NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

BEST PRACTICES FOR GOVERNMENT TO ENHANCE THE SECURITY OF NATIONAL CRITICAL INFRASTRUCTURES

FINAL REPORT AND RECOMMENDATIONS BY THE COUNCIL

April 13, 2004

KAREN KATEN
WORKING GROUP CHAIR
PRESIDENT
PFIZER GLOBAL PHARMACEUTICALS

ACKNOWLEDGEMENTS

Ms. Karen Katen wishes to acknowledge the efforts of the entire study group and their support staffs (listed below), and extends her deep appreciation to the many other individuals who have offered their time and given advice to support this effort.

NIAC Working Group

Karen Katen, Chair, Pfizer

John T. Chambers, Cisco

Chad Holliday, Dupont

Marilyn Ware, American Water

L. George Martinez, Sterling Bank

NIAC Study Group

Bruce Larson, American Water

Glenn Rust, Sterling Bank

Beth Turner, Dupont USA

Ken Watson, Cisco

Jonathan White, Pfizer

Contributors: Financial Services

David Bauer, Merrill Lynch

R. Callahan, Bank of America

Ron Davies, MBNA

John DiNuzzo, FleetBoston

Dan Donahue, DTCC

Bob Errico, NASD

Greg Ferris, Morgan Stanley

Fred Francis, Whitney Bank

Eric Goldberg, AIA

Suzanne Gorman, FS-ISAC

Doug Johnson, ABA

Tom Johnson, AG Edwards

Paula Larkin, JP Morgan Chase

John Lewicki, Bar Harbor Bank & Trust
Teresa Lindsey, BITS
Peggy Lipps, Bank of America
Aaron Meckler, Wells Fargo
Susan Orr, FDIC
Ty Sagalow, AIG
Paul Smocer, Mellon Bank Goldman Sachs
Jeff Sprecher, Intercontinental Exchange
Jeff Stempora, State Farm
Chris. Terzich, Wells Fargo
Phil Venables, CISO
Susan Vismor, Mellon Bank
Bob Vitali Morgan Stanley
Paul Webb, Occidental Fire and Casualty
Grant Westcott, CIBC

Contributors: Chemicals

Rita Ayers, Dupont
Jerry Hale, Eastman Chemical
David Kepler, Dow Chemical
Greg Lebedev, ACC
Robert McArver, SOCMA
Alan Roberts, DGAC
Anne Wilms, Rohm & Haas

Contributors: Information Technology

Edward Abbo, Siebel
Peter Allor, ISS/IT-ISAC
Rob Clyde, Symantec
Kathryn Condello, CTIA
Guy Copeland, CSC
Daryl Eckard, EDS

Jerry Fiddler, Wind River
Avi Freedman, Akamai
Greg Garcia, ITAA
Doug Hurt, V-One
David Kanupke, USTA
David Nagel, PalmSource
Will Roger, CCIA
Monique Shivanandan, Bell South
Michael Tiemann, Red Hat

Contributors: Water

George Belhumeur, San Jose Water Company
Paul Bennett, NYC Dept. of Environmental Protection
Susan Conway, American States Water Company
Tom Curtis, American Water Works Association
Mike Gritzuk, Phoenix Water Services Dept.
Rob Guzzetta, California Water Service Company
Mark Hartman, City of Lafayette
Jack Hoffbuhr, American Water Works Association
The Honorable Connie Hughes, New Jersey Board of Public Utilities
Jerry Johnson, DC Water & Sewer Authority
Daniel Kelleher, American Water
James McDaniel, LA Department of Water & Power
John Quain, Klett Rooney Lieber & Schorling, P.C.
David Rager, Greater Cincinnati Water Works
John Sullivan, Jr., Boston Water & Sewer Commission
Edward Thomas, National Rural Water Association
Diane VanDe Hei, Association of Metropolitan Water Agencies

Contributors: Transportation

Brad Ballance, ATA
Fred Grigsby, Canadian National
Jack Legler, American Trucking Association

John McPherson, Florida East Coast
Roberta Weisbrod, Independent Consultant
Nancy Wilson, Regulatory, Assoc. of American Railroad

Contributors: Energy

Gary Gardner, AGA
Kent Gee, Shell/API
Bobby Gillham, Conoco-Phillips
Barry Lawson, NRECA
Lou Leffler, NERC
Dennis Wrasse, Pepco

Contributors: Public Health

Bruce Fadem, Wyeth
Ole Mikkelsen, Amgen
Adrian Seccombe, Eli Lilly
Karen Williams, National Pharmaceutical Council

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The tragic events of September 11, 2001, and the recent failure of the Northeast electrical grid on August 8, 2003, have highlighted how dependent our nation is on its critical infrastructure. The NIAC has learned through these experiences how interconnected our infrastructure is, and how globally exposed the United States is to targeted attacks, recognizing how insufficiently prepared we are.

