Testimony of

Sally Katzen, Esq.

Visiting Professor of Law, George Mason University School of Law &
Senior Consultant to the George Mason Law School's
Critical Infrastructure Protection Program

before the

Subcommittee on Emerging Threats, Cybersecurity, Science and Technology

entitled

"Enhancing and Implementing the Cybersecurity Elements of the Sector Specific Plans"

Wednesday, October 31, 2007

Chairman Thompson, Subcommittee Chairman Langevin, Ranking Member McCaul, and Distinguished Members of the Subcommittee:

Thank you for providing me the opportunity to testify before you today on a subject that is vitally important to the American people – enhancing and implementing our plans to better protect our Nation's critical infrastructures from computer or cyber-related attacks, as well as other threats, natural or man-made. I am Sally Katzen, and I am here today by virtue of Chairman Thompson's invitation to Daniel D. Polsby, Dean and Professor of Law at the George Mason University School of Law, and Acting Director & Principal Investigator for one of its affiliated centers, the Critical Infrastructure Protection (CIP) Program, to appear before you today.

The CIP Program at the GMU School of Law is unique in that it fully integrates the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems and economic processes supporting the Nation's critical infrastructures. The Program began in 2002 as the result of a grant from the National Institute of Standards and Technology (NIST) at the U. S. Department of Commerce. Since that time, the CIP Program has undertaken a broad range of Critical Infrastructure-related research projects and sponsored many workshops and events through the on-going relationship with NIST. See http://cipp.gmu.edu/history. A key principle of the CIP Program is its outreach to the public sectors (federal, state and local), private industry – including but not limited to the private sector owners and operators of critical infrastructures/key resources (CI/KR) – the academy, and non-governmental organizations. Such inclusive, participatory and diverse "public–private partnerships," as Members of the Subcommittee well know, are essential to better protecting and defending the Nation's CI/KR.

The CIP Program also has conducted research, surveys, studies, and workshops supported by grants and contracts from two other federal agencies; the financial details for these and the NIST grant are provided in the financial disclosure form filed by the CIP Program on my behalf with the Committee. They cover published and non-published research and analysis for the U.S. Department of Homeland Security (DHS) and for the Office of Electricity Delivery and Energy Reliability at the U.S. Department of Energy (OE-DOE). It was through the CIP Program's contract with DHS that I became affiliated with the Program as a senior consultant. For one project under the contract, I led a multidisciplinary team of CIP Program researchers and legal interns from GMU School of Law in an examination of the DHS's authorities in the context of the Homeland Security Act of 2002 (as amended) and other laws. In particular, we looked at the National Infrastructure Protection Plan (NIPP) and Sector Specific Plans (SSPs) that were then in draft form. We studied CI/KR information collection, sharing, use and protection issues, including what is commonly referred to as the "NIPP metrics collection program." More information on this project can be found on the CIP Program website, http://cipp.gmu.edu/projects/NIPPMetricsProj.php.

For the record, I am speaking today as a faculty member of the School of Law and as a senior consultant to the CIP Program. However, the views and opinions expressed are my own and also reflect those of two senior CIP Program research staff members, Mr. Michael Ebert and Dr. Christine Pommerening, who have led or participated in a number of CIP Projects related to the interests of this Subcommittee and the full Committee. In addition to teaching constitutional and administrative law at the School of Law and my work with the CIP Program, my remarks today draw from my career in the federal government during the 1990s.

It is perhaps appropriate to note at this point that during the 1990s, critical infrastructure protection issues became part of the national debate. In 1996, the President signed Executive Order 13010, creating the President's Commission on Critical Infrastructure Protection (PCCIP). In the fall of 1997, the Commission released a report, *Critical Foundations*, which, among other things, identified cybersecurity risks associated with interconnected computer systems, networks, and electronic devices that, in turn, control critical infrastructure assets such as those found in energy, water, dams, nuclear power, and other CI/KR sectors as particularly serious and significant for our Nation. John McCarthy, the CIP Program's Director from 2002 until August

2007, was then serving in the federal government and made major contributions to that report and other CIP initiatives.

From 1993 to 1998, I was Administrator of the Office of Information and Regulatory Affairs (OIRA) at the Office of Management and Budget (OMB), which was tangentially involved in these issues. I then served as Deputy Assistant to the President for Economic Policy and Deputy Director of the National Economic Council, and then as the Deputy Director for Management of OMB until 2001. Among my responsibilities during my federal service that are relevant to my appearance here, I oversaw an interagency process that implemented the Paperwork Reduction Act of 1995 (PRA); was involved in various preparedness activities; and was instrumental in setting up a cooperative, collaborative public–private sector partnership to prevent a less nefarious but potentially serious failure of computer networks and digital control systems known as "Y2K." In many ways, Y2K provides a model for how the federal government, faced with a complicated set of problems that cut across government agencies, state and local governments, multiple industries, and thousands of firms both regulated and unregulated, can use its people, its convening powers, and offers of its considerable resources to successfully address an urgent situation the resolution of which was far bigger than any one institution or corporation. During Y2K, the federal government showed leadership in addressing the vulnerabilities in its own computers, networks, and systems at the same time as it offered help to the private sector. This, in my view, is the kind of positive, effective approach we now must put into action to protect critical infrastructures from malicious cyber attacks.

Challenges Facing DHS and the other Federal Sector-Specific Agencies

Although no one seems to know for sure the origin or accuracy of an oft-cited statistic, it is generally believed that the private sector owns and operates roughly 80 percent of the Nation's critical infrastructures, as these assets have been defined by Acts of Congress, Homeland Security Presidential Directive 7 (HSPD-7) and particularly the NIPP. As this Subcommittee heard on October 17th with respect to cyber and physical CIP standards that soon may apply to all owners, operators and users of the bulk electric power system, critical infrastructures are just as likely to be under the ownership and/or control of small and medium sized businesses as large corporations. And one of the challenges now facing the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC) is to identify all relevant players – particularly small businesses that have heretofore operated under the radar of NERC – so as to determine those responsible for the reliability and security of our Nation's electric power grid.

Across the 17 CI/KR sectors established by HSPD-7, there is a great variety of business structures, organizations and cultures, practices, regulatory requirements, and standards. Some of the 17 sectors, such as energy or nuclear reactors, have long histories with government regulators at the federal level; typically, these public–private relationships are well established and have produced networks of people and channels of communication. In other sectors, such as chemicals, federal CIP regulation is relatively recent and private–public trust relationships are not yet well formed. In still others, such as commercial facilities, regulation is largely non-existent. To further complicate the matter, enterprises may have lines of business in more than one CI/KR sector. Moreover, some of an enterprise's CI/KR activities may be regulated, others not – and the enterprise may well have several other formal (mandatory) and informal (voluntary) policies, guidelines and standards; these other frameworks may have degrees of nexus to CIP, but also are distinct from it.

DHS has sole Sector-Specific Agency (SSA) responsibilities for ten of the 17 CI/KR sectors. Internally, DHS's Office of Infrastructure Protection (OIP) is responsible for five sectors (chemicals, commercial facilities, dams, emergency services, and nuclear reactors). The Office of Cyber Security and Communication (CS&C) is responsible for two more sectors (communications and information technology); and the Transportation Security Administration (TSA), the U.S. Coast Guard, Immigration & Customs Enforcement, and the Federal Protective Service serve as SSAs for postal and shipping, transportation systems and government facilities. For all seven other CI/KR sectors, Agriculture and Food, Banking and Finance, Defense Industrial Base, Energy, National Monuments and Icons, Public Health and Healthcare, and Water, DHS must rely on other federal SSAs – of which there are eight.

Meanwhile, the states are vital partners in CIP. Traditionally, state (and often local) governments have been at the front line of awareness, preparedness and response when it comes to CI/KR companies within their jurisdictions. Some of these companies are regulated at the state level; others have developed informal but nonetheless effective relationships with state and local officials. Whether such relationships can survive where there are fears of impending federal preemption is an open question.

So, DHS has to coordinate (a) within DHS – itself an amalgam of existing federal pieces and new homeland security requirements; (b) with other federal agencies – some with regulatory authorities, others not; and (c) with state and local agencies – again, some with regulatory authorities, others not. Consider nuclear power reactors. Some of these facilities are owned by the federal government, but most are in the hands of the private sector. DHS is the SSA for this sector, but the Nuclear Regulatory Commission (NRC) has CIP-like operations and safety regulatory reach, and FERC and the states have concurrent or overlapping authorities over other aspects of nuclear power.

