Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Proposed Cyber-Security Law: What's the problem?

On or about March 31, 2009, Senators in the 111th Congress 1st Session initiated efforts to create a legal framework for "cybersecurity" for the United States. While this effort is laudable, there are several critical issues with this proposed legislation. This paper represents some of my initial thoughts. For each section of the proposed bill of interest to me, it includes "Basics" that describe the legislation, "Section by section analysis" that provides a third party analysis of the bill that I received via email, and my "Opinion" about issues with the section.

The advisory panel

Basics: The advisory panel is appointed by the President of the United States to advise the President on the issues. It includes representatives from industry, academia, non-profit organizations, interest groups, advocacy organizations, and State and local governments who are qualified to provide advice and information on cybersecurity research, development, demonstrations, education, technology transfer, commercial application, or societal and civil liberty concerns. It advises the President on matters relating to the national cybersecurity program and strategy and every two years provides a formal assessment of research and development, strategy realization, funding, management, coordination, implementation, and changes, societal and civil liberty concerns. The panel is uncompensated except for travel and per-diem.

Section by section analysis: This Advisory Panel provides industry, academia, and civil liberty groups an opportunity to review the federal cybersecurity effort and provide advice on its direction and progress. The Panel reports to the President every two years, providing recommendations on how the program can be improved.

Opinion: Assuming the President does a good job of selecting a panel, it is likely that such panel would be of great service. Of course the selection of panel members is always a problem. If the panel is truly representative of the best and the brightest, and if the panel members are not serving their own interests, but rather the nation's interests, this helps a lot. Unfortunately, the nature of political systems is that they are unlikely to get people who will say what they really think. After all, the unvarnished truth is something that is often hard to take, and to get along people tend to go along. But at least it's an effort in the right direction. If they can only avoid group think, it will be a net positive. The 2-year cycle for reporting is also a serious problem, given that typical computer systems are replaced on a 2-3 year cycle and threats change at a far more rapid pace. One of the major problems with government interacting with information technology is that the pace of change in the information technology arena is so much faster than the government actions. At the longest, a 1-year cycle should be used, and realistically, a quarterly update should be done. While strategy should not change at this pace, tactics may have to, and for critical systems, quarterly updates are certainly justifiable.

There is also a critical question relating to the development of strategy. In particular, there are no well understood and properly thought-out national strategies for information warfare, critical infrastructure protection under full spectrum attack involving informational aspects, economic warfare with informational attack, or any of the other potential modes in which information warfare, either on its own or in combination with other forms of warfare, can be properly managed for the United States. The previous strategy in this area is not adequate to handle the issues of today, and substantial effort should be expended to examine potential strategies.

The real-time dashboard

Basics: This calls for a system to provide dynamic, comprehensive, realtime cybersecurity status and vulnerability information of all Federal government information systems and networks managed by the Department of Commerce.

Section by section analysis: The lack of real-time visibility into the state of an information system or network is a key limitation of improving cybersecurity. This visual tool will aid major decision makers, such as the Secretary, in identifying which resources and determining how much to dedicate to address specific cybersecurity issues, as they arise. This will lead to a more efficient allocation of limited resources. The DOC may be seen as the pilot in a larger effort that the Federal government may attempt to roll out at a future date.

Opinion: While I am not opposed to the idea, it seems somehow out of place. The analysis asserts that there is some presentation of the state of some set of computers or networks that will help allocate resources. This has been tried time and again, and the basic problem today is that the information that comes from systems and networks is not particularly helpful in this sort of decision-making. Furthermore, real-time allocation of resources is a relatively minor challenge compared to the sorts of strategic decision-making that has to be done. Without a well thought out system of indications and warnings, responses may do more harm than good, and real-time decision-making should be based on a well-defined selection criteria with well thought out responses. In addition, a central collection and dissemination point comes with substantial risks, including, without limit, that it (1) provides definitive feedback on the effectiveness of attacks, (2) provides a potential single point of failure for the process, and (3) becomes a key and identified target for enemies. Given the the "insider threat" is considered important, the insider would be able to tell, for example, if they were being detected and tracked. Such decisions should be seriously thought through to avoid such unintended consequences.

Regional cybersecurity centers

Basics: This proposes to fund regional centers to help small and medium businesses improve their information security. It is a laudable goal, it explicitly supports non-profit affiliation, and it notionally supports national laboratories and similar institutions. It also identifies funding levels for these centers, and again this is all good. The term "best practices" is also used in this section.

Section by section analysis: This program is modeled off of the Hollings Manufacturing Extension Partnership (MEP). Large companies have the resources and expertise to address cybersecurity issues, but small- and medium-sized companies often do not. This program would help address that gap.

Opinion: One thing that this misses entirely is that, in the computer security industry, the best and the brightest are predominantly in small businesses, and only small businesses really understand small businesses.

