NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

RISK MANAGEMENT APPROACHES TO PROTECTION

FINAL REPORT AND RECOMMENDATIONS BY THE COUNCIL

October 11, 2005

MARTHA H. MARSH
WORKING GROUP CO-CHAIR
PRESIDENT AND CHIEF EXECUTIVE OFFICER
STANFORD HOSPITAL AND CLINICS

THOMAS E. NOONAN
WORKING GROUP CO-CHAIR
CHAIRMAN, PRESIDENT AND CHIEF EXECUTIVE OFFICER
INTERNET SECURITY SYSTEMS, INC.

I. ACKNOWLEDGEMENTS

Working Group Members:

Martha H. Marsh, President and CEO, Stanford Hospital and Clinics
Thomas E. Noonan, Chairman, President and CEO, Internet Security Systems
Erle A. Nye, Chairman, Emeritus, TXU Corp., NIAC Chairman
John T. Chambers, President and CEO, Cisco Systems, Inc., NIAC Vice Chairman
Alfred R. Berkeley III, Chairman and CEO Pipeline Trading, and former President and Vice Chairman of NASDAQ
Richard K. Davidson, Chairman, President and CEO, Union Pacific Corporation
Chief Rebecca F. Denlinger, Fire Chief Cobb County, Georgia
Martin G. McGuinn, Chairman and CEO, Mellon Financial Corporation

Study Group Members:

Scott Blanchette, Stanford Hospitals and Clinics
Peter Allor, Internet Security Systems, Inc.
William Muston, TXU Corp.
Kenneth Watson, Cisco Systems, Inc.
Bill Aimetti, Depository Trust and Clearing Corp. (DTCC)
Rick Holmes, Union Pacific Corp.
Stuart Shannonhouse, Cobb County Georgia
Susan Vismor, Mellon Financial
Adam Golodner, Cisco Systems, Inc.
Charles Le Grand, CHL Global Associates
Lawrence A. Gordon, University of Maryland
M. Eric Johnson, Dartmouth College
Stanley Johnson, North American Electric Reliability Council (NERC)
Alexandra R. Lajoux, National Association of Corporate Directors (NACD)
E.W. Stowe, Potomac Electric Power Company (PEPCO)

Department of Homeland Security (DHS) Resources:

Infrastructure Partnerships Division
Nancy J. Wong
Jenny Menna
Keri Nusbaum
Gail Kaufman

Risk Management Division
William Flynn
Lawrence M. Stanton
Susan I. Smith

II. EXECUTIVE SUMMARY

Corporate America quantifies risks based on mathematical statistics, and for lesser known events, on probabilistic modeling. As both producers and consumers of abundant risk management data, corporations excel at analyzing the effects of threats and vulnerabilities that have been previously observed and for which abundant and well-controlled data is available. This private sector experience and expertise could be of use to the Federal government as it meets the current challenge of capturing an abundance of data across a nearly endless spectrum of plausible risks, and then assessing and managing that data in a timely and efficient manner.

Compounding this challenge is an emerging, new Federal infrastructure tasked to support risk management on a national scale, the implementation of which is not yet complete. Today, many corporations possess governance and operating infrastructures that ensure the risk management mission is instituted, facilitates enterprise-wide risk management standards and practices, and provides communication channels to decision makers. Many factors contribute to this corporate advantage, including the comparably limited nature of the risk management challenge (when compared to the Federal challenge). Private sector corporations also possess a substantial base of technologies, people, and methods that have evolved over many decades, coupled with a need for effective risk management to guarantee corporate survivability.

This report will delineate three key findings, the first of which are the practices of risk quantification and modeling. Today, a substantial number of risk quantification models and methods exist. The National Infrastructure Advisory Council (NIAC) focused on the models and methods that present the most applicability to critical infrastructure protection.

The second focus of this report is risk tolerance and risk acceptance. There is very little utility in developing mature, complex national risk management models and the supporting infrastructure without a clear understanding of the nation's tolerance for risk. The Council does not intend to advise the government on risk tolerance that is a national policy question. This report does however, identify a need for a national discussion on risk acceptance and risk tolerance. Such a discussion is critical for the implementation of all subsequent recommendations provided in the report. Finally, the Council conducted and documented an analysis of effective and ineffective risk management attributes. Different than the methods discussed previously, these attributes are consistent across many methods, problem statements, and industries. These attributes, while independent of a specific method, are potentially useful tools when building a national risk management capability.

Background on Risk Management Working Group

The NIAC, through the Department of Homeland Security (DHS), provides the President through the Secretary of Homeland Security with advice on the security of the critical infrastructure sectors and their information systems. These critical infrastructures support vital sectors of the economy, including banking and finance, transportation, energy, manufacturing, and emergency government services, among others.[1]

The NIAC convened the Risk Management Working Group (RMWG), at the request of the President, to investigate public and private sector risk management best practices and solutions for use in national critical infrastructure protection.

Pursuant to Homeland Security Presidential Directive (HSPD)-7, the National Infrastructure Protection Plan (NIPP) describes a comprehensive, integrated Federal plan for critical infrastructure and key resources (CI/KR) protection. The NIPP also designates specific Federal departments and agencies as sector-specific agencies responsible for protection activities in 17 critical infrastructure and key resource sectors[2]

The NIAC is charged with:

- Enhancing cooperation between the public and private sectors in protecting information systems supporting critical infrastructures in key economic sectors and providing reports on the issue to the President, as appropriate;
- Enhancing cooperation between the public and private sectors in protecting critical infrastructure assets in other key economic sectors and providing reports on these issues to the President, as appropriate; and,
- Proposing and developing ways to encourage private industry to perform periodic risk assessments of critical information and telecommunications systems.

The NIAC also advises federal government lead agencies and that have critical infrastructure responsibilities and industry sector coordinating mechanisms.[3]

Approach

The RMWG was asked by the Council to investigate whether private sector experience with risk prioritization and management could provide meaningful guidance to the President on government programs and planning for critical infrastructure protection. The investigation considered magnitude and duration of consequences of risk, impact of consequences, and risk acceptance. The study also assessed event experience, specifically high-profile risk management failures over the past two decades.