Furthermore, the Council recognizes how much convergence there is between physical and information infrastructures. Therefore throughout this document, consider security as including both physical and cyber issues. For example, in August 2003 the Blaster worm temporarily halted CSX train operations nationwide.[1] During the recent Northeast blackout, communication among electric system operators was hindered by the same worm, limiting the operators' ability to identify and repair problems in the grid.[2] With malicious code now taking only minutes to infect vulnerable systems globally, and more vulnerabilities being detected daily, responses will have to be swift and effective in closing gaps and preventing local issues from becoming systemic.

Public and private sector organizations are responding, both within their own institutions and across industry and sector boundaries, driven by the need to secure their own operations and protect business relations with customers and partners.

The NIAC members clearly believe that where market forces are free to operate, they will be the most efficient and efficacious vehicle to enhance the security posture of critical infrastructures. However, some suggest that the pace of change may be too slow and the response may be incomplete. If market forces prove unable to operate efficiently and quickly, government should consider timely intervention, but only when there is a good characterization of the potential harm that could occur from an attack, and a better understanding of the role that market forces play in promoting an improved security posture across the sector.

The NIAC has been asked to make a recommendation on the role of government regulation in-ensuring a more effective response to physical and cyber security challenges. The Council elected to refine the definition from "Regulation" to "Government Intervention," for there is a wide range of private and public responses. In the private sector, responses may include contractual relationships, insurance, standard setting, innovation, competition, technological advances, and diffusion of best practices which government should encourage. In the public sector, the range of responses includes not only regulation, but also tax credits, subsidies, research and development investments, procurement leadership, and public education.

The Working Group therefore focused on how selected sectors differ in their physical and cyber security needs, the advantages and disadvantages of market intervention, and identifying the conditions under which government intervention should occur.

It has reviewed existing studies on government efforts in specific sectors, conducted in-depth interviews across many critical infrastructure sectors to develop a broad view of

---

[1] The Wall Street Journal, "Computer Viruses Disrupt Railroad and Air Traffic", August 21, 2003.

[2] Interviews.

security issues, and developed a framework for analysis. Subsequently, the validity of this framework was tested with extensive industry participation in four sectors: chemicals, financial services, information technology and water. It proved to be a useful tool for assessing the ability of markets to effect change, and to structure the debate on the need for intervention in each sector.

In the first section of the document, the Working Group discusses the framework for evaluating the applicability of government intervention across and within sectors, and identifies a number of best practices for government when considering intervention to encourage a more sustained and effective security posture.

The second section of the document discusses in greater detail the implications for specific sectors, and how the framework leads to different conclusions for each sector.

FINDINGS AND FRAMEWORK

Analysis of the existing literature and information from sector interviews has led to five key findings:

1. Deep understanding of sector dynamics is needed for effective intervention.
2. Organizations are responding through competition and cooperation, to address threats.
3. Government action may be required in some sectors.
4. A common framework may be used to discuss the role of market intervention.
5. Identified best practices should be considered when intervention is planned.

1. Deep understanding of sector dynamics is needed for effective intervention.

Broad recommendations on the need for government intervention are challenging because sectors differ greatly in their need for change for two reasons:

1) The need for regulation is different across and within sectors and sub-sectors because of differences in structure, market forces, and 2) Existing regulation. For example, the water sector is composed of largely independent local monopolies with weak market forces, while the financial services sector is an interconnected competitive sector with strong market forces and existing regulatory structures.

Even within sectors there is great diversity. In financial services, banking institutions are structured as an interconnected network and are regulated at the federal level, whereas the insurance companies, structured as more independent nodes, are regulated at the state level. Given the extensive differences within and across sectors, any proposed intervention needs to be designed and enforced at the appropriate level and through the most effective agency.

In the case of financial institutions, there are also supranational regulations, such as the Basel Capital Accords. The current Basel II accord makes operational risk, which includes internal controls such as network security, a factor in determining minimum cash reserves required for large global banking institutions[3]. This highlights the need for deep sector understanding when applying regulation.

Though most NIAC sectors may be deemed "critical," there are differences in the potential impact of a failure across and within sectors and it can be hard to separate those events that threaten national security and the economy from those that do not. For example: a failure in the electricity sector can quickly impact multiple industries. In addition, damage to a key payment system such as a major Federal Reserve District can have significantly more systemic impact than damage to a small regional bank. Where sector or sub-sector members are critical nodes for the system, they need to meet a higher security standard.

[3] A useful write-up of the impact is provided by Dan Geer at http://www.itsecurity.com/papers/stake1.htm.

In defining where to focus, it is essential to consider the impact of an attack on an individual player, the impact of that initial attack on other players within the sector, and the impact of the damage to the sector on other sectors. This requires a deep understanding both of industry-specific issues and of the interdependencies of systems.

2. Organizations are responding through competition and cooperation, to address threats

In all the sectors examined, a combination of market forces, sector-led initiatives, and government actions were found to interact to drive security behavior.

