Testimony of Karen A. Harper

Principal Scientist, President and Chair of the Board

Charles River Analytics Inc.

On behalf of the National Small Business Association

Senate Committee on Small Business and Entrepreneurship

"Cyber Crime: An Existential Threat to Small Business"

March 13, 2019

1156 15th Street, N.W., Suite 502
Washington, DC 20005
202-293-8830
www.nsba.biz

Karen A. Harper, Principal Scientist, President and Chair of the Board, Charles River Analytics Inc., Cambridge, Massachusetts

Good afternoon. Thank you, Chairman Rubio, Ranking Member Cardin and members of the Senate Committee on Small Business and Entrepreneurship, for inviting me to testify today on the current state of cyber vulnerabilities facing America's small businesses, and the negative impact current policies—intended to help mitigate cyber risks—are having on small businesses.

My name is Karen Harper, and I serve as President and Chair of the Board of Charles River Analytics, a small research and development company, employing 180 people, headquartered in Cambridge, Massachusetts, with a satellite presence in Wakefield, Rhode Island, and remote presence across the country, including Arizona, California, Florida, New York, North Carolina, Pennsylvania, and Texas.

Since 1983, Charles River Analytics has been delivering intelligent systems that transform our customers' data into mission-relevant tools and solutions to support critical assessment and decision-making across a wide spectrum of mission areas and functional domains. Charles River continues to grow our technology, customer base and strategic alliances through research and development programs for the Departments of Defense (DOD), Homeland Security (DHS), NASA, and the Intelligence Community.

For a small business, we bring an impressive array of deep technical expertise to these domains and customers, including artificial intelligence, sensor and image processing, situation assessment and decision aiding, human systems integration, human-robot interaction, and, notably for today's hearing, cyber security. Since 2013, Charles River is proud to operate as a 100 percent employee-owned company, which has set the stage for our next generation of scientific exploration, technological innovation, customer service, and growth.

I am pleased to also be here representing the National Small Business Association (NSBA), where I currently serve on the Leadership Council and the Small Business Technology Council. NSBA is the nation's oldest small-business advocacy organization, with over 65,000 members representing every sector and industry of the U.S. economy. NSBA is a staunchly nonpartisan organization devoted to representing the interests of America's small businesses which provide almost half of private sector jobs to the economy.

Small Business – Cyber-security Landscape

Small businesses face unique challenges and vulnerabilities when it comes to digital security. Business owners rely on information technology more than ever, yet the very tools that make small businesses competitive have also put them in the crosshairs of cyber attackers. The security of our online data and finances is a huge concern for America's small businesses. Early indicators from a forthcoming National Small Business Association (NSBA) survey show that 62 percent of small-business owners are very concerned that their business could be vulnerable to a cyber-attack—both in terms of being targeted by a cyber-attack as well as the potential for unnecessary regulatory burdens that could accompany efforts to stem online attacks. The level of risk for being a target of cyber-crime is high, that same data suggests that one-in-three have been the victim of a cyber-attack.

The most common type of cyber-attack, according to NSBA's data, caused a service interruption or information falsely sent out under the businesses name. Other common kind of cyber-attacks for small business are general computer hacks, stolen credit card information and website hacks. However, threats can also include attacks launched through email, SMS and voice phishing, even insider threat attacks, or in person cyber-security attacks. Small businesses are also very likely to suffer a reputational attack, where someone starts posting negative information in social media, websites, and blog posts to harm their brand and or reputation. Of the number of NSBA members who were victims of credit card theft, 13 percent said their company's entire network was compromised and for 10 percent their banking accounts were breached. Small businesses often operate on very tight profit margins and seldom carry a lot of excess cash. These losses can be devastating to businesses in those circumstances.

Small Business Operational Perspective

The forthcoming NSBA survey shows that in a technologically advanced economy, network vulnerabilities and the lack of a comprehensive cyber-security policy can completely disrupt business. The results indicate that resolving these issues is significant as well, with one-in-four saying it took them more than three days to find a resolution.

This is an incredible burden on an organization of any size, but when factoring in the fact that small businesses have limited financial and technological resources, the problem becomes compounded. Only 14 percent of small business rate their ability to mitigate cyber risk and vulnerabilities as effective.