Accordingly, the Working Group initiated efforts to:

- Aggregate and assess existing public and private sector risk management methodologies, practices, and decision models.
- Identify risk management commonalities and differences at both the strategic and operational levels.

---

[1] Charter of the National Infrastructure Advisory Council (NIAC), Department of Homeland Security, July 1, 2005; http://www.dhs.gov/interweb/assetlibrary/NIAC_Charter.pdf

[2] HSPD-7 outlines 17 critical infrastructures/key resources.

[3] Charter of the NIAC

- Identify trends in private sector risk management maturity; and benchmark these trends against public sector risk management.
- Make recommendations of value on behalf of the NIAC that will improve national risk management efforts.

The Working Group created a Study Group to assist with the research. The Study Group investigated risk management across all industries available to the NIAC, which included finance, information technology, electric power, and health. At the request of the Working Group, the Study Group engaged private sector representatives with experience in key areas of risk management including information technology, physical infrastructure, financial services, and commodities. A variety of interested parties was also asked to assist, including:

- Academia (Stanford University, Dartmouth College, University of Maryland)
- Industry associations (National Association of Corporate Directors, North American Electric Reliability Council, Institute of Internal Auditors, Information Sharing and Analysis Centers, Partnership for Critical Infrastructure Security)
- Government agencies (Department of Homeland Security; Department of Defense, Defense Contract Management Agency; Cobb County, Georgia).

The Study Group conducted interviews, captured feedback, and developed a document library with contributions across sectors. Input from associations, academia, government, and industry were considered. Academia provided substantial contributions on technical aspects such as risk quantification.

For the purpose of this report, the Working Group defines risk management as:

- A systematic, analytical process to determine the likelihood that a threat or vulnerability will harm an asset or resource and then identify actions that reduce the risk and mitigate the consequences of the event.

Risk management principles assume that while risk generally cannot be eliminated, enhancing protection from known or potential threats can reduce it. Historically, the most effective forms of risk management are predicated upon the manipulation of significant, actuarial data. Multiple forward-looking risk management projections and/or analysis methods are currently available and some of these methods yield highly accurate results.

III. FINDINGS

The Working Group identified three high-level findings:

Finding #1:

Robust standardized risk management methodologies, supported by advanced technologies and infrastructure, maximize the effectiveness of risk management programs.

- **Methodologies:** Investments in risk management methodologies, including interdependency management, improves standardization of reporting and enhances effectiveness of data being used for risk management.
- **Technologies:** Investments in risk assessment, modeling, aggregation, analysis, management, and reporting technologies improves risk management outcomes.
- **Infrastructure:** Investments in infrastructure that improves the aggregation, analysis, dissemination, reporting, or communication of usable risk information maximizes outcomes.

Finding #2:

Risk management leadership, accompanied by the implementation of a risk management culture and a supporting organizational structure enables the standardization of methods, allocation of adequate risk management resources, and enhancement of risk management program effectiveness.

- **Leadership:** Organizations known for highly effective risk management identify and empower risk management at senior leadership levels.
- **Culture:** Organizations that face risk frequently and develop effective risk management cultures align employee and management incentives with risk mitigation, value risk management as a core organizational competency, and ensure strong risk oversight.
- **Structure:** Organizations with significant risk management challenges develop and implement a structure that promotes standardization, disseminates methods, and provides necessary sustainment through supporting training and education programs.

Finding #3:

Independent oversight of risk management approaches enhances strategic direction, focus, and accountability.

- **Strategic direction:** Independent input about risk management, at the Board of Directors level, enhances the robustness of the risk management program and yields fully-vetted, prioritized risk management activities.

- **Focus:** Establishing risk management as a core competency of organizational leadership at the senior-most level ensures enterprise-wide focus on risk management programs.
- **Accountability:** Independent input and accountability on key risk management functions and decisions yields the appropriate level of attention, priority, and outcomes.

IV. RISK MANAGEMENT APPROACHES

Risk Quantification and Risk Management Models

Risk analysis data is generally available in three forms: statistics, models, and expert opinions.[4] The most complete, accurate and commonly preferred data are those available through statistics. Statistics provide a controlled baseline of data points that can be manipulated to conform to both retrospective and forward-looking risk management models.

With the challenge of Federal risk management, there is a potential gap between availability and usability of risk management data. Risk modeling is one mechanism available to compensate for this gap. In the absence of usable standards-based information, forward-looking, quantitative risk analysis is possible using any number of methods, including: Probabilistic Risk Analysis, Boolean logic, and Bayesian or Stochastic modeling. These methods, detailed later in this section, serve as a means to a quantitative end. Although they rely on assumptions that may alter the output of the assessment, they provide a tangible, quantifiable indication of risk.

Quantitative risk analysis provides an understanding of threats and vulnerabilities along with their corresponding impacts. Magnitude of consequence should only be a component of the overall risk equation. Stanford University Professor Dr. Elisabeth Paté-Cornell suggested:

> Distribution effects (who enjoys the benefits and who is subjected to the hazard), and the fact that some risks are uncontrollable, involuntary, new or unknown, must also be given attention. Therefore, the strict order of risk magnitudes does not – and should not – rule priorities in risk management to the exclusion of all other factors. Yet, quantification may help focus the debate on the relative importance of different risks and on the contribution factors to a particular risk. This is especially important when misperceptions of threats and priorities are shaped by unfounded fears or by the opinions of experts with strong positions at stake. Fear is a great motivator and an essential safeguard of mankind, as well as one of its weaknesses. Therefore, quantifying the different risks and debating the

[4] A significant component of this section of the document is derived from Stanford University Professor Dr. Elisabeth Paté-Cornell. Specifically, her study, "Greed and Ignorance: Motivations and Illustrations of the Quantification of Major Risks" in "Science for Survival and Sustainable Development" Pontificiae Academiae Scientarum Scripta Varia 98 (231-270); Proceedings of the Study Week of The Pontifical Academy of Sciences, The Vatican, 12-16 March 1999 and its complimentary body of knowledge is considered one of the most complete collections on risk analysis and risk management available.