In most sectors, market forces are the most pervasive and powerful drivers of change in critical infrastructure protection both across and within sectors. Companies have recognized how their critical assets can be damaged by malicious intent, and are responding effectively to the threat. The Working Group found that in many diverse industries security has been elevated from a functional issue to a frequent topic of debate at the CEO and Board level. However the effectiveness of current market forces still differs widely among sectors, and among companies within a sector.

In some sectors, sector-led initiatives and regulations were found to be effective in augmenting market forces in driving security. Industry groups such as the North American Electric Reliability Council (NERC) and the American Chemistry Council (ACC) have published mandatory security guidelines for their sectors. However, the strength of the enforcement mechanisms can vary. The ACC's guidelines are self-enforced, though physical site security enhancements currently are independently audited, and ultimately all aspects will be. NERC can notify the Federal Energy Regulatory Commission (FERC) of electric companies not in compliance, bringing unwanted regulatory scrutiny.

Across sectors, different forms of oversight exist which provide an obligation to conduct some type of activity such as performing a vulnerability assessment, meeting specific outcomes such as recovery times for financial data, or taking specific steps such as putting up a fence or firewall.

In financial services, regulation already drives security behaviors highly effectively, and many participants see regulation as being of pivotal importance in securing the system, and excluding weak players from participation. At the other extreme, in information technology little intervention exists and participants feel that where customers are in a position to switch products and services in a competitive environment, market forces eventually eliminate non-performing suppliers.

3. Government action may be required in some sectors

In determining the need for government involvement, the balance of "spill-over" impact and responsiveness of the sector to threats should be considered. For sectors with strong incentives for security already, additional government action is unlikely to be needed. This may also be true where security is incomplete, but the impact of an attack is very local and limited.

The key areas to examine for potential government intervention are where there is a relatively high potential impact from an attack and, where there are comparatively weak incentives to take preventive actions. Areas with weak incentives, but potential lower impact may be considered as a second priority.

In general, government actions distorting the market least are best. The Securities Act of 1933 and follow-on regulation prompted disclosure of financial information companies had little market incentive to provide, is a widely held example of good legislation. It added transparency and improved the operations of market forces and is seen as a pillar for the stability of the nation's financial services sector.

Furthermore, the existence of a market failure does not automatically mean that government can provide a better solution. Many examples can be found of well-intentioned regulation that has proven costly. Government audits of its own performance show that the benefits of many existing regulations do not justify the overall costs to implement or have unintended negative consequences. The Office of Management and Budget estimate Housing and Urban Development (HUD) regulations on manufactured home construction and safety standards for wind cost $412 million annually with annual benefits of $64 million.[4]

Finally, regulation should not be excessively restrictive. FDA regulations require pharmaceutical manufacturers to document and test all changes in process control systems. As a result, some manufacturers today may be disinclined to update anti-virus software or modernize systems to introduce better protection, as the process will need to be expensively revalidated.[5]

Consequently, before choosing to intervene, alternatives should be examined and the potential negative impacts should be investigated. There are three high-level concerns to discuss before reaching a conclusion that market intervention will be beneficial:

1. Will market forces work over time? While existing incentives may not be strong enough to drive adequate security for a particular market today, it is useful to consider how incentives may change over time and how market changes may increase companies' self-driven effort to enhance security. Increased awareness by customers/consumers of high profile attacks could drive switching based on security, which would drive the sector to improve security faster than regulation can be introduced.
2. Can the sector provide its own solution? Sectors may be able to establish their own mechanisms to increase security, and if they can achieve wide participation and consensus-driven recommendations, it may obviate the need for government intervention. In sectors with diverse types and sizes of firms, by contrast, government actions may be warranted, For example, while ACC represents most of the U.S. productive capacity for chemicals, it encompasses only a small percentage of facilities. Accordingly, ACC has called for federal regulation to

[4] OMB, "Draft 2003 Report to Congress on the Costs and Benefits of Federal Regulations", February 2003.

[5] Interviews.

require all chemical facilities to take steps equivalent to those its members have taken.

3. Can regulation be successfully applied to this sector? In mature sectors effective public/private partnerships and regulatory processes may be suitable to facilitate the desired security enhancements within the sector. In immature sectors with rapidly evolving business models effective intervention is difficult to construct and apply. One should determine if regulation can achieve its desired intent without causing severe negative consequences, such as stifling innovation.

4. A common framework may be used to discuss the role of market intervention

At a more tactical level, in the Working Group's assessment of whether the current level of government scrutiny will serve, or whether there is a need for new intervention, it has found eight screening questions to be of value in making this judgment. These screening filters provide a common language to discuss the power of market forces, and coordinated sector activity to provide critical infrastructure protection without guidance.

The Working Group's assessment of each of the four sectors revealed that this framework led to new insights on the sector dynamics, and a richer discussion of the effect of government oversight on industry participants.

