Senate Committee on Commerce Science and Transportation
Building a More Secure Cyber Future: Examining Private Sector Experience with the NIST Framework
February 4, 2015
Testimony of James A. Lewis
Center for Strategic and International Studies

I thank the Committee for the opportunity to testify on private sector experience with the National Institute of Standard's (NIST) Cybersecurity framework. The Framework provides a list of measures companies can take it improve their cybersecurity. I will discuss three issues: what we know about the Framework's adoption, how effective it is, and where it can be improved.

An initial conclusion is we lack sufficient data to say definitively whether the Framework is working or not to build a more secure cyber future. The Framework itself was released relatively recently, in February 2014. It will take more time for the Framework to be implemented, adjusted and to see if it what effect it has on cybersecurity. My comments on the Framework are best seen as preliminary until we have gained further experience and data on its implementation. On the larger issue of building a more secure cyber future, in which the NIST Framework may play a part, there is sufficient data and experience to describe the situation and to make general recommendations for improvement,

Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity," released in February 2013 was a major shift in U.S. policy on cybersecurity. Instead of making a single agency responsible for cybersecurity, it assigned responsibility to existing, sector-specific regulatory agencies. The EO instructed the National Institutes of Standards and Technology to develop a "Cybersecurity Framework" released in February 2014, that companies could use to guide their defensive efforts and that agencies could use to measure if the critical infrastructure companies they regulated were doing an adequate job. The process is voluntary. In addition, approximately 200 critical infrastructure companies were notified by the White House that they would be held to a higher level of scrutiny given their strategic importance. This Executive Order is likely to be followed by another executive action in early 2015 on information sharing. The executive actions and the NIST Framework are building blocks for better cybersecurity, but while they are good first steps, the U.S. remains vulnerable.

We should, if the Framework is effective in improving cybersecurity, see changes in the attacker population, with the less skilled attackers dropping out and the more skilled (or better resourced) changing attack techniques. Even if the Framework is effective now, if it is not dynamic and evolve along with the threats we face, it might not produce a lasting decrease in the rate of data exfiltration, as skilled opponents adjusts to improved defenses. This outcome is possible if the attacker seeking to exfiltrate data is an intelligence agency or foreign military who have the resources and dedication to wage a persistent campaign.

For example, and judging from public sources, it appears that Sony had not implemented most of

the NIST Framework recommendations, but it is not clear that even if it had, North Korea would have been prevented from gaining access and doing damage. The defenses needed for determined State opponents like Iran and North Korea lie outside the NIST Framework.

One way to think about critical infrastructure is from the perspective of an enemy "targeteer," planning what American targets to strike with cyber attacks in order to achieve the desired military effect. For these opponents, America is a target rich environment, with thousand of potential targets, many of which are poorly defended. If the opponent wishes to make a political statement, it will look for a single poorly defended target with symbolic or political value. If the desired effect is temporary military advantage, it might strike a few dozen civilian targets - logistics systems and perhaps critical infrastructure in the areas that would support deployed U.S. forces, in Hawaii and the West Coast, for example, if the conflict was with forces under PACCOM. If the desired effect was extensive damage to the U.S. economy and military capabilities, a broad campaign with many hundreds of civilian targets would need to be attacked. Fortunately, this attack scenario is very unlikely and only one or two countries have this capability.

The EO 13636 process attempted to identify some of these critical civilian targets, but in general we have no idea whether the Framework complicates opponent planning for cyber attack. The dilemma for cyber security is that, unlike other possible attacks against the U.S., we have not found an effective defensive strategy. Our military forces deter truly damaging attacks – no country willingly seeks war with the U.S. – but they did not deter North Korea from damaging Sony or Iran from attempting to damage banks. We need a blend of adequate defenses at the company level and robust Federal efforts to dissuade opponents if we are to build a secure cyber future and while the right formula has not been found, the NIST strategy could form a useful part of an effective national approach to cybersecurity.

A compliance approach to security lists actions taken; a better approach is to ask to see the results of those actions. Good data on results is unavailable, and much of the discussion of cybersecurity is strangely disconnected from fact. The primary categories for measurement are the number of companies adopting of the Framework and its effectiveness in thwarting opponents.

But adoption is not an adequate measurement for success. Even if all companies were to voluntarily implement the NIST Framework, it does not necessarily mean that there will be an improvement in cybersecurity. The measures listed by NIST are likely to improve security if implemented correctly, but to what degree there will be improvement is unknown, nor do we have any idea of how many companies have implemented the Framework recommendations, or how well they have done so. For example, if there was widespread adoption of the framework but little effect on penetration and exfiltration, it would be premature to say that the tide has turned in cyberspace. The difficulty in linking recommendation and effect strongly affects how we manage risk, and the lack of data hampers a range of initiatives, from creating a cyber insurance market to applying the NIST Framework.

The only way to accurately measure effectiveness is to ask if the number of successful penetrations and the outflow of data have decreased. If hackers still get in and data still flows

out, the Framework is not working. These are result-based measures, fundamental for determining the return on investment in cybersecurity. Many things can be asserted or even measured, but they are useful only to the extent they can be correlated with effects.

Judging from the news, the number of successful computer breaches against U.S. companies and agencies has not decreased. We do not know if this is because companies have not adopted the framework, have been unable to implement it, or if it is because the Framework is ineffective. An initial estimate is that all three of these estimates are likely true, but to guide policy and legislation we need to understand whether which is the most likely cause for the absence of a visible improvement in U.S. cybersecurity.