The analysis makes very bad assumptions about large companies. Many large companies do not use their resources very well in the information protection arena and do not have the expertise that many may think they have. In addition, it seems unlikely that they would support this activity without compensation.

The bill also assumes that somehow large businesses and government will help small businesses by promulgating their standards and knowledge down to the small businesses. Rather, it should assume that small businesses and academic institutions will help government and other small businesses. Big businesses can barely take care of themselves - and often do so by paying small businesses to help them do it. That's worth saying again.

The biggest mistake that could possibly be made would be to have government and large businesses dictate what small businesses do. It should be the other way around. The top-flight small security businesses should be the source of innovation and good ideas and government and other small businesses should listen to them.

Finally, the term "best practices" is a misnomer as no such things actually exist, and the longer this misperception continues to be promulgated, the longer it will take to realize that protection is something we do and not something we buy. Encoding such misnomers in laws is particularly dangerous as it leads to dogmatic approaches that tend to fail. "Best practices" really means minimally acceptable practices, and perhaps the use of the term "sound practices" would be a better approach, as that might lead to the exploration of which practices are and are not sound for different purposes and in different situations.

Information protection is about dealing with changing tradeoffs and not about defining minimal steps to take. While regional centers is not a bad idea, their role should be better defined to meet the real needs of the vast majority of people and should shy away from big business approach.

NIST as the standards body

In one (1) year, NIST is supposed to establish measurable and auditable security standards for all Federal government, government contractors, or grantee critical infrastructure information systems and networks in the areas of:

- Security metrics research to measure risk reduction and defense cost and to develop automated tools to assess vulnerability and compliance.
- Security controls standards for continuously measuring the effectiveness of a prioritized set of security controls that are known to block or mitigate known attacks.
- Standards for measuring software security using a prioritized list of software weaknesses known to lead to exploited and exploitable vulnerabilities and a separate

set of such standards for measuring security in embedded software such as that found in industrial control systems.

- A standard computer-readable language for completely specifying the configuration of software on computer systems widely used in the Federal government, by government contractors and grantees, and in private sector owned critical infrastructure information systems and networks.
- Standard configurations consisting of security settings for operating system software and software utilities widely used in the Federal government, by government contractors and grantees, and in private sector owned critical infrastructure information systems and networks.
- A standard computer-readable language for specifying vulnerabilities in software to enable software vendors to communicate vulnerability data to software users in real time.
- A standard testing and accreditation protocol for software built by or for the Federal government, its contractors, and grantees, and private sector owned critical infrastructure information systems and networks that does not require or cause any changes to be made in the standard configurations described above.
- A process or procedure to verify that software development organizations comply with the protocols identified during the software development process and provides testing results showing evidence of adequate testing and defect reduction to the Federal government prior to deployment of software.
- Establish standards based on risk profiles.

Then, after this, NIST is supposed to:

- Enforce compliance with the standards developed by the Institute under this section by software manufacturers, distributors, and vendors, and
- Require each Federal agency, and each operator of an information system or network designated by the President as a critical infrastructure information system or network, periodically to demonstrate compliance with the standards.

Section by section analysis: No analysis is provided for this section.

Opinion: It has been a mistake for the last 40 years to put the NSA in charge of security standards, and that's a large part of why we are where we are today. Unfortunately, the mission given to NIST in this case is truly "mission impossible". To start with, NIST already has a wide array of standards related to information protection, many of which can and should be applied to the national need. But the development of standards takes time and should be well thought out. Standards typically involve public comment, and without proper care, can lead to major problems. As an example, the development of standards for information protection related to nuclear power plants provides for connectivity to the Internet and elsewhere. As a result, these power plants and their providers have created supervisory control and data acquisition (SCADA) systems that ultimately use the Internet and come to depend on that connectivity. Since these systems tend to be replaced over periods of not less than 5 years and often 15 years or longer, these standards have resulted in the introduction of interdependencies that will be present for a long time to come. But that's only the start of the challenges. Item by item:

- Security metrics research is simply not funded or advanced to the point where anything can be reasonably standardized to realistically measure risk or risk reduction. The faulty approaches to this sort of measurement have been part of the reason we are in the current situation, and continuing to push down this approach without the supporting years of research required to get at the real issues will result in further delays and missteps. Automated tools to measure compliance are fine for automated mechanisms, but information protection is largely about process, and process cannot be measured reliably by such tools today. Vulnerability measurement is even more problematic because the impact of vulnerabilities is highly situation-dependent. As a result, automated tools require enormous amounts of data that is not automatically available in order to produce meaningful results. Furthermore, there are liability issues associated with knowing about large numbers of irrelevant vulnerabilities that cause resources to be inappropriately prioritized.
- Standards for measuring effectiveness of controls are problematic because controls vary over such a wide range and they have different sorts of effects depending on the specific manners in which they are applied. Continuous measurement of controls is also meaningless for many controls. For example, a very important control is personnel background checks, and continuous monitoring is meaningless for these sorts of controls. The prioritization of controls is also problematic in that the specifics of the situation and the consequences of different sorts of failures forms a complex space that is highly specific to the particular situation. Finally, known attacks constantly change and what is know to one person is not known to another. For this reason, the approach is potentially problematic.
- Measuring software security is another area of security metrics that has only been very marginally explored. When the science is not done, it is generally a bad idea to start setting standards. The notion that a list of software weaknesses, as opposed to a list of types of weaknesses, can be prioritized without the specific context of their application, is problematic. The notion that they can lead to exploited and exploitable vulnerabilities is also problematic in that covering approaches allow such vulnerabilities to exist without impact, again depending on the specific situation. A far more sensible approach, that has proven effective in other areas, has been to develop fault models and measure coverage against those fault models. However, the science required to develop these fault models has not been undertaken to a substantial degree as of yet, and this requires years of research. The notion of creating specific standards for SCADA systems is a far better idea, and in particular, these standards should include the separation of these systems from other systems and the use of limited functionality when the surety demands such controls. However, laws are not likely to be the right place to specify the details of what standards should include.
- A standard computer-readable language for completely specifying the configuration of software on computer systems is problematic because the complete specification of configuration is likely to be hard to define in terms of a language that doesn't adapt continuously with time, and because the complete configuration is not necessarily the

desirable thing to track. Furthermore, government contractors and grantees, and private sector owned critical infrastructure information systems and networks include an enormous range of different sorts of systems. A single language is unlikely to be able to be very useful while also being that flexible. For example, information systems in use in control mechanisms in critical infrastructures are often custom hardware devices that are unlikely to lend themselves to the same sort of configuration languages as general purpose computers.

- Standard configurations that include "security settings" already exist to a large extent for widely used systems, and a standard computer-readable language for specifying vulnerabilities in software to enable software vendors to communicate vulnerability data to software users in real time also exists. There is no reason that NIST should not work in this area, but such standards are not required at this time.
- A standard testing and accreditation protocol for software is an excellent idea, but given the inadequacy of black box testing in general, the inability to examine the internals of software because of the legal prohibitions of the Digital Millennium Copyright Act, and the difficulty of detecting intentional subversion even when source code is available, such protocols are unlikely to be fully effective. Perhaps a better approach would be the combination of this methodology with the use of trusted computing platforms and Trusted Platform Alliance trusted computing modules to provide the means to provide limited ongoing assurance that vulnerabilities not otherwise detected can be limited in their extent and detected when they perform select types of subversion.
- Developing a way to verify that software development complies with process requirements is a great idea, but it is almost certain to either be meaningless or ignored in today's software development environment.
- Establishing standards based on risk profiles is also an excellent idea, but this then also demands that a set of risk profiles be defined, and this is also an area where such standards will either be of little real meaning or where a substantial research effort will be required to define meaningful risk levels. Perhaps a better approach is to start by recognizing that there are only a finite number of different protective mechanisms and that they have limited surety properties. Regardless of risk levels, surety is limited, and matching surety with risk is the key issue that needs to be addressed.

Generally, it is a bad idea for laws to be as specific about how to do things as the proposed bill is. Rather, there should be a governance process defined by the laws for identifying what standards are required over time, how they should be reviewed and changed with time.

Finally, given that NIST has no enforcement capabilities or role whatsoever today and that none of its current security standards are effectively enforced, it seems unlikely that enforcement of this sort will be effective in a realistic time frame unless very substantial changes are made. These changes are not identified in a realistic manner in the law as currently proposed.

Licensing and certification of cyber security professionals

Basics: This section would require the President, through the appropriate federal department or agency, to develop and integrate a national licensing and certification program for cybersecurity professionals. This section would also require all federal cybersecurity professionals to obtain this license. More specifically:

> "it shall be unlawful for any individual to engage in business in the United States, or to be employed in the United States, as a provider of cybersecurity services to any Federal agency or an information system or network designated by the President, or the President's designee, as a critical infrastructure information system or network, who is not licensed and certified under the program."

Section by section analysis: All major professions (doctors, lawyers, plumbers, electricians, etc.) are required to have a license to demonstrate they are qualified; cybersecurity professionals should not be exempt from this. There are a number of different cybersecurity certifications available currently, but there isn't a common standard among them.

Opinion: While I agree that licensing of security professionals is a rational idea in the same sense that engineers are licensed, the notion that in three (3) years this challenge will be met for every person providing any information security services related to these systems seems more than a bit ambitious.