1. Are there network interdependencies in the sector? Do the participants in an industry interact in ways such that the failure of one can precipitate the failure of peers or down-stream industry participants? Financial services and electricity provide prime examples of sectors with rich and potentially catastrophic interdependencies.
2. Do security concerns drive customers to switch? Banking customers will not keep their assets at an institution perceived to be insecure; in contrast, commodity chemical customers frequently purchase largely on price, and may be unaware of any security exposures of the supplying company. Increasingly, security is being recognized in IT as a CEO-level issue, and supplier decisions are being made on security grounds, with the risk of asset loss driving security postures**.**
3. Is voluntary sector activity already occurring? There are many examples of voluntary bodies providing non-regulatory mechanisms to drive security and compliance. In the chemical sector, members of the major trade associations conduct vulnerability assessments and address identified vulnerabilities. The ACC has also established the Chemical Sector ISAC to allow threat information to be shared within the sector and between the sector and the federal government.
4. Can the sector exert peer pressure? Sector bodies can drive change through market mechanisms or by influencing existing bodies to produce change. For example, the Internet Engineering Task Force (IETF) plays a strong role in standard setting for telecommunications. They encourage the emergence of common standards, and provide a fast-acting and interactive way to produce international standards that could not be achieved by a single national government.

5. Do attacks occur frequently? Frequent attacks, such as hacking of military and commercial databases or virus attacks have become the norm for most companies. Consequently, considerable effort is expended on preventing and limiting damage. In contrast, even in the best-managed companies it can be hard to retain focus within an organization on unlikely and infrequent events.
6. Could the attack cause catastrophic injury or major economic damage? Even infrequent events are considered where the outcome could be severe. Chemical and water companies went to great lengths to protect the public's trust long before 9/11. Corruption of a database by hacker attack could lead to patent invalidation, and technology firms go to great lengths to secure their intellectual property.
7. Is the industry profitability high enough to invest in security? In industries with limited financial flexibility, there will always be participants struggling to survive. There is a risk that such firms will cut corners on security issues and jeopardize the public and other sector companies. Regulation may be the only route to create and maintain minimum standards.
8. Is there sufficient expertise to execute a plan? In many industries there is a high and increasing level of preparedness among most major participants. Among smaller players, however, there may not be the expertise to drive change, and without minimal standards there may not be the incentive to devote staff and resources to improving security postures.

5. Identified best practices should be considered when intervention is planned

If the government does decide to intervene, the Working Group's interviews have suggested some of the conditions under which government involvement is most likely to prove beneficial:

1. Develop plans in concert with industry. If government intervention is to occur within a sector, plans should be developed in partnership with the sector. Plans that are developed through public-private partnership will build on existing best practices, recognize sector-specific needs and have a higher degree of buy-in from the sector. Strong private-public collaboration was used in drafting the FFIEC[6] regulatory handbook, which is broadly recognized by the banking industry for its value. Given the scarcity of resources for enforcement, regulations that lack sector buy-in are generally less effective. The Environmental Protection Agency's (EPA) Underground Storage Tank (UST) program regulates leak detection and prevention in tanks containing petroleum or hazardous substances. However, more than 60 percent of states cannot inspect facilities in-line with the EPA's recommended once-every-three-years guideline due to under-staffing.

[6] Federal Financial Institutions Examination Council

Without buy-in from the industry, driving compliance through inspection would be difficult.[7]

2. Mandate outcomes rather than specific actions. Regulations requiring specific actions or technologies may quickly become obsolete, inhibit innovation, or produce inefficient business practices. For example, requiring a particular technology may initially promote cyber security but will delay subsequent implementation of more advanced security measures. A focus on outcomes gives companies full flexibility to achieve the desired goal through methods that best match their business. The government should also recognize voluntary initiatives may precede intervention, and if government agencies do not seek to leverage the work of early adopters or cause companies costly rework, they will inadvertently discourage companies from taking more timely remediation.
3. Ensure alignment between federal, state, and local regulations. With multiple jurisdictions and agencies potentially imposing regulatory requirements across a wide range of sectors, there is significant opportunity for conflict. For example, larger water systems are required by the EPA to conduct and submit vulnerability assessments. However, some state sunshine laws require public discussion of the assessments in order to secure funding, thereby making vulnerabilities public knowledge.[8]
4. Evaluate all new and existing rules through a "security filter". Rules pertaining directly to security make up only a small portion of government regulations. Other regulations may affect security, often in unanticipated ways. For example, for environmental and safety reasons EPA regulations limit the amount of fuel or battery back-up power that can be stored at a cellular telephone tower. Therefore, during extended electricity outages, backup power supply is limited, causing the rapid loss of the mobile phone network on which government and private sector services depend for restoration of services.[9]
5. Incorporate flexibility or sunset provisions. With the rapid pace of change today, proposed government interventions can quickly become obsolete. Incorporating flexibility or even sunset provisions requiring the rule to be renewed on a regular basis can ensure government actions stay relevant. Regulation of local telephone service as a natural monopoly might now be considered less necessary as technology and competition have eroded the concept of a natural monopoly.
6. Funding may be necessary to fulfill government mandates. Unfunded mandates are of special concern in the public sector, where voters may not be willing to fund security improvements through taxation. In the private sector, market distortions can be introduced if regulations are not uniformly applied.