For those owners handling it themselves, it is certainly expected that resolving incidents will require research, training, trial and error, and a great deal of time away from the core functions of the business—acting as accountant, benefits coordinator, attorney, and personnel administrator. Simply outsourcing the function is not necessarily a silver bullet either.

As a result, small businesses must become more efficient in their utilization of cyber-security methods that are designed to help mitigate the potential risks of cyberattacks. The statistics show that there is a significant amount of work to be done on part of small companies and their operational strategies.

For these reasons, NSBA is pleased that Chairman Rubio will be introducing the Small Business Cyber Training Act of 2019, which would require Small Business Development Centers

(SBDCs) that have received grants from the Small Business Administration (SBA) to develop a counseling program and authorizes the SBA to fund that training. If passed, it will increase access to cyber-security expertise for small businesses and improve the safety of their data collection and storage methods. These additional resources from the SBA through the SBDCs—which many business owners utilize in their communities—may further improve cyber-security practices across all industries.

One of the most popular responses on why small businesses do not allocate financial resources to threat mitigation is that they feel they do not store any valuable data. This is a misconception on what constitutes valuable data – email, phone numbers, billing addresses may be viewed as not valuable information to the small business, but to a cyber-criminal, these are very valuable and effective data points that can be used for malicious purposes. Although small-business owners are becoming increasingly tech savvy, limited resources and knowledge still leave many vulnerable to cyber-threats.

NSBA has long urged Congress to move forward on establishing streamlined guidelines and protocols to ensure the protection and security of our online data and financials, but cautions against a knee-jerk reaction that would unfairly place a disproportionate burden on America's smallest firms. Legislation to enhance America's cyber-security should provide clear, simple steps for companies to follow when their data is breached and must balance the need for greater information sharing with privacy rights.

Charles River Analytics

Charles River has been on the cutting edge of Research & Development (R&D) related to cyber defense for many years, working with science and technology groups within the DOD, DHS, and the Intelligence Community, to develop better ways to identify and defend against cyber-attacks.

For example, working for DARPA (the Defense Advanced Research Projects Agency), we have created tools to process millions of pieces of malware and have seen firsthand how much malware is out there, how sophisticated it often is, and how it changes over time to avoid detection. We have worked with the Air Force Research Laboratory (AFRL) to develop tools that use advanced machine learning techniques to predict changes in malware, so we are better able to detect novel malware, but are not yet able to predict all of the ways that sophisticated attackers change their attacks. Finally, we are currently finishing up a project with IARPA (the Intelligence Advanced Research Projects Agency) where we are attempting to predict specific types of cyber-attacks. As part of this effort, we have seen just how many attacks there are, both random and targeted, against small and medium-sized businesses, and how little information there is to tip cyber defenders off to pending attacks before the damage is done.

Through this research experience, Charles River has gained a deep understanding of the vulnerabilities of our nation's public and private institutions, corporate entities (including small businesses across all industries), and private citizens. We also understand the value of the data at risk to a cyber attack. Whether it is personally identifiable information (PII) of the private citizen, the proprietary and confidential data of companies and institutions, or the data that supports and protects our national security, the potential of compromise to this data can be devastating to the individual, organization, and the nation as a whole. Therefore, it is imperative to provide the nation's small businesses with straight-forward, pragmatic policy guidance and effective support to dramatically improve our own cyber defense systems.

National Institute of Standards and Technology (NIST)

Recent efforts to promote and standardize cyber defense strategies have been implemented in the defense industry, through the adoption of the National Institute of Standards and Technology (NIST) Special Publication 800-171 requirements to protect Controlled Unclassified Information (CUI) in non-federal IT systems. All DOD contractors that process, store or transmit CUI must meet the Defense Federal Acquisition Regulation Supplement (DFARS) minimum security standards or risk losing our DOD contracts.

The NIST standard is broken down into fourteen areas. In each of these areas, DOD contractors must adhere to specific security requirements. The rule requires contractors to notify the DOD CIO within 30 days of contract award of any security requirements not implemented at the time of contract award. Often, when the government comes up with new compliance regulations, it becomes a headache for businesses, especially small ones, to oblige in a timely manner.