For DHS to successfully navigate these waters requires an almost unprecedented level of constructive interplay between and among many federal and state agencies. For the most part, DHS has few authorities to force its federal or state partners or the private sector owner/operators of CI/KR to "do as we say" with regard to cyber and physical CIP. And we are *not* suggesting that DHS be given any new "command and control" authorities in the short term or possibly even the long term. Indeed, we believe that the situation would not be improved either by giving the Department additional SSA responsibilities for the seven other CI/KR sectors or by giving it any additional authorities over private-sector owners or operators of CI/KR. Rather, we believe that DHS should adroitly use its convening powers, take full advantage of its collaborative opportunities, and work collegially through problems with those federal and state agencies that have not only the expertise but also the experience and relationships with their private sector counterparts in the various CI/KR sectors.

Regrettably, the track record to date indicates that DHS has not taken advantage of the remarkable authorities and informal leadership opportunities it already has. Six years and billions of dollars expended after September 11, 2001, where do we stand? Part of the answer to this question is revealed by the title of today's hearing, "Enhancing and Implementing the Cybersecurity Elements of the Sector Specific Plans." In other words, we are still, for the most part, talking about plans. The SSPs were written by SSAs, with critical inputs and expertise from the private sector, and are necessarily only as good as the levels of collaboration and trust that went into them. And how good are they? According to the U.S. Government Accountability Office (GAO) as well as other experts, these plans fall short in many respects, including but not limited to cybersecurity. For that reason, we are here today talking about enhancing plans and then implementing them. We have a long way to go.

The Special Challenges of Cybersecurity

Turning to the special challenges of cybersecurity, the most fundamental challenge for better protecting the Nation's CI/KR from cyber attacks is understanding as best we can the full panoply of existing, emerging, and likely future cyber exploits that could be launched against enterprises and systems that are extremely complex, technically diverse, and operate within and across corporate cultures – that cover a vast range of cyber (and physical) security awareness, experience and protection – and within and across sovereign jurisdictions with very uneven laws, regulations, and cyber capabilities. Given this, the Congress, the executive branch, and DHS in particular are to be commended for not embracing a command and control, one-size-fits all approach to cybersecurity. The velocity of technological change, knowledge and progress in information technologies, particularly cyber defenses, is very rapid, perhaps exceeded only by the developmental velocity of cyber threats. For these reasons, policymakers should continue to avoid establishing or otherwise anointing a highly prescriptive set of cybersecurity standards.

Another challenge that may not fully be appreciated is the trend mentioned by some Members and witnesses at the October 17th hearing. That trend, within the corporate world generally and particularly in firms that have CI/KR, is that companies are replacing older, private analogue networks with newer, faster and more efficient networks and intranets. These are based upon IP protocols, whose primary design considerations were *not* security, and the public Internet. In the past, many regulated vertically integrated electric power utilities with CI/KR assets in generation, transmission and distribution used private microwave networks to communicate and control this triad of electricity production and delivery elements. Technological advances, industry restructuring (whether or not driven by wholesale or retail competition laws), and market pressures changed this. Particularly where generation, transmission and distribution were intentionally if not legally "unbundled," the old private networks went away. In many ways, these changes have been beneficial to producers and consumers of electricity, but the move to public networks based upon IP protocols has engendered a host of new cyber-CIP risks. Another manifestation of this trend is that many companies are building seamless intranets and internet sites that intentionally provide access to consumers, commercial partners (upstream and downstream) and investors who are outside the enterprise itself. These seamless systems may also be hooked into hitherto "back office" operations that control and secure a company's critical infrastructures. From a perspective of efficient business integration and exploiting the benefits of technology, this makes sense – but, again, it brings with it a host of new cyber-CIP risks.

Finally, we are presented by the challenge caused by the fact that responsibility for understanding and protecting against cyber-CIP risks – both in the private sector and in government – has too often been confined to those in the enterprise who own, operate and maintain computers, servers, and networks – *i.e.*, the corporate or government IT department. Viewing cybersecurity as "an IT problem" that only can be fixed by a company's IT department greatly understates the problems and seriously misperceives the solutions. Stated another way, stove-piping cybersecurity into IT prevents it from being recognized and treated as part of an enterprise-wide set of cybersecurity risks. Nearly "bulletproof" cyber protection could be assembled by technical experts in IT departments – if sufficient funds are allocated for this purpose. But even if there is funding for bullet-resistant technical cyber, the very best technical defenses are no better than the physical security and personnel security elements which must accompany them. These elements are almost always outside the control and direction of IT, involving, for example, the human resources or the physical security departments of (or often contractors for) the company.

The importance of recognizing and effectively addressing the human aspects of cybersecurity cannot be overemphasized, for well-trained personnel are the first line of defense against threats that are more likely to come from internal sources as from threats outside the enterprise. Clearly, taking effective actions to protect critical infrastructures from cybersecurity risks known and unknown involves more than a company's chief information officer or chief privacy officer or chief security officer – provided the firm is so organized and is of a scale sufficient to afford such "C-level" structures and human expertise.

Comments on the GAO Report's Findings

This leads us back, then, to the question of how much progress we have made to date in protecting CI/KR, with particular attention to cybersecurity. The report presented by representatives of GAO in the first panel today provides qualitative and quantitative assessments of the 17 SSPs and how well each of these plans is addressing – or not addressing – 30 cybersecurity criteria. The GAO finds that 12 of the 17 plans have "comprehensively" addressed the 30 criteria. Three plans – Banking & Finance, Defense Industrial Base, and National Monuments – are characterized by the GAO as being only "somewhat comprehensive;" two SSPs – Agriculture and Food and Commercial Facilities – were found by the GAO to be "less comprehensive."

On its face, this does not sound so bad – assuming, of course, that the 30 criteria are methodologically sound measures of cybersecurity. But beneath the GAO's "highlights," a somewhat more troubling picture emerges when one looks at each and every one of the criteria – plan by plan, section by section. According to the GAO's scoring for the eight sections it has broken out in Attachment 2 of its report, the average (mean) of the number of plans that have "fully addressed" the GAO cyber criteria is as follows:

Table 1: Average Number of Sector-Specific Plans that "Fully Addressed" GAO Criteria

Cyber Criteria Section	Average (Mean) Number of SSPs that "fully addressed"	Lowest Scoring Cyber Criteria in Section
Section 1:Sector Profile & Goals	15.0	N/A
Section 2: Identify Assets, Systems, Networks & Functions	13.0	N/A
Section 3: Assessing Risks	9.5	describes incentives to encourage voluntary vulnerability assessments = only 3 SSPs "fully addressed"
Section 4: Prioritizing Infrastructure	11.5	identifies entity responsible for prioritization of cyber assets = 11 SSPs "fully addressed"
Section 5: Developing & Implementing Protective Programs	11.5	identifies programs to deter, respond & recover from cyber attacks = 9 SSPs "fully addressed"
Section 6: Measuring Progress	**9.0**	**includes developing and using cyber metrics to measure progress = only 8 SSPs "fully addressed"**
Section 7: Critical Infrastructure Protection R&D	12.4	describes process to solicit information on on-going cyber R&D initiatives = 7 SSPs "fully addressed"
Section 8: Managing & Coordinating SSA responsibilities	15.8	describes process for investment priorities = 14 SSPs "fully addressed"

We have emphasized Section 6 because being able to measure progress is essential to evaluating results for the time and money spent. Again, analyzing GAO's take for the four cyber criteria in Section 6, we find a mixed message at best:

Table 2: Examination of GAO's Section 6 Individual Cyber Criteria

Section 6 Cyber Criteria	No. of SSPs that "fully addressed"	No. of SSPs that "partially addressed"	No. of SSPs that "did not address"
Ensures that integration of cybersecurity metrics is part of the measurement process	9	3	5
Describes how cyber metrics will be reported to DHS	9	6	2
Includes developing and using cyber metrics to measure progress, [emphasis added]	8	5	4
Describes how to use metrics to guide future cyber projects	10	4	3

One of the most important criteria in Section 6 – developing and using cyber metrics to measure progress – had one of the lowest indicators of "plan goodness." Only eight SSPs fully addressed this criteria, according to the GAO, while five SSPs were found to have partially addressed it and four SSPs did not address it at all. Given that interdependencies exist among the 17 critical infrastructure sectors, the weakest plans are the weakest links in the chain, again suggesting that serious gaps exist and much work remains to be done.

Examples of Cyber Attacks and Gaps in Cybersecurity

Detailed and credible information on cyber incidents that is in the public domain corroborates this charge. This Subcommittee was provided a list of selected case histories of cyber breaches in the electric power sector during the hearing on October 17th. Consider two other incidents outside this sector:

First, it is generally well known that in the Fall of 2006, email servers for the National Defense University (NDU) were completely shut down by a successful external cyber exploit – not just for a few hours or a day, but for several weeks. Faculty, staff, and students had to rely on non-NDU email systems. What is not as well publicized is that the cyber attackers who took down the NDU email system were able to do so because they had successfully hacked into the "dot-mil" architecture.