---

[7] GAO, "Environmental Protection: Improved Inspections and Enforcement Would Ensure Safer Underground Storage Tanks", May 2002.

[8] Interviews.

[9] Interviews.

Furthermore, implementation of rules that impose significant costs where circumstances do not readily permit recovery of those costs, e.g., through higher prices to consumers, will not be effectively implemented. In such instances, government could consider providing incremental funding to meet the mandate. There are precedents: when the EPA mandated vulnerability assessments only for large water systems, it provided funds so the systems would not be differentially impacted relative to their smaller peers.[10]

7. Implement interventions in phases. Depending on the scope of proposed intervention in the market, implementing all provisions at one time may put an unrealistic burden on both the industry to comply with, and the agency to oversee adoption. Gradual implementation allows the industry to prepare and spread out necessary capital investments, and allows the agency time to mobilize staff. A phased implementation with intermediate milestones allows industry and government to gain information about effective and efficient compliance strategies, and unforeseen compliance opportunities and problems. For example, fuel efficiency standards for automobiles were increased over a number of years, allowing industry time to adjust production and develop new technologies.

[10] Interviews.

POTENTIAL IMPLICATIONS FOR SELECTED SECTORS

Applying the findings to different sectors yields some preliminary ideas of where market intervention may be more or less applicable.

In accordance with Homeland Security Presidential Directive 7 (HSPD-7), discussion should take place between DHS and industry sectors to guide future recommendations, and significantly more analysis should be done before any specific policy recommendations are made. The outputs of this application are meant to serve only as a starting point for further considerations regarding government action.

1. Chemicals

The chemical sector includes chemical manufacturing, transportation, and storage/use of chemicals.

Entities in this sector are not operationally interconnected and are interdependent to the same degree as in financial services. Most buyers are not solely dependent on one supplier for a given chemical. Thus, while an attack in the chemical sector could have a large local impact such as a plant shutdown or causing a release of hazardous material, it would be unlikely in most cases to spread to other chemical sector entities or to other sectors. Thus, the potential systemic damage is lower than in some other sectors.

There are some exceptions to this generalization. First, some facilities and companies are the sole or predominant source of a material in the U.S., so a successful attack on one of those facilities could have very disruptive effects. This is particularly true in the pharmaceutical and national defense areas. Rather than causing a release at a facility, terrorists might steal a product for release at a more critical location. Finally, terrorists might contaminate a product. Discovery of a contaminated oxygen tank, for example, could have adverse effects for the health care system.

The chemical industry has long been concerned about safety and accident prevention accidents. Many safety measures have had a positive impact on security and measures to mitigate damage from an attack. However, market forces to maintain high standards for security are lower than in other sectors. Customers are unlikely to switch solely based on security, as they are more concerned with price and quality. Since the industry is not very interconnected, peer pressure is also limited. Local communities containing chemical manufacturers provide some market incentive by granting "rights to practice" in their communities, which could be withheld if there are security issues affecting public safety.

Sector-led initiatives seem to be moderate drivers of security, but are potentially stronger than any other force. The sector's Responsible Care program requires members of the major trade associations[11] to conduct vulnerability assessments and address identified vulnerabilities appropriately to the threat they pose. Recently, another industry group, the

[11] The American Chemistry Council (ACC) and the Synthetic Organic Chemical Manufacturers Association (SOCMA)

Chemical Industry Data eXchange (CIDX), developed a set of cyber security standards, based on an analysis of the ISO 17799 standard and methodologies developed in the financial services sector. CIDX is currently pushing for adoption of these standards across the sector. The ACC has also established the Chemical Sector ISAC to allow threat information to be shared within the sector and between the sector and the federal government.

Regulation has not been a strong driver of security in the chemical sector. The main agencies covering the industry[12] focus primarily on safety and environmental protection. Regulations directly involving security focus primarily on the transportation of hazardous materials. For example, under the Department of Transportation's (DOT)'s HM-232 regulations, transporters of hazardous materials are required to develop and implement security plans, and train employees in their administration. The single major security-oriented regulatory program in this sector is the Maritime Transportation Security Act (MTSA), which imposes very detailed security provisions on chemical facilities that have accommodations for vessels (and on the vessels themselves). The MTSA also requires chemical facilities in port areas to participate in port-level security planning.

The chemical sector may well pose a smaller systemic risk to the U.S. economy than some other sectors. It also has weaker market forces or regulation to drive security than some other critical sectors. There are several sector-led initiatives to improve security, but the full extent of participation remains to be seen. Therefore, if the sector-led initiatives fail to achieve traction, some regulation may be needed to encourage full participation across the sector.

Given that the chemical industry is relatively stable and mature, it is unlikely to see major changes in market forces in the United States that will drive higher security. It is possible that sector-wide bodies, such as the ACC, may be able to further drive security. If this does not prove successful, regulation could likely be successfully applied to reinforce existing sector-led efforts. As noted earlier, ACC has already called for regulation equivalent to its program.

