WRITTEN STATEMENT OF

LARRY CLINTON, PRESIDENT AND CEO,

INTERNET SECURITY ALLIANCE

on

The Promises and Perils of Emerging Technologies for Cybersecurity

before the

U.S. SENATE COMMITTEE ON COMMERCE, SCIENCE AND TRANSPORTATION

March 22, 2017

CYBERSECURITY IS NOT AN "IT" ISSUE. TO ADDRESS IT EFFECTIVELY WE NEED TO LOOK AT CYBERSECURITY AS AN ECONOMICS ISSUE

Expecting technology to provide the answer to our cybersecurity problems would be a perilous course. A more promising path would be to understand the true nature of the cyber threat and take a more enterprise wide approach to addressing it.

Two months ago, the National Association of Corporate Directors (NACD) released the second edition of its Cyber-Risk Handbook, the only private sector cybersecurity document ever endorsed by both the departments of Homeland Security and Justice.

The very first principle of the NACD Cyber Risk Handbook is that cybersecurity is not an information technology issue. While it has a substantial technological component, cybersecurity is an enterprise-wide risk-management issue.

Information technology is only the pathway for cyberattacks – the "how" of cyberattacks.

If we are to address the cybersecurity issue in a long term, sustainable fashion we need to not only address the "how" of cybersecurity, but also the "why" of cybersecurity: the reasons that attacks occur.

From the private sector perspective, (and the core of the Commerce Committee's jurisdiction) the reason cyberattacks continue to occur is the unbalanced nature of digital economics.

The basic equation of cybersecurity economics is this. Cyberattack methods are easy and cheap to access, they can generate enormous profits – in the hundreds of billions of dollars – and the business plan for the attackers is secure and sustainable as attackers reinvest in their enterprise to become ever more sophisticated and effective.

On the security side, cyber defense must protect an inherently insecure system that is growing technologically weaker with the explosion of mobile devices and the Internet of Things. We are almost inherently a generation behind the attackers, our laws and regulations are not well suited to address international and often state-sponsored digital threats. Moreover, the government mandates being piled on the private sector are often counterproductive. Finally, there is virtually no effective law enforcement. We successfully prosecute less than 2 percent of cyber criminals.

So long as we continue to try to address the cybersecurity issue from a techno-centric perspective and ignore the fundamental economics that are driving the problem, we are destined to continue to fail badly.

To effectively address this issue, we must frame it differently. The problem is not that the technology is bad. Modern technology is nothing short of amazing.

The problem is that the technology is under attack. And the reason the technology is under attack is because all the economic incentives favor the attackers.

That is a fundamentally different problem that demands fundamentally different set of solutions.

Within the private-sector, we have begun to address the issue in a broader risk management perspective that includes technology but places it in the context of the overall enterprise operation, not at the center of it. We are already seeing positive results.

For example, PricewaterhouseCoopers, in their 2016 Global Information Security Survey reported that "Guidelines from the National Association for Corporate Directors (NACD) advise that Boards should view cyber-risks from an enterprise-wide standpoint and understand the potential legal impacts. … Boards appear to be listening to this guidance. This year we saw a double-digit uptick in Board participation in most aspects of information security. Respondents said this deepening Board involvement has helped improve cybersecurity practices in numerous ways. It may be no coincidence that, as more Boards participate in cybersecurity budget discussions, we saw a 24% boost in security spending."

The Internet Security Alliance believes the Senate Commerce Committee, indeed the full Senate and Congress can help facilitate further progress by addressing the cybersecurity issue in a less techno - centric, and more enterprise risk management/economic fashion. ISA would offer three paths for the Commerce Committee to pursue.

STEPS TOWARD CREATING BETTER ECONOMICS FOR CYBERSECURITY

ISA would like to suggest three measures for improving cybersecurity that come within the jurisdiction of the Senate Commerce Committee.

1. Create a Rational Cyber Regulatory System
2. Promote incentives
3. Test the NIST Cybersecurity Framework for cost effectiveness.

Create a Rational Cyber Regulatory System

No one, certainly not ISA, is saying we ought not to have cyber controls or assessments. But we need to have a rational and well-thought out system or we will waste vital resources and undermine our security.