Second, on February 6, 2007, two coordinated back-to-back cyber attacks were launched against the 13 "root servers." These root servers form the backbone of the Internet; if attackers can compromise, clog or cause to shut down enough of the root servers, all Internet traffic can be affected and – worst case – the backbone could break. In February, six of the 13 root servers were "adversely affected" by "distributed denial of service [DDoS] attacks" that appear to have originated in the Asia–Pacific region. Ironically, a new and proven protective technology developed with US leadership known as "Anycast" was available but had not been deployed on all 13 root servers. ICANN stated that the "two [root servers] worst affected do not have new Anycast technology installed." These two servers were in the United States.

Attached to this testimony as Exhibit A is a CIP Program "Cybersecurity and Liability Workshop White Paper" which references four additional cybersecurity breaches at private sector companies as the result of both external and internal exploits. Again, the facts on the ground indicate that more work needs to be done to protect cyber-CIP.

Making Sense of the Many Applicable Frameworks and Standards: A Case for an Enterprise Risk Management (ERM) Approach

When we consider possible solutions, we begin with Congress, which has required specified elements of data and information technology security in a number of laws, such as the Public Company Accounting Reform and Investor Protection Act of 2002, commonly referred to as "Sarbanes–Oxley," the Health Insurance Portability and Accountability Act (HIPAA), and Gramm–Leach Bliley. These and similar laws and the regulations implementing them require that *certain* companies must do *certain* things, and *some* of those required actions involve cybersecurity. The Congress has also imposed specified requirements on federal agencies and federal employees for cybersecurity, data and information sharing, privacy protection and personnel security.

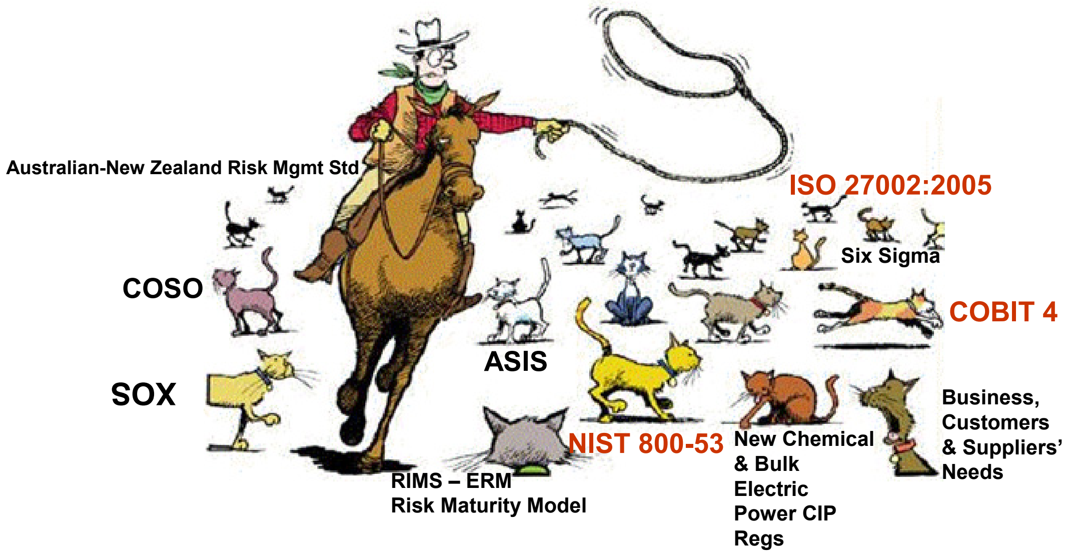
NIST has developed several "Special Publications" (SPs) on computer, information, and cybersecurity. These SPs include 800-53, *Recommended Security Controls for Federal Information Systems (Rev. 1, Dec. 2006*; which is binding on federal agencies). 800-53 was frequently mentioned at the October 17th Subcommittee hearing. The Federal Emergency Management Agency (FEMA) within DHS offers a set of useful concepts and tools that companies may use to advance their own critical infrastructure protection plans and associated voluntary measures such as vulnerability assessments. [See, *e.g.* http://www.training.fema.gov/emiweb/IS/is860.asp.] Other federal agencies may offer other frameworks.

Voluntary frameworks, standards, and tools have also been developed by such respected nongovernmental organizations as the IT Governance Institute [ITGI, co-developers with the International Systems Audit and Control Association (ISACA) of the highly-regarded "COBIT 4.0" framework]; the Committee of Sponsoring Organizations of the Treadway Commission (COSO, which has developed financial reporting, business ethics, internal controls and corporate governance frameworks); ASIS International (an organization that focuses on "Chief Security Officer" issues, including physical and personnel security frameworks); and the International Standards Organization (ISO), which develops international standards and frameworks that are ostensibly voluntary but often are codified and binding, in whole or in part, by ISO member countries. ISO 27002:2005, for example, establishes guidelines and general principles for initiating, implementing, maintaining and improving information security management. Subsets of ISO 27002:2005 have frameworks for human resource security, asset management, physical and environmental security, and incident management. Other organizations and professional associations have developed training and certification tracks that are grounded in these frameworks and standards.

Earlier this year in support of a DHS project, the CIP Program catalogued selected existing standards, training and certification tracks, and policies and procedures that could be helpful to the SSAs and private sector owner/operators of CI/KR in developing better plans and engendering higher levels of cyber, physical, and personnel security. Fortunately, there is no shortage of excellent and evolving contributions to the field. Multiplicity of security contributors is a good thing in that there are formal and informal competitions to be recognized as a leader in promoting effective levels of security, and to the extent such offerings are generally in the public domain, learning and knowledge developed by one organization can stimulate progress in others. The downside to this wealth of cyber-related guidance, standards, and education and training resources is that it makes it harder for companies to be aware of the many offerings, know how to choose among them, and, most importantly, to properly integrate them to improve cybersecurity.

The CIP Program is convinced that the key to this dilemma is integrating standards into Enterprise Risk Management (ERM) principles and techniques, represented in the picture below as the "Cowboy in the White Hat."

Using Enterprise Risk Management (ERM)
to Integrate Frameworks & Standards


Australian-New Zealand Risk Mgmt Std
ISO 27002:2005
Six Sigma
COSO
COBIT 4
ASIS
SOX
Business, Customers & Suppliers' Needs
NIST 800-53
New Chemical & Bulk Electric Power CIP Regs
RIMS – ERM Risk Maturity Model

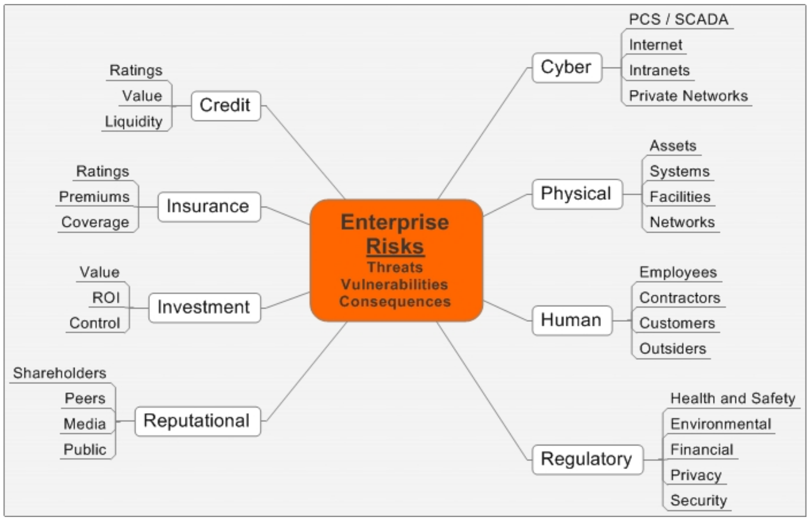
Adapted by the CIP Program from an original © Risk & Insurance Management Society (RIMS), 2006-2007. RMM, ASIS, Six Sigma, ISO 27002:2005, COBIT, COSO ,*et al* are trade- service- marks of their respective organizations.