> results may help clarify the issues, and either deflate an overblown threat or bring to light an underestimated hazard."[5]

The risk quantification process and development of finite risk management models should be considered a tool in the complete risk management life-cycle. There are substantial undertakings required to complete this life-cycle, including development and implementation of a governance and oversight process, establishment of risk data collections, analysis and dissemination mediums, hedge strategies (e.g. insurance), and other components that represent a fully matured risk management capability. However, the establishment of a quantitative risk management capability is a valuable, and necessary, starting point for national risk management endeavors.

Historically, national security and its accompanying infrastructure protection decisions were based on a largely static set of threat and vulnerability assumptions. Those static, bi-polar risk assessment assumptions do not apply to today's environment. Today's landscape, compared to decades past, has an exceptionally high likelihood of an event that would negatively impact the U.S. critical infrastructure, while the magnitude or gross consequence of such an event is likely to be significantly lower. For example, the probability of an adverse event occurring today on U.S. soil is comparably high to the threat of nuclear war during the Cold War. However, the magnitude of that threat, when compared to global nuclear catastrophe, is conversely lower. Compounding the changing nature of the threat landscape is the lack of tangible, reliable, or credible data upon which to build a defensible risk management model on a national level. This fundamental shift in the threat picture facing the nation today suggests there is much work to do to bring our risk management methods and philosophies into a more contemporary state.

Probabilistic Risk Analysis

In the absence of complete and accurate data, there are mechanisms available that will allow the U.S. to develop sound forward-looking risk management models. These models have been used, oftentimes with startling accuracy, to identify future risks well in advance of their materialization. Probabilistic risk analysis (PRA) is one such example that would allow U.S. critical infrastructure protection planners to identify potential threats and vulnerabilities. PRA relies on the use of Bayesian inference, allowing risk managers to project risk probabilities and assess potential impacts without heavily populated data stores from which to work.

Today risk managers must transform themselves into an operating mindset that allocates or commits our limited infrastructure protection resources, often with incomplete or imperfect information. This need runs counter to a basic human tendency that predisposes risk managers to indecision or inaction until all relevant information becomes available. This tendency must be overcome for critical infrastructure risk managers to be successful in the future. Probabilistic risk assessments analyze system function, failure mechanisms or modes by inputting this data into a systems probability failure formula. Through this process, management is capable of identifying not only technical weaknesses that yield

[5] Ibid.

risk, but also human, systematic, or organizational failures that yield risk. As was the case in the 1986 Challenger space shuttle disaster (see Appendix C), these human risks, often, may be managed at a much lower cost than technical risks. At the same time, addressing these human factors may reduce overall systematic risks more comprehensively than a technical solution.

Bayesian and Stochastic Risk Modeling

Warning systems are some of the most effective ways to mitigate large-scale risks, and probabilistic methods similar to those discussed above can be used to maximize their efficiency. However, these systems are seldom perfect because they can both issue false alarms and miss event signals. One weakness may be the "false-positive" effect, in which people cease to respond after too many false alerts. On the other hand, either because a system is not sensitive enough or because it involves a chain of components in which transmissions failures may occur, it can fail to issue a timely warning.[6]

Optimal assessment of data points and subsequent translation into alerting mechanisms cannot be managed in an ad hoc manner. There are multiple decision criteria required to identify what assets are of priority, what time constraints affect decision making, and what the risk spectrum is (a function of risk tolerance), before determining the appropriate response.

Stochastic modeling and analysis is a mechanism that can optimize warning systems and transition them into a state of functional utility over time. Bayesian reasoning allows a computation of overall risk, and is based on the probability of an event occurrence. The Bayesian approach was used in the past to calculate the probability of a nuclear attack on the U.S. based on signals from our command and control system. This type of system typically includes both false alerts (false-positives) and missed alerts (errors of omission). Another limitation of this approach is that probability could vary according to fundamental assumptions made by experts, for example, those regarding possible procedures and timing of attacks. The probability of an event then would depend upon which hypothesis was correct. Bayesian reasoning provides the decision maker with a full representation of the state of information – including the uncertainties about the probability of attack – after reading a positive signal from the command and control system.[7]

Financial Risk Management

One of the most commonly cited frameworks for assessing financial risk in the private sector is the COSO framework. COSO, developed by the Committee of Sponsoring Organizations, derived from the findings of the 1987 National Commission on Fraudulent Financial Reporting. This presidential commission, (commonly referred to as the Treadway Commission), initially addressed the implications of corporate fraud risk

[6] Ibid.
[7] Ibid.

management, but over 20 years has expanded its work into the broad arena of enterprise risk management.

The COSO framework for analyzing enterprise risk includes three components. The first component is the risk assessment. This assessment is both qualitative and quantitative in nature, includes specific time and objective horizons, and differentiates between inherent and residual risk. The second component of the COSO framework is the risk response mechanism. This response mechanism includes interdependencies, such as an organization's tolerance for risk, and allocates response resources based on defined cost and benefit metrics. Finally, COSO includes governance and control infrastructures to ensure the methodology is adopted across an enterprise, consistently governed with consistent data points, and included in both processes and technologies.

Limitations of Risk Quantification and Risk Management Models

There are numerous risk management methods and models available in the private sector. Understanding all of the knowledge available and identifying which methods are most applicable to the infrastructure protection mission would require a significant investment of time and resources.

Vulnerability and probability of failure is inherent in any theory. These risk analysis methods possess limitations that deserve comment from the Working Group. A representative sample of these limitations include:

- **Subjectivity and falsification:** experts can interpret differently the implications of the same evidence for the probability of an event.
- **Completeness:** it is often impossible to ensure that the set of hypotheses considered at any given time is complete, i.e., the available evidence could not support other possibilities or scenarios.
- **Insufficient data and problem structuring:** sufficient data may not be available to satisfy the decision makers.
- **Vulnerabilities of results and opportunities for manipulations:** the results are sensitive to stated or unstated assumptions and can be manipulated by interested parties.
- **Opportunities for false analogous results:** calculation of risk and interpretations of threats and vulnerabilities may produce false parallels. Seemingly similar environments may include fundamentally different risk factors that will produce differing outcomes.[8]

Beyond the discussion of methods is the difficult and more complex national policy consideration of risk tolerance, also known as risk acceptance. This debate is often colored by personal or group preferences, bias, perceptions of priority and importance, and great discrepancies on perceived magnitude or duration of consequence. Because the risk management tools identified in this report are subject to the outcome of qualitative risk acceptance decisions, a risk acceptance policy determination is paramount to

[8] Ibid.

successful implementation of a risk management system for critical infrastructure protection.

