The Palm Beach Post

Point of View: Cybersecurity keeps Florida's defense supply chain safe and competitive

Tom Feeney

Palm Beach Post
Published 7:46 a.m. ET Sep. 13, 2020

The U.S. Department of Defense (DoD) will soon require all contractors to meet new, enhanced cybersecurity standards under the new Cybersecurity Maturity Model Certification (CMMC) regulations. This will apply to every company that does business with the DoD at all points along the defense supply chain. In Florida alone, tens of thousands of businesses will be impacted and will need to take action soon to comply with these new standards to ensure they can continue to compete for DoD contracts and maintain their operations.

Essentially, the goal of the CMMC is to help ensure that a company's cybersecurity infrastructure is capable of safeguarding sensitive government information. In our current day and age, cybersecurity attacks are a known threat to every business, large and small, and their infrastructure must be protected appropriately — especially when information related to our nation's military is involved.

Heightened cybersecurity regulations, such as the CMMC, are important because they help keep our state and businesses safe from these ever-evolving attacks. And by stepping up to meet these new regulations, Florida's defense industry can remain competitive in the global marketplace.

Florida's defense industry is a vital part of our economy, and it is growing. According to the 2020 Florida Military and Defense Economic Impact Study by Enterprise Florida, it provides nearly 915,000 jobs throughout the state and accounts for a $95 billion annual economic impact — growing by more than 100,000 jobs and $10 billion over just two years.

And now is not the time to take a step back. The jobs provided by this industry are high-value and high-wage — exactly the type of opportunities we want to continue to increase for Floridians. During a time of economic recovery, it is especially important that we are proactive in protecting one of our state's top economic drivers and job creators.

It will be vital for Florida businesses in the defense supply chain to get in front of these new federal cybersecurity regulations. Impacted businesses need to review the new requirements and evaluate their current cybersecurity practices and potential gaps. There will also be a multitude of training opportunities available that businesses are encouraged to take advantage of.

In fact, the Florida Department of Economic Opportunity (DEO) recently announced it has received more than $1 million in funding from the DoD to establish the Florida Defense Cybersecurity Training Program, which will help ensure small and medium-sized defense contractors are aware of and comply with the DoD's regulations for cybersecurity, including the new CMMC standards. The program will include a series of educational events, as well as training modules for companies within Florida's defense industry.

Additionally, on September 16-17, the Foundation of Associated Industries of Florida, DEO, FloridaMakes and Workers' Compensation Institute will co-host the Cybersecurity Forum 2020, where DEO will conduct a statewide education event on the CMMC, as well as its impact on Florida's defense industry, and provide further details on the Florida Defense Cybersecurity Training Program.

While meeting these new regulations may seem like a daunting task for many impacted Florida businesses, it is critical to protecting our businesses' ability to work with the federal government. And by doing so, we will also help strengthen, protect and ultimately grow Florida's defense industry.

TOM FEENEY, TALLAHASSEE

Editor's note:
Feeney is the president and CEO of Associated Industries of Florida, and served as Speaker of the Florida House of Representatives from 2000-2002.