ERM in a Nutshell: Core Principles and Processes

Based upon a review of the literature, the CIP Program developed the following definition of ERM:

> *ERM is the systematic application of strategic and operational management policies, procedures and practices aimed at identifying, analyzing, evaluating, treating and monitoring all risks to the business processes of an enterprise.*

The emphasis is on the enterprise as a whole. There is wide-spread acknowledgment that there are vulnerabilities – in turn, risks – of interdependencies among the 17 CI/KR sectors and within each of the sectors. Equally important but often not fully appreciated, especially when the discussion of risk is artificially confined to cyber-CIP and the IT department, is that corporations themselves have many risk interdependencies. Consider the following diagram that illustrates these various risk interdependencies and where they may reside:



To assess and address the applicable risks for a given enterprise, ERM models typically include the generally recognized core principles and processes set forth below. We note that many students and practitioners of ERM point to the Australian–New Zealand Standard for Risk Management, AS/NZS 4360:2004, as one of the best contemporary expressions of what ERM is; other organizations, such as the non-profit Risk and Insurance Management Society (RIMS), have developed ERM models conceptually similar to AS/NZS 4360:2004. These are just two ERM resources; in Exhibit B, *Enterprise Risk Management for Critical Infrastructures*, we provide supplemental information and examples of ERM. Common to all of these are the following ERM principles and processes:

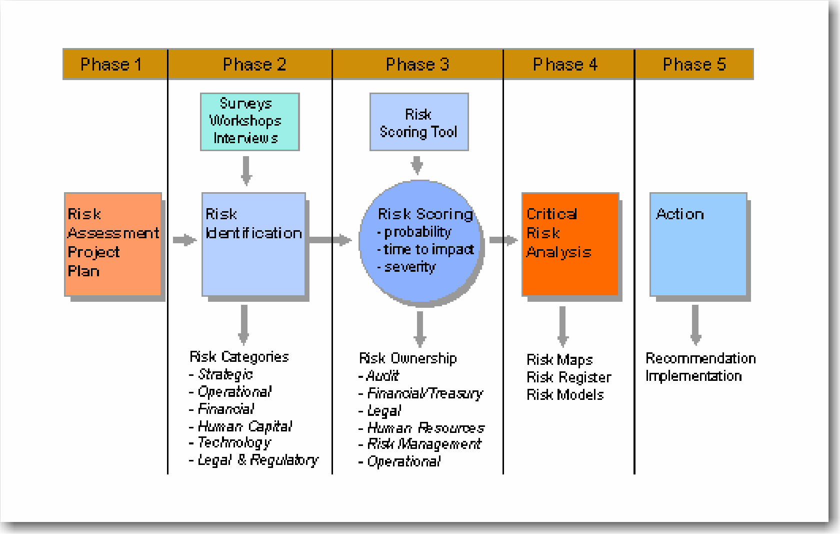
1. **Establish the context for ERM** as determined by a firm's unique business needs, regulatory environments, organizational structures, and assets of the company. Establishing the context sets up the "Risk Assessment" stage.
2. **Identify all risks** through a variety of risk identification techniques and tools. These can include interviews, surveys, on-line tools, workshops and the like, and should appropriately involve downstream and upstream stakeholders.
3. **Analyze all risks.** Whatever modest differences exist among the various ERM models, each of them stresses that risk identification, analysis, and the next step – evaluation – are not confined to a single area of the company. Thus, risks and vulnerabilities are not "stove-piped."
4. **Evaluate all risks.** This means vulnerabilities are evaluated, criticalities quantified, priorities established and mitigation roles/responsibilities assigned at an enterprise level. After this step, the enterprise's Risk Assessment (steps 2, 3, and 4 or "vulnerability assessment" in the language of the NIPP and the SSPs) leads to . . .

5. **Treat All Risks!** In other words, implement the plan.

Throughout the five steps, two other core ERM principles/processes are constantly in play:

- **Communicate and consult;** and
- **Monitor and review.**

These two are particularly important during steps 2, 3 and 4, and provide a loopback to significantly modify or merely tweak the whole exercise wherever changes may be called for. There is a helpful graphic, available on the Internet, which provides a visualization of ERM phases:



Source: http://www.aon.com/us/busi/risk_management/risk_consulting/ent_risk_mgmt/default.jsp. Accessed on 21 October 2007.

Two additional aspects of ERM should be emphasized. First, ERM requires the development and implementation of risk assessments and analyses based upon criteria and metrics that are uniformly documented; these assessments generate data (internal trails) and are verified through periodic audits. While the firm will probably not disclose to external audiences, regulatory or otherwise, the stream of data and information that assists and informs both managers and owners of risk, aggregated ERM data can inform external audiences and can provide useful indices of risk reduction over time. Second, and flowing from the first, a commitment to ERM includes a commitment to update the analysis on a periodic basis (quarterly, annually, whatever is appropriate for the enterprise) for the long haul.

The CIP Program found ERM particularly attractive because ERM shines a light on cyber-CIP risks and all other enterprise risks at very high levels of accountability in the corporation, including the boardroom. The benefits of ERM are not limited, of course, to the private sector; governments, most notably municipalities, are looking to ERM as a valuable tool. Equally obvious, ERM has benefits beyond cyber-CIP, but we believe this integrated, enterprise-level approach to the identification, assessment, and mitigation of *all* risks has particular merit in addressing cyber risks that permeate an organization's many internal structures.

For most firms that own and operate CI/KR, a good percentage of the risk-pieces are likely to fall on the operations side of the enterprise, which often is not well represented at higher levels of corporate governance. When cyber-CIP is confined to one area of the enterprise (*e.g.* the IT department), its voice, vote and authority – including "budgetary authority" – may not be adequate to the task. Therefore, placing cyber-CIP into ERM does not diminish critical infrastructure protection within a company but instead elevates it.

As awareness and corporate acceptance of ERM has grown, some firms have created broader functional responsibilities and a name for the cowboy, such as Chief Risk Officer (CRO). The CRO typically has direct lines of communication with the CEO and the firm's other C-Levels. The CRO typically has ready access to, is seen and is heard by the board of directors. Because the points of accountability for management of all risks are consolidated, ERM in theory provides the cowboy – the Chief Risk Officer or equivalent – with authorities and tools to herd several cats and thus reduce risks. Corporate resources can be more efficiently allocated by using ERM, which, after all, is an "All Hazards" approach to risk that is part of the NIPP–SSP lexicon.

Recommended Next Steps and Incentives to Get There

At the heart of enhancing and implementing the SSPs is getting firms to "do the right thing" even when there is no requirement in law for them to do so, and to repeat what we said earlier, we are *not* recommending any additional command and control authorities for DHS. We recognize that doing the right thing may provide firms with benefits and these extend beyond security. But it is also important to recognize that it will cost firms time and money; voluntarily collaborating with government on cyber-CIP is not cost free.

To be sure, companies already have many incentives to better and more comprehensively manage their risks in terms of smoother, more efficient operations. In addition, a company that lets it be known that it practices effective enterprise risk management often is rewarded in the marketplace. In 2006, Ernst & Young (E&Y) published a cross-stakeholder study entitled, "Managing Risks: Shareholder Perspectives." E&Y interviewed over 700 senior decision makers representing three distinct stakeholder groups – investors, executive management, and independent non-executive board members – to gain their perspectives on risk and risk management. The report's key findings are:

- Risk mitigation and compliance are the top risk management priorities across all three stakeholder groups.
- All stakeholders consistently state that clear ownership of risk and effective communications are key factors for successful risk management.
- All stakeholders will exercise their influence in the face of *perceived* poor risk management.
- Investors will either not invest . . . or divest in the face of poor risk management.
- High-performing companies place more emphasis on risk mitigation, compliance and seeking competitive advantage from risk management.
- High-performing companies are four or five times more likely to have a risk-aware culture.

In other words, if a firm is perceived to be, or is in fact, *not* engaging in effective risk mitigation and compliance, investors stop investing or sell off; firms that do risk management, compliance, and communications well are considered high performers who will have the confidence of investors. That is a powerful incentive government can't provide.

Having said that, but keeping in mind the criticality of advancing the ball on protecting CI/KR from cyber and conventional threats and the need to gain awareness and effective involvement from those in the small and medium business space, Congress and the federal government should consider developing incentives that will further encourage firms to do the right thing. The need for such incentives is underscored by the fact that GAO found that only three of the 17 SSPs fully addressed incentivizing vulnerability assessments.

Our suggestions for incentives include the following:

1. **Sponsor "ERM for CIP" workshops –** As part of the on-going work in providing training, conducting simulations and exercises, and convening workshops, DHS as well as the non-DHS SSAs should partner with established and recognized providers of ERM education, training and certification to develop a workshop (or series of workshops) that would be offered to private-sector

owner/operators of CI/KR. The federal government should underwrite most or all of the cost of the workshops (*i.e.*, no fee or minimal fee for those eligible to register and attend), thus providing incentives for firms to develop and implement ERM plans. If this incentive is to be offered, we strongly recommend that Congress insist on a few important qualifying criteria:

- Provide that the workshops be "customizable-off-the-shelf" (COTS) offerings from institutions and organizations that have developed well-established and accepted ERM products. Introducing high-level awareness of critical infrastructures and cybersecurity into these off-the-shelf products is an acceptable customization. An unacceptable customization, in our view, is for the federal sponsor to subordinate core ERM principles by pushing CIP to center stage. For ERM-CIP to work, it is the cowboy, not the cats, who runs the show.
- Develop selection criteria to determine companies that are eligible to attend. Preliminary research by the CIP Program using Census data indicates that the establishments in the 17 CI/KR sectors would encompass roughly 50 percent of the U.S. economy in terms of value, number of employees, and number of establishments. However, while many businesses are technically part of one or more of the 17 sectors, not all of those businesses or the assets they own and operate are truly critical for national security, economic security, or public health and safety. It is an understandable tendency for officials to seek, and the public to support, an expansive definition of what we as a Nation should protect, but in trying to protect everything we run the risk of not protecting anything truly well.
- Establish prerequisites for participants from an eligible company. The participants should be invited based on (a) qualification as measured by university degree, technical/professional certifications, or demonstrated and documented experience and proficiency; (b) enterprise-wide roles and responsibilities; and (c) diversity – the ideal workshop audience is from several CI/KR sectors.