Any regulations should follow the practices seen in the financial services sector. Regulations should be developed in cooperation with the industry and be based on industry best practice. They should recognize the ACC/SOCMA program and not require rework. They should focus on overall methodology and outcomes rather than requiring specific solutions. This would allow enough flexibility to require high security where the risk is greatest and lower burdens where the risk is less. They should also avoid a focus on process safety, due to the high potential for government decisions in this area to shift risks, or create unforeseen risks, rather than reducing total risks.

[12]Environmental Protection Agency (EPA), the Department of Transportation (DOT), and the Occupational Safety and Health Administration (OSHA).

2. Financial Services

In the financial services sector, the dynamics are considerably different between banking, securities and insurance. The illustration below will focus on banking, thrifts and credit unions, jointly referred to herein as banks or financial institutions.

Any successful attack in the banking sub-sector could cause a high level of economic damage well beyond any direct impact on affected institutions. If a critical node, such as a major Federal Reserve District Bank or one of the country's larger financial institutions were disrupted, dependent banks would be unable to transfer funds or clear transactions with consequences that would swiftly ripple throughout other commercial sectors.

Market forces operate well in the banking sub-sector. Banks are constantly under cyber attack and must maintain high levels of security. This concern even extends to formally auditing potential partners before any interconnection. Since customers can easily change to a more secure service provider without incurring significant switching costs, there is strong incentive for banks to attain levels of security at or above peer companies to avoid that vulnerability.

Supplementing the strong market forces are several sector-led initiatives. The Financial Services Roundtable, BITS[13] and the FS-ISAC[14], amongst others, are providing forums for sharing best practices, developing security standards and software security tools, and receiving and disseminating threat information to the sector.

The regulatory agencies in the financial services sector also provide strong security incentives. The five regulators[15] in the banking sub-sector have produced a single set of security guidelines, the Federal Financial Institutions Examination Council (FFIEC) handbook. This handbook represents the best practices across the sub-sector. Examiners audit and rate banks on several dimensions, including security. Poor ratings can result in fines, increasing depository insurance premiums, and other severe regulatory limits. The agencies have identified critical nodes, which are examined more frequently and held to higher standards.

The regulations are based on existing best practices within the industry, and are flexible enough to incorporate new practices or new technologies. They do not prescribe particular solutions, but rather define a risk management methodology that all banks can follow. Regulations are developed in partnership with the banks, which is aided by the mutual goal of preventing bank failures.

A bank's profitability model contains the costs factors of regulation. Additional and/or changing regulations occur all the time, and most banks easily deal with these changes. A big reason banks are able to respond quickly to changes is because they receive input and

---

[13] The Banking Information Technology Secretariat

[14] Financial Services Information Sharing and Analysis Center

[15] The five federal regulators of the banking sub-sector are the Federal Reserve (The Fed), The Office of the Comptroller of the Currency (OCC), The Office of Thrift Supervision (OTC), The Federal Deposit Insurance Corporation (FDIC), National Credit Union Association (NCUA).

guidance from their perspective associations, it has been passed to most regulatory agencies, and in some cases, through legislative branches at the state and national level, thereby contributing to an easier adoption of many guidelines and regulations. Different associations send out newsletters alerting banks on how to prepare months in advance for impending regulations or guidelines and the associated costs.

The cooperation factor among financial institutions is very high. This is due to the amount of cooperation required to handle a variety of transactions (checks and electronic funds transfers) across the country and the world. Banks also cooperate in the formation of new laws that can benefit the sector by reducing long-term costs, such as Check 21. The main point is that banks are used to cooperating on a large scale and are active in working with regulatory bodies and each other on a variety of issues.

Another significant factor in the financial sector is that all regulatory agencies create discussion forums when formulating new regulations and policies. As mentioned in a previous paragraph, this creates an invaluable dialogue for the creation of many policies, which better protect the sector.

This sector also has the ability to change with speed. Because the sector has been regulated for so long the mechanisms for reacting quickly are already in place. An example of this was the reaction to Y2K. The financial sector was one of the first sectors tested and later prepared on a variety of fronts to head off public concern and panic regarding the flow of all types of transactions, both monetary and electronic. This sector proved that with a small amount of time and the right emphasis placed on public concern and trust, it could perform and react quickly to many issues and changes.

In conclusion, while there are high risks and potential economic impact to an attack, the banking sub-sector has multiple strong incentives to promote security. Therefore, it is unlikely that the banking sub-sector would need additional regulation or oversight from the Department of Homeland Security (DHS), and if the need arises for additional action, DHS could easily work through existing regulatory agencies.

