ISSUE AREA 3: NORMS OF BEHAVIOR---HATHAWAY QUESTIONS

- How do we define the standards of due care?
- How do we create market mechanisms to promote good security behavior including insurance and other incentives?

To answer these two questions there are 3 items that must be considered:

A. What are the standards of care to be encouraged?
B. What is the best way to encourage compliance?
C. What is the best way to measure compliance in order to award benefits?

A. Standards of Care

1. Definitions

Terms like minimum standards and practices are too often used interchangeably and without sufficient definition.

There are higher level standards like Cobit, ISO/IEC 27002 and PCI DSS that are expressed at varying levels of abstraction, that are not technology-specific, and that require significant elaboration prior to implementation.

Then there are technology-specific, detailed, non-ambiguous, automated "best practices" like DISA STIGS, CIS Benchmarks, and NIST FDCC/SCAP which serve as widely used de facto standards with very little pre-implementation elaboration.

The higher level standards are developed using formal processes that consume considerable time. The detailed best practices are developed using an ongoing, dynamic, and less formal consensus process that moves at much more rapid pace.

Both the higher level and detailed "standards" must be accounted for since they play a significant role in prescribing cyber security practices at the enterprise operational level.

2. Different standards of care for different problems

For analytical purposes we will divide cyber threats into two categories. First is the ultra-sophisticated attack such as that carried out nation-state to nation state perhaps targeted at high value government targets. Addressing these attacks require specialized interventions that are dealt with elsewhere.

The following analysis deals with the second, much larger, category which comprises the vast majority of attacks both upon government and private enterprise.

3. Mechanisms for Selecting Standards of Care

Research (some of which is cited below) demonstrates that there are effective best information security practices already operative in the corporate world.

Government's first role ought to be to encourage the broader adoption of the security practices that have already been demonstrated to be effective.

Encouragement of the effective work in information security that has already been demonstrated should take two forms. First, entities, beyond the early adopters of these effective best practices, should be encouraged to emulate them and adopt these, or appropriately similar, practices. Second, the already-identified effective practices need to be continually adapted to keep pace with the changing technological and security needs that are inherent parts of the cyber-landscape

Government can provide a vast assist to this effort by fashioning an incentive program for the good actors that will create a business advantage for them over less careful players. In so doing, the power of the market can be harnessed to motivate improved cyber security. Since many of the organizations targeted are in fact international, improvements on a worldwide basis are possible.

Part of such a program ought to be an evaluation component which will provide a real world replication study of these practices and revision based on these follow up studies.

We propose companies have available federal incentives if they implement information security pursuant to and meet the:

- Information security procedures adopted by a Federal sector-specific regulatory agency.
- Standards established and maintained by the following recognized standards organizations:
    - International Standards Organization
    - American National Standards Institute
    - National Institute of Standards and Technology
- Standards established and maintained by an accredited security certification organization or a self-regulatory organization such as NASD, BITS, or the PCI structure.

4. Standards of Care Ought to be Based on What Works

Research shows that following well established practices of security can dramatically reduce the effects of attempted cyber incursions

The "Global Information Security Survey" conducted by PricewaterhouseCoopers found that organizations that followed best practices had reduced downtime and financial impact, despite being targeted more often by malicious actors.

An almost identical finding was reported in the "2008 Data breech Investigations Report" conducted by Verizon. This study of over 500 forensic engagements over a 4 year period including tens of thousands of data points concluded that in 87% of cases the breach could have been avoided if reasonable security controls had been in place.

Robert Bigman, the CIA's Chief of Information Assurance told attendees at the October 2008 Aerospace Industries Alliance meeting that contrary to popular belief most attacks were not all that sophisticated. Bigman said that with the use of "due diligence" between 80 and 90% of attacks could be prevented. "The real problem is implementation."

5. What Are the Practices that Work?

There is a tremendous similarity in the practices the research indicates work.