Risk Tolerance

The public and private sectors differ not only in approach to risk management, but also in tolerance for risk. The drivers behind risk management are an example of these differences. The private sector has incentives to proactively assume risk in order to meet growth objectives, capture new markets, services, or technologies, and to remain competitive. Public sector decision makers often weigh risks from a general welfare perspective, instead considering the well-being of society. Thus, the focus in the public sector is fundamentally on managing existing or inherent risk rather than seeking risk that may yield higher returns.

Firms in the private sector are also concerned with managing risk for the firm as a whole, referred to as enterprise risk management (ERM). ERM allows a corporation to understand its risk profile in a comprehensive and quantitative manner. Quantitative measurement of risk with specific risk metrics is usually associated with an expected loss (probability) and the uncertainty (variance) of the expected loss.[9] Private sector enterprise risk management allows organizations to identify and manage all risk. This risk may be small, ordinary, easily predicted, and affordable to hedge, or large, extraordinary, difficult to predict, and expensive to insure. Another private sector advantage is the role government plays as a guarantor for private sector activities, which further complements corporate risk management.[10]

The public sector risk management challenge is unique. When compared to the relatively well-defined and well-understood spectrum of corporate risks, the national risk management challenge is near-limitless. This necessitates discussion of risk tolerance and risk acceptance. Because these risks are involuntary to individuals, despite being inherent to the system as a whole, there will be scenarios where the government will be forced to accept risk for the good of the nation, but to the detriment of individual citizens.

Also, people who incur the costs may not enjoy the benefits of a decision. For example, those who live downstream from a dam are exposed to the risk of its failure, whereas the larger population as a whole enjoys the benefit of the electricity generated. The effects of risk-benefit tradeoffs are not only unevenly perceived but also unevenly felt.[11]

Unfortunately, there is no universal risk acceptability metric. The lack of a universal or even generally agreed upon risk acceptability metric, again, suggests the need for a national-level risk acceptance discussion. Despite the difficulty involved, the country

[9] For a more detailed discussion concerning risk management as a process versus quantitative risk metrics, the reader is referred to in Chapter 5 of Managing Cybersecurity Resources: A Cost-Benefit Perspective, by Lawrence A. Gordon and Martin P. Loeb, McGraw-Hill, Inc., 2005.

[10] Note the existence of organizations such as the Oak Ridge National Library, which has done quality work in radiation safety. For a study on government as the backup for the private sector, see: Best Practices for Government Intervention to Enhance the Security of National Critical Infrastructures – Report from the NIAC (2004) at: www.dhs.gov/niac under Final reports and Recommendations and Library of Congress.

[11] Paté-Cornell, Ibid.

would be well-served by this dialogue because the outcome would significantly strengthen risk assessment and management models. Without risk acceptance data points, the utility of any national risk management system would be significantly diminished.

Attributes of Effective Risk Management

To further understand risk assessment and risk management, the Working Group conducted an analysis both of effective and ineffective risk management episodes. When base-lined, these episodes yielded a core set of attributes common to each case studied (see Appendix C). Different than the methods discussed in previous sections, these attributes are consistent across many methods, problem statements, and industries. These attributes, while method-agnostic, are potentially useful tools when building a national risk management capability. Risk Management effectiveness can be depicted across a continuum from immature to mature. Mature risk management, or those methods that have become more effective over time, are substantially more successful than immature risk management. Immature risk management processes tend to possess a common set of weaknesses including:

- Insufficient collection of actuarial or historical data points for decision making.
- Ineffective use of data: no conversion to actionable information.
- Lack of prioritization and lack of proximity between actuaries, indicators, and decision makers.
- Limited belief that markets value investments in risk management.
- Low recognition/experience of legal precedents compelling risk management standardization (no basis for qualitative risk analysis).
- Immature understanding of failure mechanisms and failure indicators.
- Institutional or organizational failures (due to lack of clarity in risk management decision making roles and responsibilities); low awareness of risk in the organization; decentralized structure for most critical functions.
- Misalignment of incentive factors (team or individual).
- Vulnerability to error from human factors (both technical and procedural).
- Insufficient insurance against critical risks.
- No business case made for investments in risk management.

Conversely, mature (or effective) risk management methods tend to possess a common set of positive attributes. These attributes include:

- Highly actuarialized data with a mature understanding of failure mechanisms and failure indicators.
- Effective use of data; conversion to actionable information.
- Effective prioritization; close proximity between actuaries, indicators, and decision makers.
- Recognition that free market forces demand effective risk management.
- Recognition/experience of legal precedents compelling risk management standardization (which provides a foundation for the qualitative nature of risk management).
- Mature understanding of failure mechanisms and failure indicators.

- Risk management culture across all levels of organization (including the board of directors); single point of accountability for risk management (e.g. chief risk officer).
- Alignment of incentive factors (team and individual).
- Training to lessen human error (technical or procedural).
- Insurance mechanisms to improve risk tolerance; breadth of risk management coverage, including physical and cyber security, to maintain productivity.
- Strong business case made for investments in risk management.

Across all industries and within all critical infrastructures, one sees examples of immature and mature risk management. Public sector risk management efforts likewise possess many attributes of both mature and immature risk management models. For example, the Department of Homeland Security is investing resources to build a standardized, enterprise-wide risk management program. This program includes many of the attributes of a mature system, including the incorporation of highly actuarialized data points, a mechanism to convert data into actionable information, a supporting infrastructure to provide information to risk managers in a timely manner, and a constantly improving understanding of failure mechanisms and indicators. Included in the attribute lists above are a number of areas in which corporate America is particularly strong. These include the role of risk oversight by the Board of Directors, the role of insurance, and the business case for risk management investments. The following sections address these attributes in more detail and identify their utility in the risk management life-cycle.