But perhaps more importantly, in looking at the analogies to other professions (doctors, lawyers, plumbers, and electricians as examples), we see a wide variation in the needs and the licenses. The same should reasonably hold for cyber security. For example, in the medical field, there are board certified physicians in different specialties, but there are also nurses, who are licensed on a state-by-state basis with nursing boards, phlebotomists who are certified to draw blood, emergency medical technicians who are certified to carry out certain emergency procedures, and the list goes on and on.

In the information protection arena, we should have the same situation. In particular, there should be board certified specialists in particular areas, and there should be repair technicians who have different sorts of responsibilities. An enterprise security architect requires different knowledge and skills than a network intrusion detection specialist, and the list goes on and on. The creation of a set of licensing boards with different requirements should be developed and operated by the professional community, in a similar fashion to how similar boards are created and operated in other professions.

Secure the DNS system

Basics: In 3 years, the Secretary of Commerce is supposed to develop a plan to secure the domain name system and the Advisory Panel is supposed to review and approve (not disapprove) the renewal or modification of the Internet Assigned Number Authority contract to ensure that U.S. national security is not compromised.

Section by section analysis: This provision relates to the contract that the Department of Commerce has with the International Corporation for Assigned Names and Numbers (ICANN) to manage and administer the domain name system, which is at the heart of the Internet. This provision is to make sure that ICANN does not succumb to foreign pressure to unilaterally release itself of its relationship with the U.S. government. There has been widespread disagreement as to how we should implement DNSSEC, a secure version of the domain name system. This is presumably something that ICANN should lead on, but since the organization has failed in this regard, it would be appropriate for the federal government to step in and improve the security of the Internet.

Opinion: Why it takes 3 years to make a plan is beyond me, especially when NIST is supposed to do so many things in a single year and in 3 years create and implement enforcement and national licensure programs. I don't see why one of the most key systems of the Internet requires a 3-year timeframe to create a plan, while enormous volumes of other work is compressed so unrealistically. If priorities are to be set, keeping the domain name system working properly is about as high a priority as can be identified for the ongoing operation of the Internet. Regardless of the technical decisions associated with securing the Internet, which the Advisory Panel can be instrumental in helping to address, a plan need not wait for technical decision-making to be completed.

The cyber security awareness plan

Basics: The Secretary of Commerce is supposed to put a security awareness campaign in place to heighten public awareness of issues and concerns, communicate the Federal government's role and provide information to the public.

Section by section analysis: No analysis is provided.

Opinion: Other than the notion that government led awareness programs can be seen by some as propagandistic, there is no reason not to do this, even if it will be a drop in the bucket compared the the awareness people are getting every day from the news media.

Research and development

Basics: The NSF is given a priority mission to support research to figure out how to (1) design and build secure and reliable complex software intensive systems, (2) test and verify that software is free of significant known security flaws, (3) test and verify that software obtained from a third party correctly implements stated functionality, and only that functionality, and (4) guarantee the privacy of information, (5) build secure new protocols, (6) determine the origin of a message transmitted over the Internet, (7) support privacy with security, and address the insider threat. NSF is also supposed to support research that evaluates secure coding education and improvement programs, explores new methods of integrating secure coding into core curriculum, and to report on the state of secure coding education in America's colleges and universities for each school that received substantial funding. Institutions of higher education will be funded to establish cybersecurity testbeds capable of realistic modeling of real-time cyber attacks and defenses to support the rapid development of new cybersecurity defenses, techniques, and processes, and added funds for scholarships will also be made available.

Section by section analysis: No analysis is provided

Opinion: This is the area where 30 years of neglect and subversion has caused many of the problems we face today. Unfortunately, the specifics of the program only scratch the surface of the issues we face as a nation, and they direct a focus that may not really suit the national need. Some details of my views are provided here:

- Secure and reliable complex software intensive systems are certainly important, but we don't know how to do even simple secure systems well. The area that would be most effective in this space would likely be designing components with known security properties and combining them into secure composites by understanding how to compose them.
- Testing and verifying that software is free of significant known security flaws is a very important research area, but many of the most effective methods are illegal today and cannot be effectively researched with real systems because of the Digital Millennium Copyright Act. A change to the DMCA to allow the appropriate activities for research purposes would need to accompany this research effort in order for the research not to be hobbled.
- To test and verify that software obtained from a third party correctly implements stated functionality, and only that functionality, is and will remain infeasible for the foreseeable future because it depends on being able to prove both sufficiency and necessity for software, which is a known unsolvable problem for the general class of software. Nevertheless this is a laudable goal. For restricted classes of software this may be feasible, and the key is to explore limited function systems that have provable properties. With these properties, testing will also be feasible. This links closely to the notion of designing small secure components and compositions of those components to create secure systems. This is discussed above.
- Guaranteeing the privacy of information is an important objective, but information protection research has been done in this area for a very long time, and this has been done at the expense of research in other areas. In fact, the lack of research in assuring the integrity of information and systems is a large part of the reason for the lack of privacy because privacy can only be achieved with integrity. The major problem faced today is an integrity problem and not a privacy or secrecy problem.
- Building secure protocols is certainly important, and there is a lot of fine research in this area. But this is not the major source of the challenges faced today. The problem is that those implementing protocols, especially for new services, do not usually know or care about the issues underlying the design of secure protocols. Without regulatory requirements for their use, the research will be of little effect.
- Determining the origin of a message transmitted over the Internet is typically called "attribution". In particular, it is called level-2 attribution. There has been funded research in this area for some time, and it has made substantial progress. However, the need for additional research in this as well as level 3 and 4 attribution is certainly clear. This effort should be expanded to cover the entire spectrum of attribution issues.
- Supporting "privacy with security" seems to imply that privacy is not part of security. This demonstrates a lack of clarity around definitions that should be addressed in the bill as well as elsewhere.