2. **Alternatively, provide a tax credit** to qualified companies that obtain education, training, and credentialing in ERM. Congress should consider providing sufficient guidance to the Treasury Department (which will write the implementing regulations) that speak to the important criteria outlined above.

Either way, the federal government could test the feasibility and value of ERM incentives at relatively little cost, particularly if the important COTS principle and other qualifying criteria are respected. At a minimum, the Congress could authorize and fund a limited "proof of concept" pilot program, consisting of 10 or so workshops given over six months; course evaluation instruments could be developed that will provide useful feedback to the DHS, the ERM workshop vendor(s) and the Congress.

3. **Establish a public recognition and rewards program** for companies that have raised the bar on cyber-CIP. A useful analogy is the *Energy Star* program, which recognizes companies that produce energy-efficient products. To receive *Energy Star* recognition and use of its marketing symbol, products must meet certain efficiency requirements that are grounded in verifiable measurements. To receive what we might call *Cyber Star* recognition and rewards, qualifying criteria should be measurable and raise the bar over time.
4. **Provide preferences in federal government contracting** for companies that own/operate CI/KR and have obtained training and certification in "ERM for CIP" (our first incentive suggestion) and/or received the recognition/reward (our second incentive suggestion). Preferences should be sunsetted to incentivize continual improvement and continued education and training.
5. **Government leading by example.** If 80 percent of the Nation's CI/KR is owned/operated by the private sector, then governments – federal, state and local – own and operate the other 20 percent. Governments must be models of enhanced cyber-CIP if for no other reason than that failing to adequately protect 20 percent of critical infrastructures that governments own/operate for the American people is not acceptable. But there is another reason: one proven way to incentivize is to lead by example. Every successful coach, teacher, executive, or parent knows this, and it was one of the most important lessons I took from my experience at OMB during Y2K. A potent incentive for the private sector is for the public sector to clean up its act and protect the people's CI/KR – first.

Concluding Thoughts

Another very important lesson we learned from Y2K is the importance of collaborative, collegial, and effective public–public partnerships – that is, the incredible value of respectful federal–state–local government partnerships. Let me provide another even more recent example of a good public–public partnership between the U.S. Department of Energy and the states.

An obscure provision of the "State Energy Efficiency Programs Improvement Act of 1990" (P.L. 101-440) requires states to prepare and submit to the Secretary of DOE "energy emergency planning programs" if they accept federal funds for this purpose. These "state energy emergency response plans" (SEERPs), as they are now called, are in many respects state equivalents of the federal energy sector SSP. By design, these SEERPs should contain emergency planning coordinating and response components, including cyber-CIP, that are complementary to the federal energy SSP. In 1990, Congress clearly stated that the Secretary has *no* authority to dictate planning details to the states; he could review and comment, but "for informational purposes only." Recognizing the importance of SEERPs as a means to better protect CIP and cyber-CIP, DOE chose to view its limited authority as an opportunity, not an impediment. It worked collaboratively and informally with the states, engaging them through established institutions which the states knew and trusted, such as the National Association of State Energy Officials (NASEO) and the National Association of Regulatory Utility Commissioners (NARUC). The result: highly detailed NASEO guidelines for preparing SEERPs that was published in November 2005. DOE offered funding and more: it used its convening powers to bring state officials and regulators together, and DOE offered workshops, simulation exercises and the considerable expertise and experience of the department's resources. When the CIP Program evaluated 47 of these SEERPs for DOE a few months ago, it was clear that states that took advantage of DOE's offers of assistance tended to have better plans than those that did not, and plans developed after NASEO published its voluntary guidelines were, overall, better than SEERPs drafted before. Good public–public partnerships can produce valuable results.

This brings me to my final point, which goes to often obscure or seemingly arcane other federal laws, such as the 1990 energy law. I mentioned earlier that one of my responsibilities during my service at OMB was a responsibility for implementing the Paperwork Reduction Act of 1995 (PRA). I also mentioned earlier that the SSPs are written by the SSAs with input from the private sector and are necessarily only as good as the input provided. I recognize that the quality of the information provided by the private sector is dependent on many factors, several of which came to light in the controversies surrounding the NIPP metrics generally and the security-related metrics specifically. Undoubtedly, the primary concern centered on how DHS will use these metrics and whether DHS can and will provide strong assurances that the sensitive "raw data" behind metrics – if shared – will remain secure in the hands of the federal government. But the development of the metrics and collection of associated data also implicated the PRA. Some are now suggesting the PRA is an impediment to enhancing and implementing the SSPs, and that the PRA must be substantially amended for this project to proceed. That is *not* my view. The PRA provides an opportunity to enhance and implement the SSPs because it provides a known, trusted process – involving the private sector and an interagency review – to develop and collect data and information – CIP and cyber-CIP metrics – that are useful and methodologically sound.

We thank the Subcommittee for convening this hearing. As I said at the outset, six years and billions of dollars after 9/11 we are still talking about plans. If, as appears to be the case, the SSPs, taken as a whole, have not yet comprehensively developed a set of quality metrics that allow measurements and comparisons of progress or lack of progress in addressing cybersecurity criteria, then the Congress and the American public will have no meaningful benchmarks at the beginning of implementation or over time. Stated simply, unless these deficiencies are systematically addressed, we will have no idea if the expenditures and efforts we are committing to the effort are translating into measurable improvements of security. I appreciate the opportunity to testify today, and look forward to answering any questions you may have.

GEORGE MASON UNIVERSITY | School of Law

CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

3301 Fairfax Drive, MS 1G7, Arlington, Virginia 22201
Telephone: 703-993-4840; Fax: 703-993-4847

EXHIBIT A: Summary & "Moving Forward" Issues from a Critical Infrastructure Protection Program Workshop on Cybersecurity & Liability

Friday, 20 July 2007
Dean's Suite
George Mason University School of Law

Introduction

On July 20, 2007, the Critical Infrastructure Protection Program ("CIP Program") at the George Mason University School of Law held a workshop on cybersecurity and issues associated with liability. Those attending the invitation-only workshop were representatives of academia (law, economics and public policy), the US Congress, the federal government, think tanks and trade associations, and senior level executives of major insurance underwriters and reinsurance companies. A focus of the workshop was how the insurance and reinsurance industries measure and assess the cyber risks of firms seeking to mitigate their exposure to cyber-related losses.

This paper provides an overview and assessment of the workshop, and suggests steps that might be taken going forward to promote higher levels of cybersecurity awareness and protection. Reinsurers and insurers ("the industry") may play a crucial role in advancing the state of cybersecurity practices of the Nation's businesses. To use an analogy from the "bricks and mortar world", the industry has played a vital role in advancing the physical security of buildings, assets and people through the development of building and safety codes and product standards. Progress – risk reduction – has been documented through data and information often required by contractual and regulatory structures. However, at this time, there are several impediments to creating a similar, economically viable market for cyber insurance/reinsurance, most of which are associated with identifying and measuring cyber risks. As one participant remarked, the state of the industry's knowledge in writing policies for cyber risks does not readily transfer from its 150-plus years of experience in the bricks and mortar economy, and "cyber underwriting remains an art rather than a science." Another attendee pointed out a significant distinction between cyber and conventional physical risks: "Ordinarily, a fire in Cincinnati doesn't burn buildings in Indianapolis," but "cyberfires" in one location can and do burn first parties and third parties often in multiple locations and sometimes across legal jurisdictions.

Structure of the Market

The insurance/reinsurance market for cyber liability is relatively immature and evolving, starting some ten years ago with a focus on "dot-com" types of exposures. Insurance/reinsurance has the potential to become an important tool in protecting vital data/information systems and networks, thus increasing the overall security of the nation's economy. Currently, however, "cyber insurance" is a catch-all term for many different kinds of insurance, covering both first-party and third-party risks such as damage from computer malfunctions, viruses, network outages or congestion, external hacking, internal sabotage and theft, web content liability, copyright infringement, and other areas of potential loss related to technology. Companies often found that their losses in these areas were not being covered by their existing business insurance, and the courts passed conflicting judgments on where cyber-related liability resides. Insurers usually responded by narrowing the terms of ordinary liability and property insurance, and sometimes offered a new product that covered these nascent cyber issues.

