WRITTEN TESTIMONY OF RICHARD MAHLER
ON BEHALF OF REVOLUTIONARY SECURITY

TESTIMONY BEFORE THE NEW YORK STATE SENATE
STANDING COMMITTEE ON INVESTIGATIONS AND GOVERNMENT OPERATIONS AND
STANDING COMMITTEE ON VETERANS, HOMELAND SECURITY AND MILITARY AFFAIRS

"A DISCUSSION ON CYBER-SECURITY IN NEW YORK STATE."

New York, NY
OCTOBER 24, 2017

Senator Murphy, Senator Croci, and members of the Committees, thank you for the opportunity to submit this testimony regarding the cyber security threats challenging our citizens, our government, and our private industry throughout New York and the United States.

My name is Richard Mahler, and I am Vice President of Revolutionary Security, LLC. Revolutionary Security is a cyber security professional services firm working with leading critical infrastructure companies to defend against cyber threats. I have spent 15 years of my career on this issue and I have seen it grow from a topic limited to the geek and technical community to the ubiquitous coverage it now receives in the news daily. The risks associated with cyber security incidents continue to escalate at a rapid pace and they are receiving Board-level attention from the private firms across the State of NY and around the nation. The State of NY and its private firms have a critical leadership role and influence the national and global discussions on the topic of cyber security.

Being here in New York, I naturally first think of the financial services industry. As a whole, the financial services industry is a leader in understanding the threat landscape and making significant investments to mitigate the risk. Large individual firms have increased their cyber

security budgets by hundreds of millions of dollars. The industry also has a mature, effective, and collaborative approach to understanding and fighting the threats. The Financial Services Information Sharing and Analysis Center (FS-ISAC) and its Financial Systemic Analysis and Resilience Center (FSARC) identify and reduce systemic risk in the sector by working collaboratively across the sector and with the Federal government. The FS-ISAC and FSARC are recognized as the model for effectiveness and cooperation for other industries to emulate.

The State of New York is also making a significant effort to help reduce the cyber risks across the state. For example, the New York Department of Financial Services (DFS) issued Part 500 of Title 23, which set the requirements that "Covered Entities" and their third-party partners must meet to ensure secure and resilient operations. In the wake of the Equifax incident, DFS extended these regulations to the credit monitoring services. Last month, I participated in the Life Insurance Council of New York (LICONY) conference and was pleased to learn that the National Association of Insurance Commissioners (NAIC) is proposing a national standard modeled on the NY DFS regulations, as opposed to creating another unique set of requirements.

Unfortunately, the approach taken by the NAIC is not the path most regulating bodies are following. Since the beginning of 2015, there have been over 40 different regulatory requirements, issuances, guidelines, advisories and proposals from 17 different U.S. federal and state regulators levied on financial services firms. Additionally, 48 states in the U.S. have their own individual breach notification requirements. Globally, the European Union (EU) is applying the General Data Protection Regulation (GDPR) to all industries with data in the European Union or about EU citizens. China has implemented its intentionally vague cyber security requirements

for firms doing business in that country. Other nations also have their own individual data security and privacy regulations. I encourage all state and federal regulators, wherever possible, to harmonize on common standards such as the NIST Cyber Security Framework or sector-specific derivative models, rather than creating new regulations.

The current regulatory patchwork requires that firms, including NY firms operating in multiple industries and/or multiple states and nations, have a tremendously complex compliance structure. The impact is that precious resources, both people and money, that should be spent reducing the firm's risks and protecting the firm's clients are diverted toward frequently redundant compliance efforts and the corresponding preparation, internal assessments, external audits, and reporting.

Beyond financial services, another critical area that requires attention is the Industrial Control System (ICS) or Industrial Internet of Things (IIOT) landscape. These are the unique systems that power the energy, transportation, manufacturing, and other critical infrastructure industries. These systems also usually have environmental, health, and safety considerations. Here is where cyber incidents have the potential to have significant physical impacts. The Department of Homeland Security (DHS) and various state and industry-specific organizations have modeled scenarios in each of these industries that could result in loss of life or serious environmental impact. However, these systems and the environments in which they operate are unique, often decades old, and cannot be assessed, monitored, or tested in the same way that we would evaluate and secure traditional IT systems. One of the critical issues limiting progress in securing these systems is the drastic shortage of talented, experienced professionals that

understand the unique operating environments of these systems, how to properly assess their cyber risks, and how to implement appropriate security programs that will not adversely impact operations.

That brings me to my final point, and one where I think New York can strategically address cyber security with positive lasting impacts. The evolution of technology continues to accelerate. This brings new risks at an almost daily rate. At the same time, innovative companies and entrepreneurs are devising new tools and technologies to help detect, prevent, and recover from these risks. However, these are just tools and are ineffective unless they are used by experienced professionals. There is no technology that will ever be able to take out of the box, plug in, and have it defend an enterprise without skilled professionals operating it. We face a critical shortage of the required cyber security skills across the State and across the nation.

NY took a bold step when it announced the tuition free college program, known as The Excelsior Scholarship, earlier this year. NY can further its leadership in education by considering additional programs to train the future cyber security workforce. Many critical cyber security positions do not require a college degree. The state should help create alternative entry paths to cyber security careers through special programs at trade schools, relevant associate and certificate programs through the community college system, and tailored training for military veterans and other sources of talent. We must enhance our communications and outreach efforts to school students, their families, and underrepresented communities that might not be aware that cyber security is a viable, meaningful, and rewarding career path. The cyber security field has virtually 0% unemployment, millions of unfilled jobs, and a significantly higher than

average compensation structure that can provide for families for their lifetimes. Investments by the State to grow the cyber security workforce should have the highest return of any economic development program in the State. Additionally, creating the cyber workforce of the future, or a NY cyber Center of Excellence, will attract even more businesses to the state to leverage these new resources.

Thank you for the opportunity to speak to the Subcommittees and I look forward to answering any questions you have.