- Addressing the insider threat is certainly important, and it is an area requiring substantial research that should be funded by the NSF.
- Research that evaluates secure coding education and improvement programs is an outstanding idea. Supporting new methods to integrate secure coding into core curricula is an excellent idea, but research is not required in order to do this. Reporting on the state of secure coding education in America's colleges and universities for each school that receives substantial funding is an excellent idea, but perhaps a better idea would be to fund universities and programs that have such programs. The government has a long history of supporting only a limited number of schools in this area and in this case, it would be wise to support more programs in more schools rather than to continue to focus on a few schools that have failed to address the needs historically.
- Establishing cybersecurity testbeds capable of realistic modeling of real-time cyber attacks and defenses to support the rapid development of new cybersecurity defenses, techniques, and processes is an excellent idea. It would be wise to build on the previous work in this area rather than to start from scratch.
- Added funds for scholarships will also be helpful in building capacity.

The long history of inadequate funding in this area is enormously problematic. Even when legislation allocates funds to research the funds are rarely actually made available through the budgeting process. It is not unusual to have $120M allocations but budgets of only $20M. Unless the legislation provides the means to prioritize this research above other priorities for the NSF, the research will, again, end up not really being adequately funded.

The long-term lack of a scientific approach to information protection has long plagued the field as well. The legislation would be well served to require that work that is funded include experimental validation of all results including proper social science methodologies and controls to measure the efficacy of controls and acknowledge that information protection is as much a people problem as a technical one.

Historically, the NSF has also been required to go to the NSA for reviews of security-related research, and this has acted to stunt the growth of the field in areas where the NSF has decided, for whatever reason, to not support research. This must end. The NSF should not rely on assistance from other Federal agencies in the evaluation of research proposals, but rather should have an independent outside expert review panel that is non-governmental and excludes researchers it funds. In this way a fair and independent review process can be undertaken to help shake the NSF free from the influences that has stifled research for so long in this arena.

Another important improvement would be to fund three groups of university researchers with the objective of building national capacity in the cybersecurity arena.

- Select individuals who have a long track record of research in these areas should be funded. These individuals are the senior research community that represents the last of those who hold the historic knowledge of the field that is rapidly being forgotten by newer researchers who often redo research in areas that were long ago considered settled.

- A larger number of new researchers in the field should also be funded to get their careers started and assure that the best and the brightest entry-level researchers have a better chance of getting tenure. This sponsorship should also include support for meetings and the creation of refereed publications.
- A third element is to fund a wide array of different mid-level researchers at relatively small levels on the order of $50K to $150K per year for a period of 2-5 years and to spread that funding across many institutions rather than to continue to focus large amounts of funds on a small number of institutions that have been designated by NSA to support the NSA research agenda. This will help to build capacity and provide ongoing support for those researchers who have made it to the mid-level of tenure in the University but whose careers have a long way to go. It will help them build research programs and support younger faculty and graduate students.

Another key issue in research funding is that the "equities issue" in which those who attack information systems to advantage the government have been more highly funded than, and had selective control over funding for, defensive efforts. The equities issue prevents defenders from finding out about attack methods while assuring that the attackers know about the defenses. This advantages the attackers, with the result that the defenses that are supposed to support the national infrastructure are inferior to the attack mechanisms available to break into these systems. As a nation, we can no longer afford to continue to weaken our own defenses and prevent our researchers from making progress to strengthen our attackers.