The PricewaterhouseCoppoers study isolated 7 items which characterized their "best practices group"

a) Spend on Security ---best practices companies tended to spend nearly 30% more on information security than the average organization.
b) Separate information security from "IT." Cyber security is not an IT issue, it is an enterprise wide risk management issue and successful firms treat it as such
c) Penetration testing quarterly to patch up network and application security
d) Conduct security audits to identify threats to employees and corporate IP
e) Complete a comprehensive risk assessment to classify, prioritize threats and vulnerabilities
f) Define an overall security architecture and plan based on the previous steps
g) Conduct quarterly reviews with metrics to measure effectiveness

The 2008 Breach Investigations report found 10 practices that worked

a) Align process with practice. In 59% of breaches organizations had policies in place that may have prevented the breach, but failed to follow them
b) Achieve the essential then worry about the excellent. 83% of breaches were achieved by attacks not considered highly difficult to handle, Many organizations were apparently so focused on stopping sophisticated attacks they failed to take care of the basics
c) Secure business connections with partners. Nearly 40% of breaches were associated with business partners and might have been prevented with basic business partner facing security practices
d) Create a data retention plan. 66% of breaches involved data the victim didn't know was on the system. A comprehensive plan ought to force organizations to understand where their sensitive data is and take appropriate steps to protect it.

e) Control data with transaction zones. Once data is properly categorized it can be places in an appropriate zone to allow for more sensitive data to receive more comprehensive security
f) Monitor event logs. In 82 % of cases studies information about events leading up to the attack was available and either went unnoticed or not acted upon
g) Create an incident response plan. If and when a breach is suspected an effective response plan can ensure that the breach is stopped before data is fully compromised
h) Increase awareness among employees. Increased awareness can increase timely reporting and prevent incidents as well as assist in mitigation and recovery
i) Engage in mock testing, on a mandatory and routine basis

B. Creating Incentives for to Promote God Security Behavior

1. Regulations vs. Market Incentives

Federal regulatory mandates are generally designed to protect consumers from corporate malfeasance, or as part of a social contract providing entities such as public utilities with economic viability in return for consumer protection.

Considering cyber security from the infrastructure protection and development perspective the problem is not one of corporate malfeasance, but the lack of a perceived business case for, and hence lack of sufficient investment in, cyber security.

Regulations will add cost and may not improve security. By adding cost to US firms it may even be counterproductive. As such, regulations may be appropriate for consumer protection in highly regulated sectors, but inappropriate and even counter productive for the vast majority of the economy. The model outlined above accounts for both scenarios

We do not endorse the creation of a federally specified standard of information security to be applied to the vast private sector. We are concerned that such an approach would be too static and could put U.S. business at a competitive disadvantage, since it would not apply internationally. Such an approach also might not be appropriate across various sectors, might be weaker than needed due to the political nature of the regulatory process, and hence, could be counter productive. It would also be very hard to enact legislatively.

B. Specific Incentive Models, Pluses and Minuses

1. **Proposal**: Tie federal monies (grants/SBA loans/stimulus money/bailout money) to adoption of designated effective cyber security standards/best practices. Using model described above for selecting standards and practices receipt, and on-going eligibility for federal grants and loans is made contingent on compliance with identified security practices

Advantages: No significant impact on federal budget since this money is already designated for distribution to the public. Potential for relatively immediate impact since it utilizes current standards, practices and government programs. Allows for adaptation to future needs since most applications must be periodically renewed. Renewal process in place allows for compliance testing. Reach of positive effect goes beyond major players to include broader universe of suppliers and contractors to CI/KR
Challenges: Requires government coordination and breakdown of government turf to adapt to new model.

2. Proposal Tax incentives for development of and compliance with cyber security standards practices and use of technology Using model described above for selecting standards and practices receipt, and on-going eligibility for tax credits made contingent on compliance with identified security practices.
Advantages. Same as #1 but perhaps more efficient from a federal spending perspective. Could be targeted to smaller businesses. Could be reach broader group than those likely to apply for and receive federal grants.
Challenges. Negative effect on federal budget

2. **Proposal:** Grants/Direct Funding of Cyber Security R&D the Federal Government could give grants to companies developing and implementing cyber security technologies or practices. Alternatively, R&D could be run through one or more of the FFRDCs. This would reduce the private-sector cost of developing and deploying cyber security technologies.
   Advantages: Getting ahead of emerging cyber security needs**.** Allows government to target cyber security R & D funding to their specific needs.
   Challenges: Increase in discretionary spending. Could compete with private R&D

3. **Proposal: Leverage Purchasing Power of Federal Government.** Government could increase the value of security in the contracts it lets to private sector thus encouraging broader inclusion of security in what is provided to government
   Advantages. Could facilitate broad improvement of the cyber security posture among CIKR owners and operators by "building in" security from the beginning in products and services that are developed and delivered to the government. If the requirements were extended to suppliers and sub-contractors as well, this initiative could have a significant affect on down-stream entities as well.
   Challenges. Regulatory: Rewriting FAR and DFAR regulations Policy: Requires broad interagency buy-in and enforcement Economic: Could raise the cost of contracts which must be weighed against the benefits of additional security