3. Information Technology

An attack on technology products has potential for great damage to the overall economy since these products form the cyber infrastructure for all other critical sectors. Over the past few years, security has been a significant focus of technology companies. In fact, it is currently the area of the industry with the most activity, innovation, investment, and attention, with customers increasingly focusing on the security attributes of the products they buy. Until recently, non-national security customers have demanded features, performance, and interoperability over security from technology products. The current focus on security across all sectors has made IT providers more aware of the need to provide secure products. Similarly, peer pressure has recently shifted more towards security. The sector can afford to invest in security measures, and is investing heavily.

Recent market trends are showing greater emphasis on security, and with time may show more consistent customer demand for security in technology products. The Analyst Surveys section of the Goldman Sachs December 2003 IT spending survey shows that

security is the highest priority.[16] The same is true of the UBS report on the same period. "Top priorities: security themes ranked #1 and #2—intrusion prevention and SSL/IPSec—with storage area networks #3."[17] Credit Suisse First Boston's survey results "continue to indicate that security remains a top spending priority, as 89 percent of reseller(s) surveyed indicated that business during the first six weeks of the March quarter had increased sequentially versus the December quarter."[18]

Some sector-led initiatives address security across various segments of the sector. The IT-ISAC facilitates information exchange for its members, but membership is currently a small group. The IETF, Institute of Electrical and Electronics Engineers (IEEE), as well as other public and private groups also have initiatives to set standards and share information, but there is no consensus for any single initiative.

There is a broad consensus that the market is the strongest and most vibrant force for innovation and technological progress. The federal government's Common Criteria Evaluation and Validation Scheme rates the security of IT products and is used by certain government agencies in purchasing decisions, but it does not place any requirements on IT providers selling to the private sector.

There are many valid arguments against intervention in the IT sector, it can be highly counterproductive. Adopting specific security regulations could stifle innovation in the US and drive business offshore, and the international nature of the cyber security issue demands attention which single market rules cannot achieve. The ever-evolving nature of the Internet and the cyber-security threat demand a solution that can be quickly adapted to changing circumstances, which is inconsistent with the nature of the traditional regulatory structure.

The NIAC believes that regulation of the Internet is unwise, and market innovation will continue to drive adoption and innovation. The traditional regulatory structure is an open process including public comment. Such a process could lead to providing a roadmap of vulnerabilities to nefarious parties intent on causing damage. Government bodies do not currently possess the array of tools necessary to adequately police Internet security standards leading to the potential of unsophisticated decisions yielding less, rather than more security. The political process by which traditional regulatory standards are reached encourages compromise rather than maximum effectiveness. Hence, the political process could result in an inefficient program that could yield a false sense of security. Government regulation of technology may blunt innovation resulting in less consumer choice, economy and security. Therefore, by the filter criteria outlined above, there seems to be no case today for government intervention in the market.

Policy makers could consider incentives like tax credits, research and development, subsidies, procurement leverage, and enforcement of existing criminal laws. For

---

[16] Brantley Thompson, Christopher Fine, Angelo Liberatore, and Natalie Hayday, "December 2003 IT Spending Survey," Goldman Sachs Global Equity Research, January 20, 2004.
[17] Pip Coburn, Faye Hou, CFA, David Bujnowski, and Qi Wang, CFA, "PM Summary: CIO Survey," UBS Global Equity Research, January 2, 2004
[18] Todd D. Raker and Philip A. Winslow, "Secure Channels: Channel Survey & Analysis v. 1.04," Credit Suisse First Boston Equity Research, February 20, 2004

example, the federal government could demand strict security best practices for technology purchased by all its departments and agencies. Since it is difficult for most buyers to compare the security of technology products, the government could work with the private sector to develop security standards, test products and publish results. The government could also fund more security research to better understand the cyber threats and ways the IT sector can defend against them. Funded research would be especially attractive to industry if private researchers do not lose their rights to intellectual property, and if government uses flexible research vehicles such as "other transactions" or Cooperative Research and Development Agreement (CRADAs). Additionally, a program of insurance, liability, and tax incentives is more likely to yield an effective, comprehensive, and ongoing program of cyber-security consistent with the evolving and international nature of technology and threats. These actions could augment market forces and drive technology companies to improve the security of products.

4. Water

Of all critical infrastructure systems, the security of water systems has the most immediate and pervasive impact upon the public's health and welfare. Critical infrastructure, which DHS defines as, "those assets, systems and functions vital to our national security, governance, public health and safety, economy and national morale," includes approximately 54,000 municipal and investor owned water systems across the U.S.[19] According to evidence gathered by the Federal Bureau of Investigation (FBI), terrorists have researched various ways to attack water supplies, such as physically destroying water systems, hacking into computers that control and monitor operations, thus disrupting supply or contaminating the water supply.

American citizens have a right to expect that all the players and operators of the nation's water systems, utility regulators and elected officials will take every precaution to protect the health and safety of the American drinking water from the imminent threat of terrorist attacks. In recognition of this expectation, the President's Homeland Security strategy has called on the water sector in conjunction with the Department of Homeland Security to undertake specific threat assessments and take action to protect water sources, filtration and processing plants, and distribution lines.