Additional areas that are also good candidates for NSF research include, without limit,

- Availability
- Use control
- Accountability
- Digital forensics examination
- Deception and counterdeception
- Control architectures and alternative approaches to control
- Secure virtualization and isolated sub-file-system areas
- Limited functionality, sharing, and transitivity
- Information control procedures including retention and disposition processes
- Drop boxes and processors
- Security fault isolation
- Independent computer and tool use by auditors
- Information flow controls
- Integrity shells and related integrity mechanisms
- Least privilege mechanisms
- Lockouts

- Minimizing copies of sensitive information
- Multi-person controls and multi-version programming
- Numbering and tracking for sensitive information
- Path diversity
- Periods processing and color changes
- Properly prioritized resource usage
- Separation of duties and functions
- Simplicity principle
- Spread spectrum-like approaches to protection
- Strong change control
- Suppression of incomplete, erroneous, or obsolete data
- Tempest protection
- Temporary blindness
- Time, location, function, and other similar access limitations
- Trusted applications
- Information warfare and national security strategies

In short, there are a wide range of longstanding and important research areas that should be pursued and NSF should have a far more extensive program, addressing all of these issues at more depth and over a far longer period.

The competition and challenge

Basics: NIST will establish cybersecurity competitions and challenges with cash prizes to (1) attract, identify, evaluate, and recruit talented individuals for the Federal information technology workforce; and (2) stimulate innovation in basic and applied cybersecurity research, technology development, and prototype demonstration that have the potential for application to the Federal information technology activities of the Federal government. High school students, undergraduate students, graduate students, and academic and research institutions are included.

Section by section analysis: No analysis was provided for this section.

Opinion: While such competitions are a reasonable idea, the key to success in this arena is to provide places for candidates to "play" with security-related issues in a safe and legal environment. It is vital that students learn how to stay legal while doing legitimate work in the information protection arena, that they find ways to innovate while still following rules, and that they learn to think about the broad range of issues rather than focus narrowly on how to attack one mechanism.

An ideal model is to start with summer internships modeled after the Cyber-Defenders program at Sandia National Laboratories that preceded the Cybercorps. It is also worth noting that such competitions tend to feature attacking computers rather than defending them, and defending computers and networks is a far more complex task than attacking them. Competitions should include creating and implementing defenses and include the same sorts of legal restraints that are put in place for real systems.

A public clearinghouse

Basics: The Commerce department serves as the clearinghouse of cybersecurity threat and vulnerability information to Federal government and private sector owned critical infrastructure information systems and networks. They (1) get access to all relevant data concerning such networks without regard to any provision of law, regulation, rule, or policy restricting such access; (2) manage the sharing of Federal government and other critical infrastructure threat and vulnerability information between the Federal government and the persons primarily responsible for the operation and maintenance of the networks concerned; and (3) report regularly to the Congress on threat information held by the Federal government that is not shared with the persons primarily responsible for the operation and maintenance of the networks concerned. They also control how sharing is permitted and supported between critical infrastructure providers and the Federal government.

Section by section analysis: One major weakness of existing federal cybersecurity efforts is the sharing of information, both within the federal government and with industry. Agencies are not willing to share data with each other. The federal government has access to threat data and does not share it with industry (who may be the target of an attack). The CSIS Commission explicitly called for the government to recast its relationship with the private sector and promote information sharing in order to improve cybersecurity overall. The legislation would require the government to come up with a way by which it will share information with the private sector. By exempting the data managed by the clearinghouse from FOIA requests, we hope to encourage industry to share their data.

Opinion: This will almost certainly not work, even if it is worth trying to get it to work. The model that has worked best historically is the NSTAC model, but this will not provide for the sort of real-time sharing that is anticipated by the present situation. Sharing has also been problematic for the private sector because of the one-way nature of information flow (the government appears to listen but gives no feedback and provides nothing of use to industry). Industry has built its own intelligence operations in the form of commercial firms that provide limited intelligence, and gain decreasing value from the interaction with the Federal government. In addition, many firms are multi-national and by their nature do not favor the interest of the US government over their corporate interests, which may be better served by not providing information.

There are also serious risks associated with the sharing of security-related information in that those who share the information risk its being used against them. There is real value in not releasing information on weaknesses or even on the status and mechanisms associated with security infrastructure. Among other problems, it provides intelligence to attackers on the extent to which their attacks are working and allows them to do experimentation with feedback. There is also a long history of government abuse of such information and their inability to keep it private. Such a database also provides a very efficient means of performing systematic attacks, which is the thing it is supposed to act to mitigate.

Risk management reporting

Basics: The President, or a designee, reports to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Science and Technology on the feasibility of (1) creating a market for cybersecurity risk management, including the creation of a system of civil liability and insurance (including government reinsurance); and (2) requiring cybersecurity to be a factor in all bond ratings. The President issues orders to do it. An authentication and civil liberties report is required.

Section by section analysis: No analysis was provided for this section.

Opinion: The notion of creating a market for privacy and civil liberties seems to me to be ridiculous on its face. The notion that market forces will provide proper optimization for information protection has never been sensible, and certainly is not sensible for the national security. For example, what would prevent an enemy from using its financial resources to simply buy victory in an information war? Similarly, bond ratings have proven to be problematic in the financial markets and a similar result will likely occur in a security market.