While small-business leaders such as myself, understand the intentions of the NIST SP 800-171 standard to protect the cyber vulnerabilities we all face, compliance with NIST SP 800-171 is extremely costly and overly burdensome, particularly for small businesses. The publication includes 110 (!) IT control requirements, many of which require highly complex solutions. As a result, many contractors are still grappling with the complexities of NIST SP 800-171, as well as other aspects of DFARS, such as what actually constitutes "Controlled Unclassified Information (CUI)" under the clause.

For Charles River, the development of this standard certainly represents a critical step forward in combatting the cyber threat. However, it has also missed the mark in several critical ways. The NIST standard targets the protection of CUI. But, what is CUI? It obviously includes U.S. federal government information that is considered sensitive, but not classified. But, one of the "selling points" of NIST compliance is that it also targets the protection of the proprietary and confidential data of our company, the PII of our staff and our customers. But, until we can confidently identify and label CUI, we are challenged in its protection.

The Deputy CIO of the DOD, at one industry meeting attended by our IT team in 2017, responded to a question about the department's challenge in properly defining and marking CUI sent to our facility, by saying "we are working on that, but we don't have a plan in place right now." To this day, CUI sent to our facility by DOD customers is often improperly identified and marked—and we know it. This has been a critical concern in our decision-making around NIST compliance implementation. Because CUI data is not always clearly identified, we chose not to put our staff in the untenable position of making those calls on the fly in their daily work. So, we declared that all data on our corporate networks is to be treated as CUI for compliance purposes. Therefore, all network devices had to be equally compliant with the standard. This may sound simple … it has been far from it.

Given the lack of clarity in how we were to approach the NIST standard, I am very proud that our IT and Software Engineering teams, recognizing the importance of the goal of better protecting our company's and the government's data, took on the challenge with gusto.

However, they encountered multiple non-fiscal issues with ensuring compliance. First, NIST implementation requirements are vague. All of the 110 NIST controls can be approached and implemented in a variety of ways, and there is a dearth of *specific* guidance, information, or documentation on preferred implementation methods. As a result, we spent approximately 800 person-hours between April and July of 2017 on research and discussions with external consultants to interpret the control requirements. Second, the NIST document was written in a manner and voice unfamiliar to us, even though we have been working with the DOD and other federal agencies for more than 35 years. Finally, we found that many of our customers, from contracting officers to technical sponsors to senior staff at the Pentagon, seemed equally confused and unable to provide helpful clarification and guidance.

Fortunately, being a software engineering company, our team is very technically savvy and highly experienced. After deciphering all of the NIST controls, we were able to develop a Risk Gap Analysis and formulate a plan of action. We then spent an additional 1,500 person-hours between August and December of 2017 to implement that plan. It was a significant challenge to meet all of the requirements with the limited amount of information and guidance provided. Furthermore, while we are confident that Charles River Analytics is fully NIST-compliant, we are still not sure how or when that compliance will be confirmed through audit.

The costs of NIST compliance were quite burdensome as well. Charles River Analytics ended up spending more than $300K in hardware, software, vendor maintenance contracts, and license tier upgrades. While allowable and allocable to our government contracts, these costs were entirely unbudgeted, and adversely affected the cost mix on our projects for fiscal years 2017 and 2018.

The unexpected costs did not end with these one-time-only purchases—Charles River Analytics now estimates that we will spend an additional 30 percent every year on non-labor IT overhead, for as long as the company continues to sign contracts containing the updated DFARS clause requiring NIST compliance. Now, I recognize that as a software engineering company operating across a number of sites, our IT infrastructure may be significantly more complex than the average U.S. small business, and so, our costs may be on the higher end of the spectrum.

However, we cannot kid ourselves that true NIST compliance can currently be achieved at a minimal cost to businesses.

The labor costs associated with ensuring NIST compliance were diverse and varied, and high across the board. Apart from the cost to interpret, discuss, plan, and implement compliance solutions, NIST compliance has required additional and ongoing costs that have affected previously planned initiatives, backlogged other infrastructure upgrades, and future quality-of-life improvements (which indirectly affect staff retention issues). Planned and ongoing infrastructural maintenance/improvements were either delayed, resulting in an increased overall cost of roughly 20 percent across the board, or were "solved" by spending money on external consultants, at an approximate markup of 200 percent over qualified in-house labor. By mid-2018, the IT Department staff (and therefore, our overhead IT costs) was increased from five to eight full-time staff, specifically to support our ongoing infrastructure work and maintain NIST compliance.