A terrorist attack on a single water system can have an immediate psychological effect with the public losing confidence in the reliability and the purity of community water systems. America's water utilities, therefore, need to continue to take appropriate and substantial preventive measures to both protect their customers and be able to respond effectively to any attack.

The value and extent of water sector infrastructure developed over the past 100 years is beyond calculation; the replacement costs of this critical infrastructure could be measured in hundreds of billions of dollars.

[19] The term, "investor owned" includes private water systems as well as water companies that offer shares to investors.

Both municipal and investor owned water systems share concerns about the heretofore under recognized interdependencies with first responders and those who manage disaster relief. For example, firefighters need to be assured of a constant volume of high pressure water. This could be disrupted before, during and after a terrorist attack, permitting further devastation. In the recovery period, the need to wash down people, vehicles and buildings also raises new public health and safety issues as potentially contaminated water is subsequently drained from the attack site.

Beyond the security of water sources such as reservoirs, treatment plants, pumping stations and distribution pipelines, municipal and investor owned water companies have a shared concern with respect to the physical safety of dams. In addition to the disruption of supply that would attend a dam break, history has shown us that such breaks can be truly catastrophic events in their own right.

In an interdependent mode, both municipal and investor owned systems may provide water to cool electric generation stations. This cooling may take the form of primary or secondary supply. Any disruption in the water supply may deleteriously affect the energy sector if a generator relies on a water system to provide cooling.

While some historic funding and operational differences exist between municipal and investor owned water systems, these differences do not prevent the formulation of a comprehensive national strategy. Indeed, it is through the sharing of experiences and information in a secure forum that a motivated sector is most likely to arrive at a high quality, comprehensive national strategy.

Differences between these respective systems for instance, occur at the jurisdictional level. Both, however, are governed and incented by regulatory "market" action. Investor-owned systems generally fall within the regulatory authority of state public utility or public service commissions with overlapping jurisdiction from public health agencies. They can, therefore, be ordered to act or to refrain from acting. Municipal systems, on the other hand, are accountable to either local government or a local board that makes determinations on whether to act or not, in a somewhat different political context. Both municipal and investor owned water systems are dependent on legislative bodies that are presumed to be fully informed as to the complex operational realities of physical and cyber security at the same time they are bombarded by innumerable other complex responsibilities and diverse constituencies.

Despite the differences in funding and cost recovery methodologies available, at present neither investor owned or municipal systems are able to make the rapid infusion of capital necessary to mitigate or recover from a terrorist attack; both water entities are not incented from taking preventive measures by the regulatory or administrative lag associated with any rate increase, this is a major impediment to action.

This funding availability and timing issue raises another significant public policy concern: should available resources be directed to large, urban water systems that serve most customers and where the quantitative risk is greatest, or to smaller, often public systems that may have greater vulnerability? While the adequacy of safeguards and security research needs are also issues for all companies in formulating a comprehensive

national strategy, the failure to address funding issues may create significant differences between municipal and investor owned water companies.

The economic impact of enhancing security as well as the costs associated with recovering from an attack poses a daunting challenge. Some water providers are economically marginal to begin with, as a result of public and regulatory directives. Neither provider is legally or politically capable of unilaterally raising rates to recover dramatic, unanticipated costs such as those associated with infrastructure security.

A number of municipal and investor owned companies have, nevertheless, already made infrastructure security improvements at considerable expense. Many of these costs incurred from September 11, 2001, to the present remain unrecovered. The regulatory response to cost recovery requests for security measures has been uneven, and in some cases has consisted largely of public pronouncements rather than regulatory approval of specific cost recovery proposals.

The methods of cost recovery should also reflect the Administration's preference that market-based solutions apply to infrastructure security issues. The rationale here is that the consuming public -- which includes residential, commercial and industrial as well as governmental users -- should directly fund infrastructure security measures necessary to assure safe and reliable service at historic levels. This should be our point of departure in addressing cost recovery concerns.

Members of the water sector holding different views have advanced alternate cost recovery methodologies. With respect to federal funding, in order to stay within the President's mandate, creativity and efficiency in terms of cost recovery should be encouraged in both the municipal and private sectors, and first priority of funding should be given to those showing that kind of initiative. Many agree that the cost of attaining a baseline security posture across the water sector could exceed $750 billion. With this staggering scale of investment envisioned, government subsidization may not be the most practical method of intervention. The water sector is committed to providing water at the "true cost of service". Government standards for the sector to attain a security posture appropriate to the threats evident will allow the cost of securing the sector, to be accurately reflected in the cost of service to the ratepayer. This is the market process within the sector and best reflects the goals of having market forces incent the necessary security improvements.

CONCLUSION

The Council believes market forces are the most powerful drivers of change. They have identified the conditions where selected government intervention could be beneficial and use a framework that allows exploration of the efficacy of market forces in any sector. Applying the findings to different sectors has yielded preliminary ideas of where market intervention may be more or less applicable. Outputs of this application are meant to serve as a starting point for further considerations regarding government action. Further discussion should continue between DHS and industry sector representatives.