Civil liberties enforcement historically falls under the realm of the Justice Department, but they have few meaningful laws to enforce when it comes to information protection issues, and they don't have the knowledge, skills, or capacity to deal with these sorts of crimes. The issues also extend beyond national boundaries, which limits what the Justice Department can do. The information gathering functions, while facilitated by the Secret Service Task Forces, remains very inefficient and of only limited effect, and there is no national database or reporting mechanism to track computer-related crime as there is for other types of crimes. Risks cannot be realistically understood until actual events are systematically reported and relevant information is released for analytical purposes. Without data release disclosure laws we would be largely unaware of the privacy-related events happening every day, and these are only the tip of the iceberg when it comes to what is really going on.

Responsibility and reporting

Basics: The President:

- Develops and implements a comprehensive national cybersecurity strategy within one (1) year. This includes a long-term vision of the nation's cybersecurity future and a plan that encompasses all aspects of national security, including the participation of the private sector, including critical infrastructure operators and managers.
- May declare a cybersecurity emergency and order the limitation or shutdown of Internet traffic to and from any compromised Federal government or United States critical infrastructure information system or network.
- Designates an agency to be responsible for coordinating the response and restoration of any Federal government or United States critical infrastructure information system or network affected by a cybersecurity emergency declaration.
- Reviews equipment that would be needed after a cybersecurity attack and develop a strategy for the acquisition, storage, and periodic replacement of such equipment.

- Directs the periodic mapping of Federal government and United States critical infrastructure information systems or networks, and develops metrics to measure the effectiveness of the mapping process.
- May order the disconnection of any Federal government or United States critical infrastructure information systems or networks in the interest of national security.
- Directs an annual review of all Federal cyber technology research and development investments.
- May delegate original classification authority to the appropriate Federal official for the purposes of improving the Nation's cybersecurity posture.
- Promulgates rules for Federal professional responsibilities regarding cybersecurity, and provides the Congress an annual report on Federal agency compliance with those rules.
- Directly acts to punish violations and provides certification of legality to US persons.

Section by section analysis: No analysis was provided for this section.

Opinion: Of course this process puts a new and substantial burden on the executive branch, but this is outside of the purview of this discussion. From a technical standpoint:

- For the President to plan for the participation of the private sector, including critical infrastructure operators and managers, seems to me to be problematic, at least as the private sector today is composed of private companies, many of which are not even US in ownership.
- While the President may declare a cybersecurity emergency, ordering the limitation or shutdown of Internet traffic to and from any compromised government or critical infrastructure information system or network may be extremely problematic. For one thing, even if ordered, it is not clear that such an action can be technically accomplished upon order. Furthermore, such a limitation or shut-down may well create large-scale failures of government operations, missions, or national infrastructures, because many such systems now depend on Internet connectivity for their proper operation. In order for this to be feasible, these systems would first have to be disentangled from the Internet. This would be an excellent strategic approach, but it flies in the face of current movements in technology including the "smart grid" approaches and the pricing models associated with the energy and other markets as they currently exist.
- The designation of an agency to be responsible for coordinating the response and restoration of any Federal government or United States critical infrastructure information system or network affected by a cybersecurity emergency declaration would likely be FEMA, as this is really the only agency that deals with disasters of this sort today. But no current agency is prepared for any such responsibility.
- Reviewing equipment that would be needed after a cybersecurity attack and developing a strategy for the acquisition, storage, and periodic replacement of such equipment is problematic because almost all of the equipment is privately owned and some of it, particularly in the critical infrastructure arena, is very expensive and custom

built. A better approach would seem to be the creation of a national industry that provides key pieces of equipment with a very rapid manufacturing capability so that critical equipment can be built in the United States in a short time frame and deployed without relying on external capabilities.

- The periodic mapping of Federal government and United States critical infrastructure information systems or networks, and metrics to measure the effectiveness of the mapping process seem reasonable but hardly seem to be the sort of thing that would be mandated by congress. Such mapping is regularly done today and, subject to various inaccuracies, is a relatively simple problem.
- Ordering the disconnection of any Federal government or United States critical infrastructure information systems or networks in the interest of national security is problematic in the same way as the emergency declaration identified above. In order for this to be a functional capability, a national level effort would have to be put in place along with the creation of supporting enforced standards to assure that such separation from the Internet would function and not be destructive to the critical infrastructures or national missions. To the extent that this is a critical issue, it should be mandated throughout the legislation and dramatic changes put in place to force it to be done. The likely time frame would be in the 5 year range for initial testing of such a capability.
- The annual review of all Federal cyber technology research and development investments is an excellent idea.
- The delegation of original classification authority to the appropriate Federal official for the purposes of improving the Nation's cybersecurity posture is reasonably compatible with other current laws of similar sort.
- Promulgating rules for Federal professional responsibilities regarding cybersecurity, and providing the Congress an annual report on Federal agency compliance with those rules is workable.
- Having the President directly act to punish violations and provide certification of legality to US persons seems to me to be in appropriate, as legal punishment is normally considered in the purview of the courts.