Role of Risk Oversight by Boards of Directors

In the private sector, most corporations are managed under the direction of boards of directors. Boards are compelled to oversee risk management. Directors understand the risks facing the organizations they serve, and ensure there is a process to proactively identify and address risk. Directors expect management to identify the principal, material risks the company faces, indicate the likelihood that they will occur, and assess costs of management against the potential impact. The board ensures that management establishes risk management practices, and continually reevaluates those practices and the board's own role in overseeing them. Directors are responsible, now both criminally and civilly, for the effective execution of the risk management mission.

Taking direction from both the Public Company Auditing Oversight Board (PCAOB) and the Sarbanes-Oxley Act, directors are required to prioritize risks and ensure processes are in place to comply fully with relevant laws and regulations. Accordingly, directors and management outline corporate plans, not only for addressing risks, but also for mitigating their impact. Directors are sensitive to specific risks and take into consideration the impact that they might have on different groups of stakeholders, such as employees, customers, suppliers, and local community groups. The board works with management

to set up plans that enable continued board oversight and enable corporate leaders to continue to manage during both daily operations and during a crisis.[12]

Role of Insurance

Insurance plays a vital risk management role in the private sector. Tangible and intangible assets, as well as human safety and lives, may be insured against a variety of perils, ranging from human malfeasance to accidents, catastrophes, and acts of nature. Insurance serves as a hedge against risk, both inherent and introduced. This hedge allows private sector entities to continue to accept more risk as part of a growth or operations strategy, while limiting the negative impact of risk factors. For the corporation, insurance plays a central and critical role.

For those organizations that cannot obtain or afford insurance to cover certain risks, companies set aside money to self-insure. They do this as individual companies, or in some cases, as industry groups. The insurance industry insures itself through "reinsurance," or insurance for insurers. Groups of companies establish funds that provide for contributors to respond to claims that come from catastrophic losses. This insurance infrastructure ensures that corporations remain competitive and have sufficient mechanisms available to help hedge risk. Self-insurance or reinsurance are two mechanisms worth considering within the national risk management framework. While it is extremely unlikely there will be opportunities for the Federal government to seek outside insurance, opportunities for self-insurance or reinsurance do exist.

Insurance coverage for a particular risk can range from non-existent to limited coverage to full coverage as insurers learn more about risks and/or as risks diminish. Five years ago, it was difficult to purchase coverage for cyber security threats. The threats were too rare and catastrophic; not enough was known about how to predict such risks, and more important, there was little understanding or agreement about prevention mechanisms. Today, cyber insurance is an increasingly important and common mechanism for risk management in the private sector.[13]

[12] The citations are from Julia Allen, "Governing for Enterprise Security (CMU/SEI-2005-TN-023), Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, June 2005. The first quote is from The Institute of Internal Auditors', "Global Technology Audit Guides: Change and Patch Management Controls: Critical for Organizational Success," IIA, June 2005. http://www.theiia.org/index.cfm?doc_id=4706 . The second is from Anthony Tarantino, "The Impact of SOX and Corporate Governance on IT," Executive Update 7 18, Cutter Consortium, September 2004.

[13] For a discussion on how to consider insurance in cyber security, see "A Framework for Using Insurance for Cyber Risk Management," Communications of the ACM, March 2003, by Lawrence A. Gordon, Martin P. Loeb, and Tashfeen Sohail.

V. RECOMMENDATIONS

As part of the recent restructuring of DHS resulting from his Second Stage Review, Secretary Chertoff announced a sharp focus on risk management, driving analysis towards threats, vulnerabilities, and consequences, and then prioritizing risk. This approach is entirely consistent with the needs of the nation and the approaches to infrastructure protection advocated by the NIAC. Like the private sector, government can not protect against all risks, and should focus on those things that hold the greatest risk and would be most costly. Although there are differences between private and public sector risk management methods and priorities, the essential risk management objectives are the same. Both share common concerns about threats, vulnerabilities, and consequences, and the necessity to prioritize risk management efforts.

DHS's stated focus on catastrophic loss is fundamentally correct from the risk management perspective. It is impossible for any organization to cover all risks, and attempting to achieve zero risks bears too high a cost. Therefore, a clear-eyed national focus on the costliest risks is appropriate. The private sector does this in its own way. It sets priorities, makes choices based on data, and manages risk. This renewed focus of DHS to drill down on the exact nature of each threat, develop a better understanding of vulnerabilities, and finitely identify consequences is the right course of action.

Given the scope of the national security challenges facing the country today, the Council is encouraged that DHS is addressing the prioritization of risks, and focusing resources on the greatest threats and consequences. The Council urges the Federal government to continue its focus on risk assessment and management, and also makes five recommendations to support this continued focus. The Council hopes these recommendations, which flow from our findings, can assist the Federal government in undertaking this critical risk management task.

Overall Recommendation: Continue the government's focus on risk management

Leadership and action does not happen in a vacuum -- people make it happen. DHS senior leadership and the Federal agencies must continue to press and drive policy and decision making though sound risk management practices. Federal agencies need standardized methods of assessing and managing risk, educating in risk management practices, and a clear test for policy implementation on this basis.

It necessarily follows from this recommendation that government needs a meaningful national risk management plan, and prioritization. DHS has now started the Strategic Risk Analysis Process referred to as the Risk Analysis and Management for Critical Asset Protection (RAMCAP). This effort, and a number of complementary initiatives, should be driven to conclusion. As many of the threat, vulnerability, and consequence factors consider people, assets, and conditions at the intersection of the public and private sector, DHS should use the new Sector Coordinating Councils to check facts, assumptions, and real world conditions as it builds out this new important risk management structure.

Also, in early January 2005, the House Committee on Appropriations Report mandated that DHS create a Risk Assessment Policy (RAP) Group to align risk assessment policies

and methodologies within the Department. The DHS Science and Technology Directorate's Office for Interoperability and Compatibility (OIC) is spearheading this effort, which includes representation from each of the DHS directorates.[14] While the RAP Group remains in the early stages, the Group intends to base its framework to include threat, vulnerability, and consequences. It also is relying on the General Accountability Office (GAO) Risk Management Framework.[15] However, at the time this report was written, the RAP Group has not indicated plans to incorporate private sector insight into its efforts, which would benefit the final product from this organization.

