGE K-12 FOCUS ON MORE SECURE CYBERSPACE

Creating a Pathway to Address the Challenges of 21st Century Security Issues

CANTON, OHIO -- May 9, 2019 – In a bid to augment traditional IT security programs in the federal government and corporate America, President Donald Trump has signed an executive order that will foster greater reliance on IT Asset Management (ITAM) principles as America wages its war against cyber-attacks. The Trump move also aims at making cybersecurity a part of elementary and secondary school curriculums.

Dr. Barbara Rembiesa, president and CEO of the International Association of Information Technology Asset Managers (IAITAM), praised Trump’s efforts to build a team that will be better able to meet the challenges of 21st century security issues now plaguing cyber systems.

“President Trump’s executive order will help create a professional pathway for IT Asset Managers who want to join the fight against the ruthless predators who seek to compromise our data infrastructure,” said Rembiesa. “The training opportunities that this order promotes will help pull practitioners out of their individual silos and create education opportunities in cybersecurity beginning in childhood through advanced certification as adults.”

“I’ve said in the past that you cannot secure what you don’t know you have,” said Rembiesa. “Before we can have a discussion about the technology necessary to block these cybersecurity breaches, we first need to identify what we have in our IT inventory.”

Foundational ITAM practices that involve 12 Key Process Areas are part of the core concepts in the seven certification courses IAITAM offers. One of those courses – Certified Asset Management Security Expert (CAMSE) – teaches IT Asset Managers how to empower IT security to leverage the knowledge generated by the ITAM program. That includes understanding what assets an organization has, where they are and how they are being used. With that knowledge, security will come from the power to mitigate risk to the environment.

“The goal is to quantify the IT environment and reduce the complexity of those IT assets, which in turn will reduce the number of opportunities for loss, theft and piracy,” said Rembiesa. “Establishing policies to help simplify the management of those IT assets, educating their users about those policies and keeping open lines of communication with those affected are essential to cybersecurity success.”

The White House announced in a statement last week that Trump’s order will strengthen the cybersecurity workforce in the U.S. and help fill more than 300,000 vacancies that risk “our critical infrastructure, national defense and modern economy.” The order focuses on promoting STRONG job opportunities and encourages wide adoption of the workforce framework created by the National Initiative for Cybersecurity Education (NICE).

The latest executive order builds on the president’s efforts to protect critical IT infrastructure. Last year, the president released a National Security Strategy that prioritized a strong cybersecurity workforce.

Trump also signed an executive order in 2017 to strengthen the cybersecurity of federal networks and critical systems.

Meanwhile, the National Institute for Standards and Technology (NIST) – which developed the NICE model – also said in its 2018 Framework for Improving Critical Infrastructure Cybersecurity that creating a mature ITAM program that begins with identifying IT assets is the first critical step in developing a plan to combat cybersecurity issues. A mature ITAM program is one that includes well-established, repeatable best practices and manages IT assets based on exception.

Cybersecurity issues have dominated information technology headlines internationally during the past decade. A study released in March by Kaspersky Lab found that more than 54 percent of European organizations said they had experienced a cybersecurity attack during the past two years, leading to an interruption in their business activities. That same month, aluminum producer Norsk Hydro was hit by ransomware that shut down global operations. That attack cost the Norway-based company about $50 million, according to recent reports.

Norsk Hydro is hardly alone. Equifax, Target, Home Depot, Subway, Goodwill Industries, JPMorgan Chase, Visa and MasterCard have all had a major cybersecurity breach in just the past six years. The number of organizations affected by a cybersecurity issue has become so large that some have argued it would be impossible to include them all.

The White House said in its statement that the president's most recent order would allow federal workers to temporarily be reassigned to other agencies so they can increase their cybersecurity expertise. Trump also created a new President's Cup Cybersecurity Competition and the Presidential Cybersecurity Education Awards. The latter of those will recognize elementary and high school teachers who include cybersecurity-related content in their classrooms.

Federal agencies will also create cybersecurity aptitude assessments that they can use to reskill employees and train future talent.

"America built the internet and shared it with the world," said Trump. "Now we will do our part to secure and preserve cyberspace for future generations."

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.