MEP
MANUFACTURING EXTENSION PARTNERSHIP

Growth Based Solutions for Manufacturers

For Immediate Release
July 5, 2017

For More Information Contact:
Zenagui Brahim
President, NH MEP
603-226-3200

Smaller Defense Contractors Face Big Security Changes

NASHUA, NH - As the Dec. 31 deadline looms for defense contractors to comply with new cybersecurity requirements, New Hampshire business leaders gathered last week to hear about the program's importance.

"It seems like every day we wake up, and there is a new story on the news - something has happened in cybersecurity, new ransomware, some other company has been hacked, a government agency or your insurance company or where you shop," said Patricia Toth of the National Institute of Standards and Technology. "It doesn't matter where it is. We are all vulnerable to cyber attacks."

Toth, one of the architects of the NIST SP 800-171 standard, presented an overview of the new technical requirements that defense contractors must be in compliance with by year's end.

Protecting sensitive government data from hackers is the primary objective of the new requirements, particularly controlled, unclassified information, Toth said.

Contingency planning, disaster recovery plans, physical security and access control are all necessary to keep private company data - as well as customer information - secure, she told the audience at a cybersecurity conference hosted by the New Hampshire Manufacturing Extension Partnership and the New Hampshire Government Contracting Assistance Center.

"Small-business people, generally when they are dealing with contract information from the Department of Defense, the major requirement is for confidentiality," Toth said.

There are 14 different families of security controls included in the new requirements, addressing issues such as media protection, personnel security, risk assessment, access control, awareness training, audit and accountability.

As larger companies ramp up their security measures, smaller businesses are being targeted by hackers, she said.

"Do you have a plan in place when something does happen in your business?" Toth asked, stressing the importance of small businesses being able to restore their computer systems. While a series of technical controls may be necessary to prevent cyber attacks, policies and procedures must also be in place to address natural disasters, structural failures and more.

"We are also concerned about human errors," she said, explaining untrained employees or new employees could mistakenly open a file they should not have, or allow someone to enter the building who should not be there.

One click on a computer can cause devastating consequences, and security controls need to be in place to protect sensitive government data, Toth said.

"Small businesses tend to grow rapidly. You need to build in some of that maturity," she said.

Some of the new requirements include limiting system access to authorized users, limiting unsuccessful login attempts, automatic lock out after unsuccessful login tries, recognizing and reporting insider threats, employee security awareness training, annual refresher training, establishing and enforcing security configuration settings for information technology products employed in organizational information systems, tracking and reviewing audit changes to information systems and more.

Protecting defense information is critical, and the concept is not new, said David Pease, program manager with the New Hampshire Government Contracting Assistance Center. Now, however, he said there is a stable set of rules and standards that should help guide businesses into the future.

"We understand why this is necessary. What we don't understand is what we need to do to comply - what is it going to cost my business?" said Pease, describing the new requirements as somewhat complicated.

Zenagui Brahim, president of the New Hampshire Manufacturing Extension Partnership, agreed that the headaches related to cybersecurity must be addressed in order to protect client data.

“Defense contractors need to fully understand what must be done to reach full compliance in just a few months,” Brahim said.

-END-