Specific Recommendations

Recommendation #1: Create and standardize risk management methodologies and mechanisms across the government.

Risk management is a complex topic. The Government expanding of the use of risk management best practices will not be achieved without recalibrations, lessons-learned and continuous improvement. The private sector can provide guidance with this task because of its long experience and deep roots in risk management.

Risk management is a private sector profession. Complementing this career designation are a number of associations, such as the Risk Management Association, and the Fiduciary and Investment Risk Management Association, that aggregate risk management professionals across sectors. The best practices of these groups may well apply to aspects of government-based risk management. Like critical infrastructure protection, and for many of the same attendant reasons, risk management should continue to be viewed as a public-private partnership.

As the importance of risk management becomes ingrained in Government's processes, formalizing this public-private risk management partnership will bring additional benefits. Whether through the Sector Coordinating Councils or a separate Private Sector Risk Management Advisory Council to the Secretary, there are ways in which the public-private sector risk management partnership should be strengthened and expanded.

The private sector benefits from a risk management infrastructure that has evolved over many decades, and continues to mature. This infrastructure includes identified and time-tested methodologies; collection, assessment and analysis technologies and processes; and communications mechanisms that facilitate all of these components. Building this infrastructure required years of continued investment, improvements, standardization, and education. It is clear the development of a similar function, built on a national scale, and addressing a near-limitless set of threats and vulnerabilities, will take a substantial period of continued investment and leadership.

DHS should also continue to expand its ability to identify, acquire, collect, and analyze threat, vulnerability, and consequence data. Some of this data likely exists in public sector resources and a good proportion can be mined from the private sector. DHS should continue to dedicate resources to explore mechanisms that would facilitate incorporation

[14] The House Committee on Appropriations Report 109-79, 117 (January, 2005).
[15] General Accountability Office, "Strategic Budgeting: Risk Management Principles Can Help DHS Allocate Resources to Highest Priorities,"GAO-05-824T (Washington, D.C.: June 29, 2005.

and protection of private sector data in the national risk management equation. There is the potential that government efforts to compel participation would induce resistance and detract from the data collected for risk modeling, assessment and management. Alternatively, active engagement of the private sector as a partner in this effort would likely be welcomed and encourage private sector participation. DHS should also consider other sources of data, including academic institutions and the data which has been used over time to support academic research.

The identification of critical data is only the first step in building a national risk management infrastructure. Housing, manipulation and analysis of this collected data are the key next steps. Identification and implementation of a standardized risk management framework for the execution of risk analysis would be an important part of this approach. Another important part of this framework would be to include the attributes of a mature and effective risk management model identified previously. Again, mature risk management methods and technologies in use today required substantial investments in time and money to bring to fruition.

Finally, recognizing that communication failures are common across many of the cases studied, DHS investments in improved, streamlined communications would be an important consideration. Ensuring sufficient mechanisms to communicate risk assessment and risk management data to decision makers is critical for risk management success.

Recommendation #2: Establish a risk management leadership function within departments, bureaus or agencies

To help drive the risk management structure throughout the government, there needs to be greater focus and accountability at senior levels. Each cabinet-level department should consider a Chief Risk Officer (CRO), in line with the practice at many private sector entities. The CRO would serve as the single, senior focal point for risk management in the agency. The CROs would coordinate the risk assessment and mitigation activities through the organization including physical, cyber, and human. The CROs would also serve as the focal point to educate and communicate the risk posture of the department throughout the organization. Consistent with the public-private sector partnership advocated in Recommendation #1, the CRO should interface with the Sector Coordinating Councils, and have a cross-agency CRO Council, similar to what exists in government for Chief Financial Officers and Inspectors General to exchange best practices, lessons learned, and assist in the growth of this important new function.

The Council also encourages the creation of a CRO within the DHS. This position would serve as the senior focal point for risk assessment and risk management activities on an agency-wide basis, and at the same time, serve as the CRO for the Federal government. It would not be difficult to envision this position as the lead risk official, ensuring the execution of the risk management mission and the distribution and enforcement of risk management standards across the government.

The Council identified a number of ongoing efforts to collect data and assess risk across the critical infrastructure and nation. The RAMCAP initiative within the Risk Management Division (formerly called the Protective Services Division) is one example of a formal risk management methodology currently under development. The RAP Group

has indicated that a CRO should be responsible for overall risk policy and cross-agency integration of the risk assessment framework and would work with designated risk officers responsible for risk policy within each Directorate and office or agency with a risk management mission to coordinate related activities.[16] In addition, the RAND Corporation is providing substantial risk assessment expertise to DHS in the areas of risk modeling and prioritization on a national level. These efforts focus largely on collection and analysis of risk data, but as of yet, have not matured sufficiently to serve as risk management tools. They both appear to be vectoring in the right direction, but time and resources supporting this maturity are the primary barriers to success.

The Council agrees with Secretary Chertoff's focus on risk management and believes his vision is on point. As part of the larger exercise of risk management, DHS should specifically undertake the process of drilling down into threats, vulnerabilities, and consequences for all risks (including nuclear, biological, chemical, physical and cyber), for all 17 critical infrastructure sectors and key resources. A logical extension of this data set would provide exceptional utility in development of a risk management solution. Ultimately, there is significant work to be done around risk acceptance and risk tolerance before a consistent risk management framework can be effectively applied.

Recommendation #3: Establish risk management oversight function

Corporations significantly benefit from risk management oversight provided by boards of directors. The corporate governance structure ensures accountability, promotes standards, and prioritizes risk management resources against threats and vulnerabilities in an effort to mitigate risk. The Federal government would benefit from similar risk management accountability and oversight.

The Establishment of a Risk Management Advisory Council would benchmark risk management activities and advise the government on risk management practices and priorities. This will help to institutionalize the importance of risk management within the government. The Council may benefit from inclusion of ex officio members with demonstrated risk management expertise, representatives from the Federal government with demonstrated risk management expertise, from entities such as the GAO, the Office of Management and Budget, the Council of Economic Advisors, the Department of Defense, and the newly created office of the Director of National Intelligence.