Comparable Markets: Other insurance products illustrate how new risks, or perceptions of risks and responsibilities, can change markets. For example, when legal liability for environmental harm first arose, insurers fought coverage because the risk had not been calculated and premiums had not been collected to cover the loss. After the initial shock, insurers began to offer environmental risk insurance, which evolved from a small niche offering in the 1960s to an accepted facet of business risk to be covered today. However, this only happened because government statutes and regulation set standards, making loss calculation possible and widening the risk pool to the point that insurance was profitable to offer. At the same time, regulatory standards and associated business reporting requirements provided data and information needed by the industry to model and appreciate risks and to develop appropriate environmental liability products. In the field of property insurance, the idea that a building can and should be insured against a range of risks has become so commonplace that building codes now parallel the standards for insurability. Such is the potential with cyber liability.

Around 2003, carriers began to expunge the dot-com "internet language" from policies and, driven largely by major events/litigation[1] and new state privacy laws, issued approximately $350 million in total cyber liability coverage by late 2005. While the market has grown in dollar volume over the last decade, cyber liability insurance remains a very small and unsustainable slice of the industry's portfolio. Several impediments to growth of the market – and thus higher levels of cyber protection – were identified and discussed:

- In many larger companies, cybersecurity issues have not emerged "from the server room into the board room." (i.e. Business continuity and risk managers are not aware of the need to buy cyber insurance, and IT managers all think that their own security is adequate. Nonetheless, companies have lost millions of dollars in data losses and other cyber liabilities.)
- Corporate accountability for cyber liability has been unclear, and in smaller firms "O-Level" structures (chief security officer, chief risk officer, chief information officer, *et al*) often do not exist. Such small business can store large amounts of data (e.g. patient information, individually identifiable customer data, etc.), yet do not know that they thus have a cyber-liability or how to minimize it.
- Consensus on what constitutes "best cyber practices" is fragmented across industries.
- Lack of demand for cyber liability products also is inhibited by lack of a comprehensive body of cybersecurity standards.
- The nature of cyber threats and thus risk evolves at an extremely high velocity.

[1] *E.g.*, Ingram Micro, AOL v. St. Paul, Seagate v. St. Paul, Choicepoint, and TJ Max.x. "Nutshell" summaries on these cases are provided as a supplement to this document.

Cybersecurity Metrics

Issues associated with cyber metrics were raised frequently and throughout this workshop. A facilitator read a quote from a transcript of a previous CIP Program event that neatly framed the metrics issue:

Issues of homeland security are of critical importance, but concerns should not be exclusive to government agencies and entities. Like first responders, when bad things happen people immediately look to the government or the insurance/reinsurance industry to maintain or preserve liquidity. The private sector has a critically important role to play in emergency preparedness and in ensuring that our national infrastructure is as secure as possible. The government has data, the scope of which is difficult to imagine. If we could develop a way to work with the government to mine [that data] effectively, we can build even more sophisticated models that will help to provide insurers and reinsurers with additional confidence. [Mr. Harrison Oellrich of Guy Carpenter & Company, 27 September 2006]

Metrics are data and information that, if readily available, would inform the industry, its actual and potential clients, and policymakers about cyber risks. Over time, cyber metrics could form an actuarial body of data that would allow the industry to produce accurate models for, and thus define and price, cyber insurance coverage. This data would facilitate a better understanding of risks, predict behaviors associated with cyber threats, and even construct models of catastrophic "cyber-hurricanes." More importantly, the availability of cyber metrics allows improvement over time to be measured and drives the development of better cybersecurity standards and practices. Workshop participants discussed the following questions:

- What kinds of data are needed?
- Is the data being collected?
- If so, what entities are collecting the data and are there restrictions on industry access to the data?

Though workshop attendees did not pinpoint specific answers to these data questions, anecdotes discussed during the workshop strongly suggest that data that is "cyber-analogous" to the kinds of "bricks and mortar" actuarial metrics upon which the industry has historically relied and used either is not being collected or currently is not accessible to the industry. Data might be available from cyber devices and networks, but it may be technically difficult or too costly to collect. One participant suggested that the cyber metrics challenges were reminiscent of problems faced by the electric power industry in collecting and providing data that enables modeling and post mortems of large disturbances and outages.[2] One attendee noted that the manufacturers of cybersecurity software and appliances often incorporate automatic-remote threat reporting into their products. It was suggested that the industry might seek partnerships with these manufacturers so that the industry could have conditional, secure access to *aggregated* threat reports. Such information might allow the industry to see the intensity, duration, frequency, location (jurisdiction), nature and resolution of cyberthreats. Such aggregated data also may have uses in modeling.

In addition, for certain types of risks the data does not exist because the relevant event has never occurred; as with terrorism data in general, insurers lack and will continue to lack meaningful data on a large-scale successful terrorist cyberattack. If the industry had better data on non-cataclysmic losses, however, it would be possible to model larger attacks using methods now employed by reinsurers and risk management groups.

[2] The US – Canada Task Force's report on the August 2003 outage that hit the northeastern US and Canada provides an excellent examples of the impediments to obtaining and normalizing disturbance and outage-related data even when it is being collected and maintained by utilities.

Modeling

Professor Kevin McCabe of GMU's Center for the Study of Neuroeconomics ("CSN") and the Mercatus Center made a presentation over lunch during which he suggested a neuroeconomics modeling technique that the industry might consider in lieu of the conventional actuarial data based models. Neuroeconomics is an "experimental study of how emergent mental computations in the brain interact with the emergent computations of institutions to produce legal, political, and economic order."[3] Emilia Siravo from Guy Carpenter stated that combining neuroeconomics with game theory might produce cyber liability models that provide value to insurers and reinsurers given the metrics limitations discussed above. Additional discussion of this topic is provided in the final section of this paper, **Moving Forward**.

Cybersecurity Standards & Professional Certifications

Issues associated with standards and certifications were on the workshop agenda for discussion after lunch, but due to discussion overflow on the luncheon topic, such issues were not thoroughly discussed at the workshop. Cursory mention was made of voluntary and mandatory regimes such as COBIT, COSO, ISO 17799 and 27001, NIST, Section 404 of the Sarbanes – Oxley Act, and others. Two participants suggested that as a next step consideration should be given to the mandatory cybersecurity standards that have been developed by the North American Electric Reliability Corporation (NERC) and which will be approved by the Federal Energy Regulatory Commission (FERC).[4] These cyber standards apply to over 500 entities identified by NERC and FERC as owners-users-operators of the "bulk electric system" and, as such, fall under the scope of new section 215 of the Federal Power Act. A broad spectrum of stakeholders developed the NERC cybersecurity standards by using an American National Standards Institute (ANSI[5]) process. In the Energy Policy Act of 2005 (EPACT-2005), the Congress specifically required the inclusion of cybersecurity standards in the larger body of electric power reliability standards.[6] On the same day the workshop was held, the Federal Energy Regulatory Commission (FERC) published a proposal to adopt eight of the NERC Critical Infrastructure Protection ("CIP") cyber standards and further proposed to direct NERC to make specific modifications to other cyber standards. A couple of workshop participants suggested that while statistically significant data and information flowing from these cyber standards may not be available for some time, the insurance/reinsurance industry may find it useful to engage NERC and its members as part of the industry's effort to develop and expand cyber liability insurance.[7]

Another participant suggested that the industry, in its quest for data and information that would better inform the market and models, may wish to examine the role of recognized professional certifications. For example, the industry could identify professional certifications and certifying organizations that are relevant to a company's development and implementation of robust cybersecurity. If these certified professionals could be linked to specific companies (or industries), case studies and models could be developed that advance cybersecurity's knowledge base. The CIP Program recently completed a review of these and other

[3] http://www.neuroeconomics.net/
[4] For more information, please refer to the FERC Notice of Proposed Rulemaking, *Mandatory Reliability Standards for Critical Infrastructure* Protection. 120 FERC ¶ 61,077, 19 CFR Part 39, Docket No. RM06-22-000 (20 July 2007),
[5] The following is taken verbatim from the ANSI website (http://www.ansi.org): "The ANSI coordinates development and use of voluntary consensus standards in the United States and represents the needs and views of U.S. stakeholders in standardization forums around the globe. The Institute oversees creation, promulgation and use of thousands of international norms and guidelines that directly impact businesses in nearly every sector: from acoustical devices to construction equipment, from dairy and livestock production to energy distribution, and many more. ANSI is the official U.S. representative to the **International Organization for Standardization (ISO)**."
[6] A summary of the revised cyber standards implementation plan is provided on the NERC website at ftp://www.nerc.com/pub/sys/all_updl/standards/rs/Revised_Implementation_Plan_CIP-002-009.pdf.
[7] If any workshop participant seeks an introduction to NERC cybersecurity experts, please contact Michael Ebert of the CIP Program at (703) 993-2288 or email mebert@gmu.edu.

standards/certifications/risk management issues for a federal agency. We offer to assist workshop attendees with contact information for organizations and selected vendors who set certification requirements and implement training curriculae to those requirements.