The success rate of opponents, determined by their ability to penetrate target computer networks and to exfiltrate data from these networks, is the only true measure of the Framework's effectiveness. In 2013, press reports state that the FBI notified 3000 companies that they had been hacked – and there may have been more that we do not know about. If this number declines in 2015, it indicates that the Framework is successful.

NIST did put out a Request for Information on the private sector's experience so far with using the agency's cybersecurity framework and in October it received more than fifty responses form companies and associations. A majority of respondents were supportive of the Framework and acknowledged its increasing adoption in various sectors. Other comments included support for the Framework's easily understood guidance, worries that small and medium size enterprises were not capable of meeting the guidelines due to costs, and confusion about the voluntary nature of the Framework. A majority of respondents called for continued support for the Framework.

A Request for Information (RFI) is not the best approach to assessment, because companies that report "self-select," with only those with good stories to tell providing a response. There will be a desire to say that the Framework is working well, as this would remove the impetus for further cybersecurity measures. These are normal problems with survey data, but they could skew responses to produce an overly rosy picture. An alternative approach would be to use Commerce Department (of which NIST is a part) authorities under the Defense Production Act (DPA) to require companies to respond. Using the DPA would allow Commerce to devise an adequate sample of companies that would allow it to estimate adoption rates by sector and company size. Other agencies also can collect information for sector specific groups. There may be some resistance to conducting a survey. This resistance in itself would be a good indication of intent regarding the Framework.

There have been only few efforts, such as DHS's continuous monitoring effort and the Australian Signals Directorate work on its "Strategies to Mitigate Targeted Cyber Intrusions, to show that implementing a measure produces an observable reduction in successful attacks. These efforts allow us to say that some measures drastically reduce opponent success rate. Many of these measures are included in the Framework, along with a quantity of other.

Several issues complicate the implementation of the NIST Framework. Many small and medium sized companies lack the manpower, training and resources to fully implement the Framework.

Straightforward measures, such as the ASD mitigation strategies, are appropriate from small and medium companies but may not work as well in the complicated networks of large companies. Cost is an important issue for companies of all sizes – essentially cyber security requires a business to allocate resources to purposes that will not generate a return on investment. In cybersecurity, we are asking companies to spend money on activities that do not generate a return and we have not offered any mechanisms for them to recoup this cost. Of course, a good way for companies to think about spending on cyber security is that it is like insurance, where a company spends money to reduce and manage risk.

This means that at the level of the firm, cyber security involves business decisions where companies should decide how much risk they are willing to take, what mitigation efforts (like insurance) best manage risk, and then spend accordingly on protection. Anecdotal evidence suggests that many companies still underestimate cyber security risks, but this is changing and the recent series of events, in particular the Target breach (which led to the resignation of the Chief Executive Officer and a dramatic decline in revenue), have helped to focus attention and raise awareness in company management and boards.

The Framework provides a useful focal point for company discussions of cybersecurity, and a commonly held view is that it is a good first step. Over time, it is likely that as companies implement the Framework, they will modify it and identify measures that best fit their own purposes, as they experiment with different approaches and find what works best. Each critical infrastructure sector may find that some parts of the framework are more important for their business than others and modify implementation in ways that works best for them.

The effect of the Framework on reducing cybersecurity risk might be different for critical infrastructure than for intellectual property. Survey data on penetration and exfiltration success rates will show where individual defense are inadequate and where collective action is needed, through increased international engagement in diplomacy and law enforcement cooperation to reduce cyber risks. To continue the insurance analogy, we want to take governmental actions that reduce systemic risk so that companies can spend less on "insurance," e.g. cybersecurity.

One of the most valuable lessons of EO 13636 is that one size does not fit all. In retrospect, one of the most serious flaws of the 2012 draft Senate legislation was its efforts to assign a single agency the authorities to regulate cyberspace. The EO, by tasking regulatory agencies to ensure that their existing regulations adequately take the Framework into account, better reflects the diversity of the economy.

What is emerging is a structure for national cybersecurity shaped by the different incentives (or lack thereof) that companies faces in making business decisions about cybersecurity. These incentives are created by are regulatory authority, business risk, and civil liability.

- Critical infrastructure: improved cybersecurity will be the result of partnerships between companies and their sector regulators. This is the area where the Framework and the Executive Order have made the most valuable contributions, since it provides a basic template against which company actions can be measured.

- Personally identifiable information: Federal Trade Commission (FTC) actions and market penalties can incentivize companies to better protect personally identifiable information, but the level of cybersecurity at major companies holding PII is has been inadequate.

- Intellectual property: there is no regulatory mechanism to penalize companies for the loss of IP, nor should there be. When a company is hacked and loses IP, a part of the responsibility is shared by the Federal government, which needs to do more to discourage economic espionage by foreign actors, but the bulk of the responsibility is held by the company, which has made bad business decisions to under-prioritized cybersecurity. Increasingly, the market will penalize such companies, at least temporarily, and these companies face increased risk of civil liability. Shareholders and customers can now ask if a company had implemented the NIST Framework; if it had not, a case could reasonably be made that the management had failed to exercise due diligence.

From one perspective, cobbling together measures like the Framework, FTC rules, and some yet-undefined set of mechanisms for information sharing might seem like a ramshackle approach to one of the principle security problems of our time. There is some truth to this, but another perspective is that the complexity of the problem, the deeply ingrained problems with the technology, and the consequences of any cyber action for security and economics at both the global and national level, militates against any single solution that can be easily and rapidly adopted. Federal action can accelerate progress and provide structures for collective action, and from this perspective, the NIST Framework is a valuable step forward in what will be a long and uncertain process to make cyberspace more secure.

I again thank the Committee for the opportunity to Testify and would be happy to answer any questions.