[16] Progress Report on the Department of Homeland Security's Risk Assessment Policy Group, compiled by the U.S. Department of Homeland Security Science and Technology Directorate, October, 2005.

VI. CONCLUSION

The Council identified specific positive Federal government actions underway that indicate significant resources and attention are being applied to the Nation's risk management challenge. Investment in risk management methodologies, recruiting and retention of risk management experts to lead initiatives, and Secretary Chertoff's focus on risk management in future DHS efforts all indicate the Federal government understands the importance and scale of the risk management problem America faces today.

The Council has found there is room for continued investment in nearly all aspects of the risk management life-cycle. These investments should include technologies (e.g. the identification, collection, analysis, and dissemination of information), human resources (e.g. outside advisors or internal CROs), methodologies (e.g. forward-looking or backward-looking risk management models), and education and training. In addition to recognizing that investment is required to build, standardize, disseminate, and fine-tune the nation's critical infrastructure risk management plan, there should also be a general recognition and acceptance that full fruition of this roadmap will take time, resources, and commitment.

In the interim, the Federal government should attempt to incrementally improve the national risk management capabilities in a time-sensitive and cost-effective manner. Similar to the 1986 Challenger disaster report, many of these interim improvements can address the managerial aspects, not the longer-term technical ones (see Appendix C). Going forward, leaders should have greater access to information necessary to make decisions. The Federal government needs a culture that can act on reliable, but impartial data, which will be necessary for the foreseeable future. The infrastructure to support a more complete picture of the nation's risk is many years and investments down the road.

The Federal government's ability to manage critical infrastructure risk will depend heavily on the development, implementation, and distribution of a risk management methodology across organizations. This framework will standardize the collection and analysis of data, contribute to a consistent understanding of risk in its many forms, and serve as the primary tool for resource allocation decisions. These tools, while critical, are not the end state, and do not guarantee success. However, the implementation of these measures will serve as a good starting point for subsequent risk management efforts and are necessary for the U.S. to achieve an enlightened state of risk awareness.

VII. APPENDICES

Appendix A: National Infrastructure Advisory Council Members

Chair: Mr. Erle A. Nye, Chairman Emeritus, TXU Corp.
Vice-Chair: Mr. John T. Chambers, President and Chief Executive Officer, Cisco Systems, Inc.

1. Members

Mr. Craig R. Barrett, Chairman of the Board, Intel Corporation
Mr. Alfred R. Berkeley, III, Chairman and Chief Executive Officer, Pipeline Trading Systems LLC (former Vice-Chairman, NASDAQ)
Mr. George H. Conrades, Executive Chairman, Akamai Technologies Inc.
Mr. Richard K. Davidson, Chairman and Chief Executive Officer, Union Pacific Corporation, (former NIAC Chairman)
Chief Rebecca F. Denlinger, Chief, Cobb County (Georgia) Fire & Emergency Services
Lt. Gen. (ret.) Albert J. Edmonds, Chairman, Edmonds Enterprise Services, Inc.
The Honorable Robert L. Ehrlich, Jr., Governor, State of Maryland
Mr. Gilbert G. Gallegos, retired Chief of Police, City of Albuquerque, New Mexico
Ms. Margaret E. Grayson, President, AEP Government Solutions Group, Executive Vice President, AEP Networks
Mr. Enrique (Rick) Hernandez, Jr., Chairman, President and Chief Executive Officer, Inter-Con Security Systems, Inc.
Commissioner Raymond W. Kelly, Police Commissioner, City of New York, New York Police Department
Ms. Martha H. Marsh, President and Chief Executive Officer, Stanford Hospital and Clinics
Mr. Thomas E. Noonan, Chairman, President and Chief Executive Officer, Internet Security Systems, Inc.
Mr. Gregory A. Peters, Former President and Chief Executive Officer, Internap Network Services Corporation
Mr. Bruce Rohde, Chairman and Chief Executive Officer Emeritus, ConAgra Foods, Inc.
Dr. Linwood H. Rose, President, James Madison University
Mr. John W. Thompson, Chairman and Chief Executive Officer, Symantec Corporation
Marilyn Ware, Chairman Emerita, American Water.

Appendix B: Resources

1. Additional Study Group Resources

Dennis M. McKnight, Defense Contract Management Agency
Elisabeth Paté-Cornell, Stanford University
John S. Tritak, CEO of Good Harbor Consulting, LLC.
Henry H. Willis, RAND Corp.

2. Bibliography Resources

- The 9-11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States, Official Government Edition (Washington, DC: Government Printing Office, 2002).
- 9/11 Commission Report: Reorganization, Transformation, and Information Sharing, Statement of the Honorable David M. Walker: Comptroller General of the United States: GAO-04-1033T 2004)
- Analyzing Critical Infrastructure Dependencies: Security and Survivability Effects in the Service Sectors, NSF 02-029 by Chris T. Hendrickson, James H. Garrett, and H. Scott Matthews, Carnegie Mellon University, 2002.
- Best Practices for Government Intervention to Enhance the Security of National Critical Infrastructures.
- Corporate Information Security Working Group: Report of the Best Practices and Metrics Teams (Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census; Government Reform Committee, U.S. House of Representatives). November 17, 2004 (Revised January 10, 2005).
- COSO Enterprise Risk Management – Integrated Framework, 2004 (www.coso.org).
- Finding and Fixing Systems Weaknesses: Probabilistic Methods and Applications of Engineering Risk Analysis, by Elisabeth Paté-Cornell; Department of Management Science and Engineering, Stanford University; Society for Risk Analysis, 2002.
- A Framework for Using Insurance for Cyber-Risk Management, by Lawrence A. Gordon, Martin P. Loeb, and Tashfeen Sohail, Communications of the ACM, Vol. 46, No. 3.
- Fusion of Intelligence Information: A Bayesian Approach by Elisabeth Paté- Cornell, Department of Management Science and Engineering, Stanford University; Society for Risk Analysis, 2002.
- Probabilistic Modeling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities Among Countermeasures by Elisabeth Paté- Cornell and Seth Guikema. Department of Management and Engineering, Stanford University; Military Operations Research Vol. 7, No. 4, 2002.
- Risk and Uncertainty Analysis in Government Safety Decisions by Elisabeth Paté – Cornell, Department of Management Science and Engineering, Stanford University; Society for Risk Analysis, 2002.
- "Governing for Enterprise Security" (CMU/SEI-2005-TN-023), by Julia Allen. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, June 2005.