Moving Forward

CIP Program Director John McCarthy opened this final section of the workshop by returning to the alternative models theme articulated by Professor McCabe and Emilia Siravo. McCarthy recommended establishing an experimental working group that would employ game theory, neuroeconomics and other concepts to develop a model prototype of cyber insurance markets. Workshop participants who are interested in participating in such a group are asked to call Michael Ebert at the CIP Program, (703) 993-2288 (email mebert@gmu.edu). Experimental models might allow the industry to identify risk categories, market conditions and data needs for different cyber insurance products, thus potentially bypassing the problems identified of unavailable or unusable data. Mr. Leigh Williams of the BITS Financial Services Roundtable and others weighed in favor of further examination and experimentation with "scenario-based game theory models." If nothing else, working through alternative models may help inform a fundamental data question the answer to which remained illusive at the end of the workshop: *Exactly what kind of data are needed to populate cyberliability models that are acceptable to the industry and its clients?*

Mr. Williams and Dr. Kenneth Friedman of the US Department of Energy also suggested that the insurance/reinsurance industry actively seek partnerships with the US Department of Treasury, the National Labs (specifically DOE's Sandia Lab), and to "talk directly with [the US Department of Homeland Security]." Williams and Friedman[8] volunteered to facilitate these partnerships, and McCarthy offered the possibility of using an existing CIP Program contract vehicle with DHS as another possible means to engage the agency and its sector specific critical infrastructure planning elements. Time is of the essence, as the Sector-Specific Plans are slated to be sent to the White House around the first of September.

Michelle Boardman, Assistant Professor of Law at George Mason University School of Law who holds both practitioner and government experience, notably with insurance and contract law, suggested that central to the future of cybersecurity third-party insurance, both for gathering data and modeling, is the ability of insurers to forecast how liability for breaches of security will be assessed under the law. In the absence of clear industry standards or legal/regulatory requirements, courts may find that businesses are not liable in tort because their security systems met a bare minimum of industry practice. Moreover, this uncertainty about the finding and amounts of liability make it difficult for insurers to forecast loss amounts and frequency. The insurance industry, she concludes, should consider leading the way in setting standards for cybersecurity. Leadership could take many forms. Initially, insurers could require certain standards of their policyholders in order to maintain cybersecurity coverage and favorable rates. Professor Boardman recommends that insurers could offer to certify those with coverage who meet these goals and such certification might have value in assuring the public that a business is responsible. Moreover, while the industry is hesitant about seeking particular governmental standards, where standards will inevitably be adopted, the industry should contribute its knowledgeable views to their formation.

Another suggestion made is to examine the "14 FTC consent decrees" as being possible sources for developing a cybersecurity best practices template. Lastly, several participants urged the industry to very carefully consider whether the political, policy and technical environments would support an industry-backed federal legislative initiative to engender a regulatory framework for cyber. Seeking this kind of federal intervention may be premature and/or produce unintended results.

[8] Dr. Friedman may be contacted at (202) 586-0379 or email kenneth.friedman@hq.doe.gov.

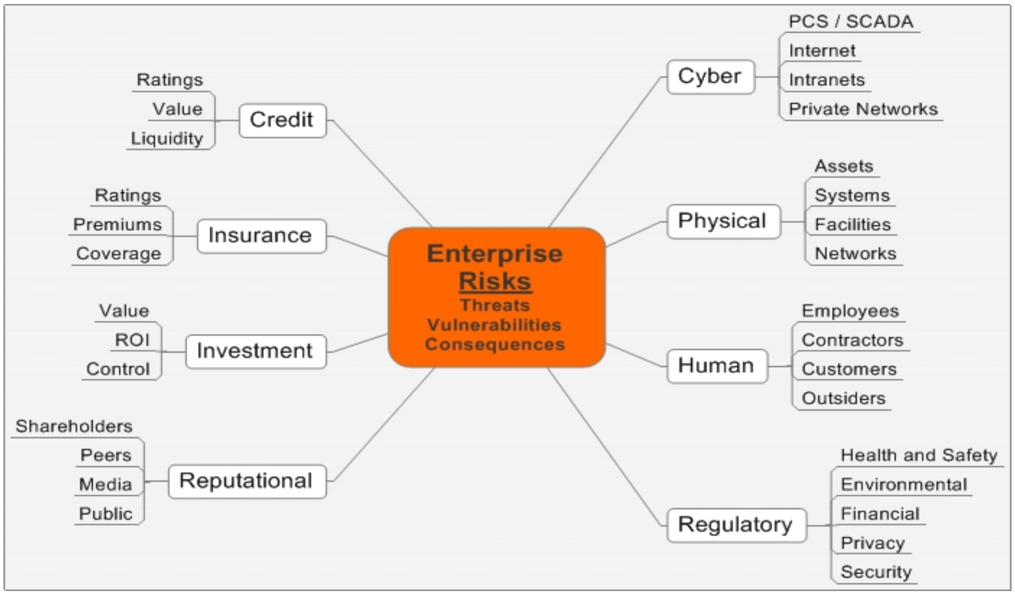
EXHIBIT B: Enterprise Risk Management (ERM) for Critical Infrastructures (ERM – CIP)

1) Defining ERM in the Context of the National Infrastructure Protection Plan (NIPP)

The U.S. Department of Homeland Security (DHS) is specifically charged, among other things, with establishing a common framework among public and private sector stakeholders to address the overall management of risk, and communicate the value of a risk-based approach.[1] The principal framework for public-private sector coordination in matters related to critical infrastructure security is the National Infrastructure Protection Plan (NIPP), which also defines a Risk Management Framework for identification, prioritization, measurement and mitigation of risks.[2]

Indeed, companies in the private sector have been employing various forms of risk management for a number of years to protect their assets and revenue. Businesses routinely face operational (physical, cyber, human) and financial (market, credit, insurance) risks. They are also very susceptible to extreme events. It is estimated that "43 percent of businesses that close following a natural disaster never reopen [and] an additional 29 percent of businesses close down permanently within 2 years of a natural disaster."[3]

The following chart summarizes the types of risks an enterprise in a CI sector typically faces:



There are numerous definitions for both risk management and enterprise risk management (ERM).[4] Synthesizing all of them into one sentence, we suggest the following:

> *"ERM is the systematic application of strategic and operational management policies, procedures and practices aimed at identifying, analyzing, evaluating, treating and monitoring all risks to the business processes of an enterprise."*

[1] U.S. Department of Homeland Security, "Directorate for National Protection and Programs," *U.S. Department of Homeland Security*, 2007, http://www.dhs.gov/xabout/structure/editorial_0794.shtm (cited April 10, 2007).

[2] U.S. Department of Homeland Security, *National Infrastructure Protection Plan,* 105.

[3] *Gulf Coast Back to Business Act 2007*, 110th Congress, 1st Session, S. 537IS.

[4] See Appendix B: Definitions of Risk Management and ERM for a list of quoted risk management and ERM-related definitions.

The ERM approach differs from traditional business risk management and continuity planning in two dimensions:

1. **Holistic Dimension.** ERM promotes a holistic view of the entire company, as opposed to risk affecting only an internal process or a particular division. This view became necessary because of the increasing integration of internal and external business processes through information technology.
2. **Compliance Dimension.** ERM is being used to provide transparency to analysts, auditors, and stakeholders, as well as to support regulatory compliance. This function is a result of legislation to stop financial and accounting breaches that led to corporate collapses.

2) Providing Education and Training in ERM to CI/KR owners and operators

Targeted education and training courses that integrate government-led risk analysis efforts with private sector standards are a prime mechanism to increase the security of physical assets and cyber systems, since large parts of the Nation's critical infrastructure and key resources (CI/KR) are owned and operated by the private sector.[5]

The NIPP itself outlines an educational program that conveys the type of expertise and awareness essential for CI/KR protection, and "recognizes the importance of leveraging existing accredited academic programs, professional certification standards, and technical training programs" to provide individuals with up-to-date risk management knowledge and skills to perform their roles and responsibilities as CI/KR owners and operators.[6]

A very rough estimate of the number of establishments, value, and paid employees in 13 sectors reveals that close to 50% of economic activity in the U.S. takes place in businesses that are part of current CI/KR sector definitions.[7] Clearly, not all of these businesses are indeed critical to national security, economic security, and public health and safety in the sense of the Patriot Act.[8] Also, not every small establishment has a dedicated security function tied into a risk management process. [9] However, even if only 10% of all sector establishments fulfilled those criteria of criticality and size, there would still be a pool of close to a half million potential participants for ERM and related curricula.