Quadrennial review

Basics: Beginning with 2013 and in every fourth year thereafter, the President, or a designee, reviews the cyber posture of the United States, including an unclassified summary of roles, missions, accomplishments, plans, and programs. The review includes a comprehensive examination of the cyber strategy, force structure, modernization plans, infrastructure, budget plan, the Nation's ability to recover from a cyberemergency, and other elements of the cyber program and policies with a view toward determining and expressing the cyber strategy of the United States and establishing a revised cyber program for the next 4 years. The Chairman of the Advisory Panel submits the Panel's assessment of work undertaken in the conduct of the review as of that date and includes recommendations for improvements to the review, including recommendations for additional matters to be covered in the review.

Section by section analysis: This review is modeled off of the Department of Defense's Quadrennial Defense Review to provide periodic review and analysis of the country's cyber program.

Opinion: This process should be done annually for the first several years until the situation is stabilized, and should then be set to no longer than every 2 years. This is because of the rate at which these issues change in today's environment.

The threat assessment

Basics: The Director of National Intelligence and the Secretary of Commerce shall submit to the Congress an annual assessment of, and report on, cybersecurity threats to and vulnerabilities of critical national information, communication, and data network infrastructure.

Section by section analysis: No analysis was provided for this section.

Opinion: In order to do this properly, a far better intelligence capability regarding cyber threats than exists today would have to be created. This would have to span national and international arenas and would likely involve a far greater open source effort than current methodologies support. Current threat assessment methodologies are not typically adequate to this task in the information arena and have fallen far short of the realities of the information world. There are problems associated with fusing together domestic and international information as well, and much of the information required resides in private hands. This could be better addressed with changes to laws to require reporting of certain types of events, which would then allow the data to be available for measurement as well. But current laws and regulations do not support this sort of information gathering, and without these sorts of laws, this sort of information will not be available.

Compatibility with foreign approaches

Basics: The President works with representatives of foreign governments to develop norms, organizations, and other cooperative activities for international engagement to improve cybersecurity; and encourage international cooperation in improving cybersecurity on a global basis. An annual report to the Congress is also required.

Section by section analysis: Since the Internet is not limited to geographic boundaries it is necessary to coordinate cybersecurity efforts on a global basis.

Opinion: Clearly this approach will be required to deal with the international issues associated with information protection.

Secure product and services acquisitions

Basics: A Secure Products and Services Acquisitions Board responsible for cybersecurity review and approval of high value products and services acquisition. This follows and cooperates with the NIST standards efforts.

Section by section analysis: Many critics have encouraged the federal government to use its acquisition authority as a way to compel software and product vendors to improve the security of their goods and services. Many contracting officers do not incorporate security provisions into acquisition contracts (either because it is not considered a performance requirement or they lack the knowledge and understanding to make it a requirement), and this Board would eliminate that problem by requiring all information and communication technologies are reviewed and approved.

Opinion: The only real problem with this provision is the development of the mechanisms by which such testing is to be undertaken. But it turns out that this is a very big problem indeed because such testing represents a substantial breakthrough in research.

Summary and alternatives

To summarize my overall thoughts, the cybersecurity bill is a reasonably good idea and it has a lot of worthwhile provisions, but more thought and care is required in the writing of such laws because they tend to have consequences that extend far beyond the intended ones. In the case of this bill, many commonly held misimpressions are superimposed on what is otherwise a reasonable set of governance decisions.

There is also a core challenge that is largely unaddressed in the legislation, and that is the means for development of national security strategy for the information arena and the information age. While the legislation puts that responsibility squarely in the hands of the President, it provides no realistic means for doing strategic development, for studying potential strategies, or for clearly understanding the elements of strategy that are appropriate to the national need. Without a clear understanding of the strategic issues, the remainder of this effort will continue to be problematic for a long time to come. Just as the nuclear age introduced strategic challenges that took a long time and a great deal of effort to gain clarity around, so may the information age.

Some overall alternatives worth consideration are:

- The NIH model: Create a cybersecurity general and create a national institutes of cyberhealth to run the information protection functions - similar to NIH - with national laboratory like status and funding for extensive research, national surveillance from cyber security participants, public health reporting requirements, epidemic tracking, and so forth.
- The national laboratories model: Repurpose national laboratory capacity toward this end and use the national laboratories as the regional centers. They can then support research and build national capabilities similar to in the NIH model.
- Create a Department of Information tasked with protecting the national information assets and moving forward the information age. This to include both the security elements and the general research and development of information infrastructure and related areas.

Any of these models might work as well as the notions put forth in the present legislation, and they might create the necessary long-term institutions of government that will ultimately be required for this aspect of the future of the nation.