Earlier this week ISA released a "Cyber Regulation Fact Sheet." The fact sheet (attached) demonstrates multiple examples of how the tremendous growth in cybersecurity rules and regulations is diverting scarce security resources and undermines our nation's cyber defenses.

One of the unintended consequences for organizations like ISA that has been raising awareness of the cyber threat for 15 years, is that we now have cyber mandates spring up like weeds as virtually every governmental entity, federal state and local fight to be the "cyber guy." The result is an uncoordinated, inconsistent and often counterproductive setoff requirements that is actually hurting, not helping, to increase security.

Research tells us we are experiencing more than a million cyber-attacks a year and we don't have nearly enough cyber professionals to help protect us. We need to use our scarce resources efficiently and effectively. Yet some firms are now spending 30 percent of their budgets and 40 percent of their time of various compliance regimes none of which have been shown to empirically aid in securing our cyber systems.

ISA's fact sheet offered numerous examples from multiple industry sectors of the growth on cyber regulations often inconsistent with the risk management philosophy that professionals overwhelmingly suggest is a more effective approach to cyber defense. Among the statistics cited are:

- In financial services increases of over 300 percent in cybersecurity and privacy related questions financial institutions now need to answer.
- In defense there are new rules for unclassified controlled information that force companies to label bits of information based on 23 categories, 84 sub-categories and hundreds of different citations. Ironically these rules could actually make it easier for attackers to find useful data.
- In Energy DOE has proposed requirements (10 CFR 73.53) that all networks in the sector meet controls (DG 5062) so overly broad that the mandate will require the expenditure of millions of dollars to implement controls not tailored for the risk of the networks.
- New defense acquisition rules will require small companies to comply with extraordinary detailed requirements that may well drive many smaller firms out of the defense business which is both inconsistent with DoD policy to promote the use of smaller companies but also harms national security as many of these firms are the top suppliers who can find markets for their services that don't require the extensive compliance
- Various regulators are demanding public disclosure of supposedly material cyber-attacks when in fact the attack itself may not have a material effect, but the disclosure may well trigger unjustified (and usually temporary) stock fulgurations. As a result, it is the disclosure creating the material effect and provides a path for stock manipulation contrary to the regulator's mission.

Our fact sheet is by no means an exhaustive list it sim early illustrative of the uncoordinated government response to the cybersecurity problem that need to be brought under control.

Part of this problem is that the government itself is not properly structured for the digital age and hence digital age issues like cybersecurity run into legislative and executive jurisdictional barriers. However, the Commerce Committee with its overarching mandate to promote US commerce may well be positioned to provide some of the needed coordination.

Promote incentives

We believe that the most effective way for the private sector to improve the level of its cybersecurity is for the Congress and the federal government to consider what sets of incentives for better risk management can be brought to bear.

Government incentives allocated to the private sector in exchange for behaviors that, without incentives, would be not economically sustainable are not unprecedented. They are responsible for the telecommunications and electric infrastructure that undergird much of American prosperity. We call this the "social contract" approach to infrastructure and the Internet Security Alliance has long argued that a similar approach is needed for cybersecurity.

In the early twentieth century, the hot technologies of the time were telecommunications (phones) and distributed electricity. Initially these services were provided where the economies justified them: urban and affluent areas. The policy makers of the era not only understood that universal service of these technologies would have broad social benefit but also realized government couldn't accomplish this on

its own. Moreover, compelling the private sector to provide the services without adequate compensation would be an unsustainable model. So a "social contract" – essentially an economic deal – was developed. Private companies agreed to provide universal service at regulated rates. In exchange, the government agreed to guarantee a substantial rate of return on their investments.

And it worked. The broader systemic benefits of the social contract were enormous. The electric and telecommunications infrastructures were deployed at an accelerated pace compared with other nations that chose a government-centric model. Moreover, the infrastructures, adequately supported by the economic incentives imbedded in the contract, were continually made more sophisticated and innovative. The rapid development of these infrastructures provided the foundation for accelerated industrialization, job creation, and innovation. These systemic effects were essential to turning the United States from a second-rate world presence at the turn of the twentieth century into the world's leading superpower in a little more than a generation.