- High Risk Series: An Update (Washington, D.C.: Government Accountability Office, Office of the Comptroller General, January 2005).
- Global Technology Audit Guide (GTAG): Information Technology (IT) Controls. Dave Richards, Institute of Internal Auditors (Institute of Internal Auditors, November 2004).
- Information Security Oversight: Essential Board Practices (Washington, D.C.: National Association of Corporate Directors, 2001). Sponsored by KPMG's Audit Committee Institute in collaboration with The Institute of Internal Auditors and the Critical Infrastructure Assurance Office, U.S. Department of Commerce.
- Managing Catastrophic Risks Using Alternative Risk Financing and Insurance Pooling Mechanisms. Finance Sector and Infrastructure Department. Caribbean Country Management Unit. Latin American and Caribbean Region. The World Bank. June 2000.
- Report of the NACD Blue Ribbon Commission on Risk Oversight (Washington, D.C.: National Association of Corporate Directors, 2002.
- The Radiation Safety Information Computational Center (RSICC): Forty Years of Nuclear Knowledge Management, Oak Ridge National Laboratories (www.ornl.gov).
- Report of the NACD Blue Ribbon Commission on Risk Oversight (Washington, D.C.: National Association of Corporate Directors, 2002)
- Report of the Presidential Commission on the Space Shuttle Challenger Accident (Washington, D.C.: Government Printing Office, 1987).
- Software Security Assurance: A Framework for Software Vulnerability Management and Audit, by Charles H. Le Grand, CHL Global Associates. July 2005 (www.ouncelabs.com/audit).

Appendix C: Case Studies

1. The Challenger Disaster

Following the Challenger accident in 1986, NASA commissioned a series of extensive analyses of systematic risk management failures. Specifically, they studied the failure of the heat shield tiles that protect the shuttle during re-entry. In the case of the 1986 shuttle disaster, misalignment of the heat shield tiles caused a shift from laminar to turbulent airflow over the underside of the orbiter. This shift increased the heat load on the Challenger beyond the heat failure point. NASA's root cause analysis suggested that the Challenger accident was predominantly organizational and human, rather than technical in nature. The relevance that this failure was organizational and human in nature, not technical, comes into more specific relief in the "Recommendations" section of this paper. However, a brief discussion on the mechanism used to assess failure, assess risk, and address risk is of value in understanding the Working Groups approach.

Engineers commissioned by NASA following the Challenger incident modeled and mapped risk factors across the skin of the orbiter. Although covered in a uniform heat shield blanket, this risk mapping allowed engineers to understand that specific heat shield tile failures created exponentially higher risks of catastrophic failure than other areas of the shuttle. In fact, 15 percent of the heat shield tiles covering the orbiters skin represented 85 percent of the heat shield failure risk.

The second component of the Challenger assessment included an analysis of human factors that may have contributed to heat shield failure. The assessment identified artificial time constraints that resulted in human compromises in work processes and quality. This assessment identified basic managerial limitations that negatively impacted the quality of Challenger construction and maintenance. For example, the low wage and rate structure surrounding key construction workforce members created high turnover, limited the domain expertise and experience levels of tile technicians, and negatively impacted, again, the quality of the work.

The assessment concluded that there were a number of risk management failures in the Challenger incident, but the nature of those failures were generally non-technical in nature. For example, focused testing on the critical 15 percent of tiles prior to launch, reduced by 85 percent the overall risk of heat shield tile failure to the orbiter prior to re-entry. This focused, risk-based testing approach lessened the overall testing timeline and improved the output of the exercise. Improved training, rate structures, and more flexible timelines resulted in performance and quality improvements. In conclusion, the risk management experts provided recommendations to NASA managers that there existed ample room for improvement in the weakest technical links (bonding between the tiles and the shuttle), the most frequent human errors (shortcuts to meet artificial timelines) and the most common management errors (keeping trained people and prioritizing critical risk management efforts).

2. The 9-11 Commission

Another risk management initiative worthy of study is the 9-11 Commission Report. The 9-11 Commission suggested that components of the risk management failure included the inability to integrate information resources in a timely and accurate manner and the inability to get data to those who needed it in an efficient manner. To address these information sharing deficiencies, the Commission proposed an integrated approach to intelligence in the public and private sector. [i] Comptroller General David M. Walker noted that the public and private sector should work together "to provide incentives for sharing and creating a 'trusted information network.'" Many Commission recommendations address the need to "improve information and intelligence collection, sharing, and analysis within the intelligence community itself." In addition, the report stated, "we must not lose sight of the fact that the purpose of improving information analysis and sharing is to provide better information throughout the Federal government, and ultimately also to state and local governments, the private sector, and our citizens, so that collectively we are all better prepared."

The 9-11 Commission recommended the following practices:

- Establish trust relationships with a wide variety of Federal and non-federal entities that may be in a position to provide potentially useful information and advice on vulnerabilities and incidents;

- Develop standards and agreements on how shared information will be used and protected;
- Establish effective and appropriately secure communications mechanisms; and
- Take steps to ensure that sensitive information is not inappropriately disseminated."

Again, in the case of the 9-11 Report, the failures identified by the Commission were managerial and procedural in nature and not predominantly technical. These two examples suggest that there are commonalities in unrelated, high-profile risk management failures. The litany of available disasters to study and the body of accompanying knowledge is extensive, and worthy of more detailed analysis.

These two examples, the Challenger disaster and 9-11, identify common trends across the many case studies reviewed. These trends include management failures, human factors, information collection, analysis, and dissemination limitations, and technical breakdowns. These findings are further delineated in earlier sections of this document and the commonalities identified in these case studies translate well into actionable, achievable recommendations from the NIAC.