3) Improving Qualifications and Certifications to Support the NIPP Process

There is little harmonization in either roles, responsibilities, qualifications, or experience of security managers. Even the overall number of officers in this field is difficult to determine since these positions have no single job classification or particular degree requirement. The Bureau of Labor Statistics, which maintains extensive occupational records by industry sector, counts more than

[5] The common estimate is 85%, even though this number still needs to be substantiated. For example, it is unclear whether this means 85% of infrastructure facilities, or employers, or employees, etc. See Table 1 for a differentiated approach.

[6] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, 80.

[7] In mid-2006, the CIP Program prepared a research brief for DHS entitled "Estimating the Economic and Employment Value of Critical Infrastructure Sectors in the United States," which is available upon request.

[8] Here, the term "critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (Critical Infrastructure Protection Act of 2001, 42 USC 5195c).

[9] Establishments are economic units, such as a farm, a factory, a store or an agency that usually is at a single physical location.

200,000 Computer and Information Systems Managers.[10] Some, but not all of them, may be Chief Information Officers (CIO). A different source estimates the number of CSOs in the U.S. as being close to 27,000.[11]

In terms of security budgets and expenditures, estimates range from $22 to $47 million in companies that have $8 to $10 billion revenue, and 15,000 to 20,000 employees.[12] Other sources contend that enterprises, regardless of size, spend between three to ten percent of revenues on technology, and one to three percent of those technology expenditures on security.[13]

Despite this lack of standardization in roles and responsibilities, there are a number of security-related certifications that are offered by industry associations, vendors, or academic programs. For example, ASIS International (ASIS), formerly known as the American Society for Industrial Security, has created optional certification programs such as Certified Protection Professional (CPP) and Physical Security Professional (PSP). Some have gained quasi-industry standard prominence, in particular the Certified Information Systems Security Professional (CISSP) by the International Information Systems Security Certifications Consortium (ISC2), and the Certified Information Systems Auditor (CISA) by the Information Systems Audit and Control Association (ISACA).[14]

4) Introducing Industry Standards, and Best Practices

Risk Management – AS/NZS 4360

The Australian Standards organization has developed a risk management standard that employs a method of identifying, analyzing, evaluating, treating, monitoring, and communicating risks in order to minimize losses and maximize opportunities for an organization.[15] This standard may be applied at all stages in the life of an activity, function, project, or asset. The documentation is very short and simple, and thus particularly useful for smaller companies.

Information Risk Management – ISO 27002

The International Organization for Standardization (ISO) has developed a code of practice for information security management, which is published as ISO 27002.[16] It is an internationally recognized information security standard consisting of a set of controls representing best practices in information technology.[17] While IT systems-centric, the strength of ISO 27002 is that it is accepted internationally, and sector-independent. This might be of significant appeal to those

[10] SOC code 113021, May 2005. Bureau of Labor Statistics, "Occupational Employment Statistics," *Bureau of Labor Statistics*, 2005, http://data.bls.gov/oes/search.jsp (cited April 10, 2007).

[11] "CSO Audience," *CSO* (May 6, 2002), http://www.csoonline.com/marketing/audience.html.

[12] Ibid.

[13] Packer, Ryon, "Battling for budget: Diverging perspectives," *SC Magazine* (cited March 1, 2003), 1.

[14] Additional professional organizations provide valuable information for ERM and risk professionals, including: Global Association of Risk Professionals (GARP; http://www.garp.com), The Institute of Internal Auditors (IIA; http://www.theiia.org), and The Risk Management Association (RMA; http://www.rmahq.org).

[15] AS/NZS 4360: 2004. *Australian/New Zealand Risk Management*. Standards Australia, 2004.

[16] ISO 17799 was renumbered ISO/IEC 27002:2005 in July 2007. ISO/IEC 27002:2005 has a companion standard, ISO 27001, a specification for information security management systems. Hereafter, both standards are collectively referred to as "ISO 27002." ISO/IEC 27002:2005 (E). *Information Technology-Security Techniques-Code of Practice for Information Security* Management. International Standards Organization, Geneva, 2005.

[17] ISO standards are voluntary. As a non-governmental organization, ISO has no legal authority to enforce their implementation. However, some standards have been adopted in member countries as part of their regulatory framework (mainly consumer safety standards), and others have become a market requirement (such as ISO 9000 quality management systems. ISO 9000:2000. *Quality Management Systems – Fundamentals and Vocabulary* . International Standards Organization, Geneva, 2000.)

CI/KR owners and operators that have establishments in the United States and overseas. The standard addresses the following areas of information security management:[18]

- Security policy;
- Asset management;
- Human resources security;
- Physical and environmental security;
- Information systems acquisition, development and maintenance;
- Access control;
- Organization of information security
- Information security incident management;
- Business continuity management;
- Communications and operations management;
- Compliance

Included in the standard documentation are business impact analysis, disaster recovery, business continuity, internal audit review procedures, and detailed checklists that allow for the establishment of metrics and benchmarks, thus facilitating longitudinal assessments of compliance and progress. Organizations can choose to go through an ISO certification process, which means third party evaluators review the organization's business processes. Overall, ISO 17002 can be used to determine and improve upon a company's information security posture.

Financial Risk Management – SOX

The Public Company Accounting Reform and Investor Protection Act of 2002, commonly known as the Sarbanes-Oxley Act (SOX), was intended to regain the public trust in corporate governance and financial practices in the wake of corporate scandals.[19] The Act is arranged into 11 titles and applies to various topics including:

- Compliance;
- Auditor independence;
- Corporate governance; and
- Enhanced financial disclosure.

The aim of SOX is to, among other things, "enhance corporate governance through measures that will strengthen internal check and balances."[20] To reach that end, the Act and subsequent regulations require continued reporting and, ultimately, continuous oversight of all company operations. Since all of this is enabled through information technology, SOX has become as much a guideline for IT systems as it is for auditing systems. Corporate security executives have started to redesign their asset, system, and network security to meet the requirements of SOX by:

- Assessing the current state of the IT control environment;
- Designing controls necessary to meet the requirements of Sarbanes-Oxley;
- Developing an approach for testing and sustaining controls into the future;
- Identifying exceptions and related remediation plans and adding; and
- Compensating controls for exceptions identified.[21]

[18] ISO/IEC 27002:2005 (E). *Information Technology-Security Techniques-Code of Practice for Information Security Management.* International Standards Organization, Geneva, 2005.

[19] Sarbanes-Oxley Act of 2002. HR 3763, 107th Congress, 2d Session (July 30, 2002) PL 107-204; 116 Stat 745.

[20] *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition*, IT Governance Institute, 2006.

[21] Ibid.

Due to the size of and complexity of the reports required under SOX, a great deal of information about the internal operations of a company are continuously gathered and analyzed. Compliance with the Act thus lays a foundation for implementing enterprise risk management capabilities that did not previously exist for many companies; an organization cannot manage its risk when it suppresses information about business realities.[22]

5) Defining the Role of DHS

Measurable risk management improvements for critical infrastructure sectors, as laid out in the NIPP, require effective ERM practices on the enterprise level. Industry standards, metrics, and best practices, such as SOX and ISO, are promoted through professional certifications, such as the CISSP and CPP, and through academic degree programs.

A DHS-sponsored curriculum that contains elements from existing education and training programs used by the private sector has two advantages:

1. It allows DHS to integrate methods and metrics laid out in planning documents with private sector enterprise risk management approaches, including assessments costs and benefits of security investments.
2. It will attract private sector participants who may use the instruction provided as continuing education leading to certification of their security personnel.

As a result, the participants in the courses will have a better understanding of the DHS risk framework and metrics requirements, and will be able to select and implement one or more enterprise risk management processes that are geared towards increasing their asset and system security consistent with the national protection framework.

6) Integration

Within DHS, a number of initiatives have been developed to assist in establishing baseline knowledge of sector security postures, evaluating ongoing CI/KR protection activities, and making informed decisions about future CI/KR protection activities, such as a Metrics and Reporting Program (NIPP Metric Collection Program or NIPP Metrics Survey).

Ideally, sector-level metrics would be aligned with standard data already gathered by individual companies in the course of their enterprise risk management process. Provided on a voluntary basis, and aggregated through the sector coordinating mechanisms, they would contribute to a better understanding of the state of security in critical infrastructures. Appendix D (Metrics for IT Security) contains a list of metrics that are used in the context of ERM. Further research is required to a) identify what companies use which of these metrics, and over what period of time, and b) develop categories, filters, and algorithms to match up the individual company metrics with the sector-level categories.

[22] James DeLoach, "Building Enterprise Risk Management on the Foundation Laid by Sarbanes-Oxley," *KnowledgeLeader"* (August 25, 2003), available at: http://www.knowledgeleader.com/KnowledgeLeader/Content.nsf/Web+Content/Sarbanes-OxleyActBuildingEnterpriseRiskManagement!OpenDocument (cited April 26, 2007).