Finally, NIST compliance, as currently defined, places a significant burden on our technical staff and on our frequent partners. Creating and maintaining compliant infrastructure drains resources from project work, resulting in less progress per dollar, and makes it more difficult to put contracts in place with other research organizations, including universities and other small businesses. NIST assumes that the software configuration of a workstation will remain relatively static and contain well-known software, which is simply not the case for an R&D-driven software engineering company, such as Charles River. The resulting controls add significant resource and time barriers to the execution of R&D, as a key ingredient in such work is exploring and analyzing multiple solutions, each of which must be made compliant. This effectively raises the overhead of compliance in areas that we cannot afford—that is, finding solutions for the coming years and decades.

Small businesses must also analyze commonly used tools (e.g., inter-organizational collaboration tools) for NIST compliance, further impairing collaboration and productivity. Perhaps most importantly, NIST compliance hinders and frustrates top-performing personnel, causing them to seek employment in other sectors, making it difficult to maintain competitive business advantage and competitive national advantage. Ultimately, NIST significantly impairs a small business's ability to do defense-driven R&D, and to be forward-looking, effectively handing advantages to our nation's adversaries.

Charles River Recommendations

Given the challenge, expense, and business impacts of Charles River's NIST compliance program, I recommend improvements to the government's specification and support for its implementation by small defense contracting businesses across three areas.

First, we require *clarity* in the definition and management of Confidential Unclassified Information (CUI), both provided by our DOD customer base, but also information generated by our company in the course of business execution. Second, we require *flexibility* in the application of the defined NIST controls. IT requirements across industries and companies varies widely, and the implementation of NIST-compliant controls should reflect this diversity in IT system needs. Finally, we require *clear guidance* to support the nation's small businesses in the defense sector to comply properly. This guidance must be delivered in easily accessible implementation guides—using plain language—that target the range of IT challenges faced across the community.

If programs like the NIST SP 800-171 are to be leveraged outside the government contracting sector, it will also be imperative to incentivize large IT commercial vendors, such as Microsoft, Amazon, and Cisco, to develop NIST-compliant variants of market-leading IT products. Then, and only then, can this valiant effort begun by the NIST SP 800-171 standard be extended to the U.S. small business community, in its entirety.

Conclusion

Federal government agencies rely upon external contractors to carry out a wide range of functions. Many contractors have access to sensitive data that could, if compromised, potentially reveal classified information, threaten national security or even put lives at risk. As a result, cybersecurity is a critical and growing concern for both federal agencies and those who do business with them.

However, the implementation requirements for NIST SP 800-171 is just one example of the barriers small businesses face when engaging in the federal acquisition process. As demonstrated throughout my testimony, not only is the cost of compliance significant, the required overhead is quite extensive, costly and onerous on both prime contractors and subcontractors who need to be compliant.

Understandably, many small businesses feel overwhelmed. If you don't comply, your contracts – and, perhaps, your business – are at risk. Yet, many do not know where to begin or even after all their efforts, know if they are truly compliant. Unlike Charles River, many small businesses do not employ a dedicated IT employee or consultant. Often, an owner or key employee performs IT functions in addition to their regular duties. And even Fortune 500 companies with vast resources struggle with information security. No wonder small-business owners feel overwhelmed when dealing with cyber protections!

Still, when you submit a Request for Proposal (RFP) or sign a contract containing one or more information security clauses, you are affirming your ability to comply with the contract. You need to employ as many best practices as possible to show that you have employed good faith due diligence to achieve compliance. As with any compliance program, you must be able to demonstrate that you are doing – or trying to do – the right thing. Nonetheless, the NIST SP 800-171 requirement makes this extremely hard to do. Therefore, it is critically important for Congress to always bear in mind the unique challenges that small businesses face when it comes to cybersecurity and continue to include the small-business community in the process of preventing unnecessary burdens that could accompany efforts to stem cyber-attacks.

Thank you for allowing me to testify before the committee today. I would be happy to answer any questions you might have for me.