   4. Proposal. Streamline regulations/reduce complexity. Regulatory and legislative mandates and compliance frameworks, such as Sarbanes-Oxley, Gramm-Leach-Bliley, and the Health Insurance Portability and Accountability Act, & state regimes, could be analyzed to create unified compliance mode for similar items & eliminate any overlaps. Specialized sector specific requirements could be identified

Advantages: Compliance with one might be considered as compliance with all. Thus reducing compliance costs and allowing the freed resources to be returned to security as opposed to compliance efforts
Challenges: Due to the rapid evolutionary pace of both technology and cyber threats, any stipulated control should be regularly reviewed for adequacy and efficiency. Would require government to break down turf issues.

5. **Proposal:** Limit liability for good actors. The Federal Government could create limited liability protections for certified products and processes such as compliance proven as effective designated industry best practices using model described above. Liability might be assigned on a sliding scale such as limiting punitive damages but allowing actual damages and providing affirmative defenses with reduced standards (preponderance of evidence vs. clear and convincing etc.)
Advantages. Liability costs are among the most sensitive at senior corporate levels. Tying adherence to best practices and standards might be extremely effective in building a business case for extended cyber security investment
Challenges. Limits the rights of the customers whose data is compromised in a cyber attack; requires continuously updating evaluation criteria.

6. Proposal. Create a Cyber Safety Act. The SAFETY Act, passed after 911 to spur the development of mostly physical security technology by providing marketing and insurance benefits could be adapted to provide similar benefits for the design, development and implementation of cyber security technology, standards and practices.
Advantages. By designating or certifying organizations under the SAFETY Act for developing or using cyber security technology, practices and standards these organizations can use the marketing and insurance benefits thus providing business benefits to extending their cyber security spending beyond what is initially justified by their business plans. The program has been successful in the physical arena
Challenges. Could require government expenditure and upgrade in cyber security personnel to accommodate organizations seeking designation or certification.

7. Proposal. Create Award for Excellence in Cyber Security The Government could create an award for companies that adopt cyber security best practices (e.g. Baldridge).
Advantages. Low cost. Organizations may strive to receive the award which can be used for product marketing. Consumers may be more likely to purchase goods and services from companies that have this certification.
Challenges. Organizations may be reluctant to participate since it could increase their attractiveness as a target for attacks.

8. Mandate Adherence to Cyber Security Standards The Federal Government could mandate the adoption of cyber security best practices through new statute or regulation. This approach would require companies to deploy technologies and processes that meet performance metrics defined in the statute or regulation.

Much like Chemical Facilities Anti-Terrorism Standards for the Chemical Sector, the Government could identify cyber security requirements for different CIKR sectors. Sector-Specific Agencies (or third-party vendors) would conduct audits to ensure compliance.
Advantages. Establish a minimum security standard for CI/KR enforceable via fines or other penalties including senior corporate incarceration. Eliminate the uncertainty created by relying on the unreliable private sector market incentives. Easily adaptable to highly regulated sectors.
Challenges. Policy: Coordinating requirements for cyber security across the 18 sectors would require a complex, sector-by-sector analysis. Legal/Regulatory: Requires new regulations. Technologies and threats constantly change so regulations may quickly be out dated. Mandatory minimum standards might become de factor ceilings (e.g. campaign finance regulations) not solving the problem while creating a false sense of security. No guarantee government is adequately staffed to perform this task. Punitive approach would undermine needed cooperation with industry. Monitoring compliance would be difficult and expensive. Substantial US business costs could drive many business, jobs and tax revenues off shore worsening an already tenuous economic situation.

9. Include cyber security in rate base. The U.S. Government could begin a dialogue with relevant Federal regulatory agencies, state public utility commissions (SPUC), and the Council of Mayors to explore ways to implement early rate-based recovery of appropriate and effective cyber security investments in the rate base for affected CIKR services.
Advantages. This would capture the true cost of service for these CIKR owners and operators to provide safe and reliable service to the rate payers. Facilitated by the U.S. Government, regulators and mayors could evaluate with their utility service providers the effectiveness of existing cyber security controls and could work with those service providers to prioritize the early implementation of appropriate and effective cyber security measures.
Challenges. As part of this program, mayors and SPUCs would need to be educated on cyber threats to increase their awareness and strengthen the argument to incorporate cyber security into the rate base. Policy: Requires a broad acceptance of the need to implement cyber security controls; the Federal Government's authority to drive this process is unclear. Could drive up utility costs for consumers "Rate base" not the same for all providers as regulatory systems vary and some providers have different regulatory regimes (cable/phone) than their competitors for the same services.

