Statement for the Record

Dr. Jane LeClair, Chief Operating Officer

National Cybersecurity Institute at Excelsior College

Before the

United States House of Representatives

Committee on Small Business

Small Business, Big Threat:

Protecting Small Businesses from Cyber Attacks

April 22, 2015

Mr. Chairman and members of the Committee, on behalf of the National Cybersecurity Institute at Excelsior College I appreciate the opportunity to address you and provide a statement for today's hearing. The National Cybersecurity Institute is dedicated to increasing knowledge in the cybersecurity discipline and assists small businesses (SMB's) to better understand and meet the challenges in today's digital world. My name is Dr. Jane LeClair, and I am the Chief Operating Officer of the National Cybersecurity Institute located in Washington, D.C.

SMB's are challenged both by the ability and the desire to secure themselves against cyber threats which makes them uniquely vulnerable to cyber attacks. Fifty percent of SMB's have been the victims of cyber attack and over 60 percent of those attacked go out of business. Often SMB's do not even know they have been attacked until it is too late. SMB's are under attack from many avenues including social engineering, the internet of things, insider threat, weak passwords and cyber theft through weak payment systems. Mobile devices and the lack of formal cyber plans and policies spell trouble. Infections brought in through browsers pose a threat, and finally, outdated technology and poor maintenance top the list of problems. SMB’s are characterized by central management focused around the owner, with lack of a specialized IT or cyber staff, inadequate control systems, and day-to-day rather long term planning for asset protection. Almost 70% of SMB’s manage their own websites, use the Internet for sales, social media, marketing, and a host of other needs. SMB’s have resource constraints and often ignore cyber-security in favor of day-to-day operations or other financial needs. Yet SMB’s remain a gateway to gain access to clients, business partners, donors, and contractors working with the SMB . . . a backdoor into many large organizations. These organizations frequently lack the knowledge needed to develop and implement a cyber policy or the expertise to develop a response strategy. Surprisingly, 96% of the attacks on SMB’s were fundamentally basic attacks. SMB’s need employees trained in networking, operating systems and multiple layers of security. Otherwise, who’s watching for signs of an attack and making sure the operating systems are properly patched? Who’s responsible for regular backups and reviewing system logs?

There are several ways that the National Cybersecurity Institute is offering assistance to SMB’s. An affordable package that provides a targeted cybersecurity plan, basic training for owners, IT staff and employees, and ensures that the basics of antivirus software and firewall protection are in place, is under development. Our media campaign raises awareness through quarterly webinars and weekly blogs. The National Cybersecurity Institute is publishing two short books on Cyber for Small Business and Cyber Insurance, and is partnering to offer a SMB workshop in medium-sized cities around the country that is affordable and aimed at SMB owners and their IT staff. Cybersecurity is without a doubt one of the prime concerns of the SMB community in America today. The efforts of this Committee in seeking ways to help alleviate those concerns cannot be understated. Mr. Chairman and members of this Committee, thank you for your interest in this important area, and I thank you for the opportunity to address you today.