More recently, the House GOP Task Force on Cybersecurity made their number one recommendation to develop a menu of incentives for the private sector to begin to address the economic incentive imbalance discussed above. To be fair there has been some progress since the House GOP report. In 2013 President Obama in his Executive Order 13636 also embraced the notion of using market incentives as opposed to regulatory mandates to promote cybersecurity and in the last Congress bipartisan legislation on cyber information sharing used the market incentive of liability protection.

As we move forward we need to enhance and accelerate the development of market incentives. While obvious techniques such as tax breaks for smaller companies to adopt sophisticated defenses not otherwise commercially justifiable can be used, there are many other models of incentives that can be adapted. For example, just as pharmaceutical companies with good records can gain access to an accelerated drug approval process perhaps good actors in technology could get patent approval preference, or utilities could gain access to a fast rerack permitting system. Regulatory forbearance could be offered for organizations meeting specified levels of maturity in traditionally regulated industries and streamlined audit and assessment process can also be developed.

The reality is that many cyber-attacks are nation-state backed and no private organization can match the resources of a nation state. It may well be that private companies will have to take on traditionally governmental responsibilities in the digital age and government needs to find a sustainable and cost efficient mechanism to deal with this new reality.

No less a source than the National Infrastructure Protection Plan (NIPP) has observed that the private sector and the public sector assess cyber risk on very different dimensions. For the private sector – operating under a mandate to maximize shareholder value – the cybersecurity calculus is largely economic. This reality generates a higher level of security risk tolerance in the private sector than the public sector. For example, a private entity maybe comfortable with allowing 10 percent of inventory to "walk out the back door" every month because it will cost 11 percent to purchase the additional guards and cameras to fully secure themselves. The public sector doesn't have this luxury. Government has enormous non-economic concerns it must accommodate such national security and citizen privacy.

Today, we need a twenty-first-century systems approach to address the cybersecurity issue. The new model needs a much more dynamic motivator than backward-looking regulations and potential enforcement. Since 90 percent of infrastructure is owned and operated by the private sector and the

principal problem with cybersecurity is economic, the best model to promote a forward-thinking risk-management approach to cybersecurity would be injecting positive economic incentives into continual upgrading and management of private cyber systems.

Test the NIST Cybersecurity Framework for cost effectiveness.

The NIST Cybersecurity Framework rightly enjoys the praise of wide swaths of government and the private sector. We join in that praise, although we note that the Framework is not a standard but a broad framework that can, and ought to be, implemented in many ways depending on unique aspects of the system its being applied to and the threats that system is facing. As such, the specific way the Framework is used is not necessarily the most cost effective approach. This is why the executive order that called for the Framework's creation, E.O. 13636, also stipulates that the Framework ought to be *cost effective*—a direct call to address the economic imbalance causing the cybersecurity crisis.

Unfortunately, three years after NIST released the Framework, there have been no efforts to evaluate it for cost effectiveness.

This is even despite Section 104 (b) of the recently signed American Innovation and Competitiveness Act, which in states that NIST shall "conduct research and analysis (A) to determine the nature and extent of information security vulnerabilities and techniques for providing **cost effective information security**" (emphasis added).

The lack of data in this area is a huge drag on cybersecurity since the commercial sector cannot afford economically unsustainable cybersecurity measures. It's likely led to an underinvestment in cybersecurity in many sectors, since it's impossible for companies to trace the quantitative reduction in risk exposure caused by cybersecurity measures.

Most importantly, lack of cost data makes it impossible for the government to understand which specific areas of cybersecurity it should spend its considerable powers on encouraging within the private sector. In the absence of data, cybersecurity advice tends toward the general, along the lines of "implement best practices." But abstract exhortation is not working. We now need to know *which* best practices, and *why* they're not being adopted. The ISA suspects cost is a major factor.

After determining cost effectiveness, the government should move to create incentives to encourage adoption. Steps that improve the bottom line by diminishing quantifiable risk will find natural take up by the private sector. But measures that are effective but too expensive to justify economically—but necessary for securing the economic and national security of the United States—are precisely where targeted incentives should be deployed.

We urge the Committee ought to use its tools and processes to test the cost effectiveness of NIST Framework implementation.