10. Promote Cyber Insurance. Cyber insurance, if more broadly utilized, could provide a set of uniform and constantly improving standards for corporations to adopt and be measured against while simultaneously transferring a portion of risk the Federal government might face in the case of a major cyber event.
Advantages Insurers require some level of security as a precondition of coverage, and companies adopting better security practices receive lower insurance rates. This helps companies to internalize both the benefits of good security and the

costs of poor security, which in turn leads to greater investment and improvements in cyber-security. The security requirements used by cyber-insurers are also helpful. With widespread take-up of insurance, these requirements become de facto standards, while still being quick to update as necessary. Insurers have a strong interest in greater security, and their requirements are continually increasing. As well as directly improving security, cyber-insurance is enormously beneficial in the event of a large-scale security incident. Insurance provides a smooth funding mechanism for recovery from major losses, helping to businesses to return to normal and reducing the need for government assistance. Finally, insurance allows cyber-security risks to be distributed fairly, with higher premiums for companies whose expected loss from such risks is greater. This avoids potentially dangerous concentration of risk while also preventing free-riding Insurance companies can also provide a market based monitoring and assessment function thus reducing the cost to the government while assuring compliance with ever increasing standards and practices

Challenges. Market would need to be developed. Cyber-hurricanes represent an uncertain risk of very large losses, and as such are very difficult for insurers to plan for. Because computer systems are interdependent and standardized, they tend to be especially vulnerable to correlated losses of this nature. This fear increases insurance premiums, because insurers naturally focus on worst-case estimates of the expected loss from such an event so that they can maintain underwriting profitability. In addition, "cyber-hurricanes" raise a barrier to entry to the insurance market, because an insurer may be wiped out if a major event occurs before they have built up sufficient cash reserves. Prices for private market reinsurance for cyber-insurers is extremely high as the fear of a "cyber-hurricane" is felt most by the reinsurance community. Second, because cyber-insurance is a relatively new area, insurers are hampered by a lack of actuarial data with which to calculate premiums. In addition to increasing price, a lack of data leads to problems with the risk analysis undertaken by companies when deciding whether insurance against a particular risk is worthwhile. A lack of data also makes cyber-insurance appear less desirable to companies, while simultaneously increasing the price of cyber-insurance.

C. How Best to Monitor Compliance

It is sometimes blithely asserted that if the private sector doesn't do a better job of cyber security the government will simply have to regulate them.

Often these assertions are followed by suggestions that Sarbanes/Oxley/GLB or HIPPA standards could simply be expanded.

Leaving aside the broad policy problems with these simple solutions which are articulated above, research suggests that such expansion of government regulation is unlikely to succeed even if enacted.

The sixth annual Global State of Information Security study conducted by PricewattershouseCoopers and reported in the October edition of CIO Magazine reports on regulations such as HIPPA and Sarbanes Oxley. That study found only "44% of respondents say they test their organizations for compliance with whatever laws and industry regulations apply." The study notes that this is indeed an increase in compliance, but it is extremely noteworthy that several years after these laws and their regulations have been in effect, well less than half are even testing for compliance.

CIO goes on to note "many organizations aren't doing much beyond checking off the items spelled out in regulations---and basic safeguards are being ignored" (which is consistent with the findings of the 2008 Data Breach Investigations Report cited earlier).

The federal government's lack of success in getting federal agencies to meet their own FISMA requirements also suggests this is not an area the federal government does well.

It is impractical for the federal government to take on the massive role of determining, monitoring and constantly adjusting cyber security requirements funded only by tax dollars.

Far more practical would be for the federal government to use its resources to establish a functional private sector system which the federal government could participate in and where necessary regulate. Insurance companies are the best available vehicle for such a program.

The insurance industry is in a uniquely motivated to understand and communicate to its insured's what are the standards of due care appropriate for the management of network security because they have "skin in the game". That is to say, in the event of a loss it is the insurance company that will pay excess of any self-insured retention, and any damages to third parties as well as reimburse the policyholder for any loss of business and additional expense associated with the event.

A robust cyber insurance industry, operating under traditional regulatory regimes, could serve the public interest by providing a mechanism for continually upgrading security practices and standards, monitoring compliance and reducing governments risk exposure in the event of a cyber hurricane.