

Report on National Cyber Defense Initiative Industry Workshop

Report and Recommendations

March 27, 2009

This report provides a summary of a workshop, held at the Information Sciences Institute of the University of California November 5 – 6, 2008. The workshop was a continuation of an ongoing sequence of meetings in connection with a “grass roots” effort to create a 10-year research plan for the protection of our national cyber critical infrastructure from strategic damage. The purpose of the plan is to realize the vision—transforming the cyber-infrastructure to be resistant to attack so that critical national interests are protected from catastrophic damage and society can confidently adopt new technological advances. It is vital that this be accomplished in such a way as to create a lever to enhance U.S. high-tech competitiveness, attract top students into strong educational programs, and strengthen government, industry and academic research.

Attendees

Peter Allor (IBM), Terry Benzel (USC-ISI), Scott Borg (US-CCU), George Cox (Intel), Mary Ann Davidson (Oracle), John Frink (OSD), Carrie Gates (CA), Bret Hartman (EMC/RSA), Cynthia Irvine (Naval Postgraduate School), Steve Kent (BBN), Carl Landwehr (IARPA), Karl Levitt (NSF), Rich Mathews (NSA), Douglas Maughan (DHS), Charlie Meister (USC-ICIIP), Jelena Mirkovic (USC-ISI), Cliff Neuman (USC-ISI), Bridget Rogers (Sandia), Sami O. Saydjari (CDA), Rick Schlichting (AT&T), John Sano (Cisco), Tom Vagoun (NITRD), Ralph Wachter, (ONR), Norman Moulton (ODNI/DS&T), William Searcy (FBI)

Contents

Executive Summary	5
1 Introduction.....	7
2 Workshop Charge	8
3 Context.....	9
4 A Vision	12
5 Potential Costs of Cyber-Attacks on Critical Infrastructure Industry.....	13
6 Roles and Market Forces	15
7 Results and Recommendations	17
7.1 Policy and Strategy Recommendations	17
1. National Cyber Recovery Plan.....	17
2. Presidential Cyber-Response Plan	18
3. National Cyber Command and Authority	18
4. Cyber Security Rating Institution	19
5. Economics and Cyber Security Planning.....	19
6. Academics and Cyber Security.....	19
7. Advanced Research in Cyber Security	20
7.2 Recommended Technical Approaches and Mechanisms.....	20
1. Supply Chain Security Assurance.....	20
2. Security Modeling (unclassified technology).	20
3. Quantifying Problems/Impact.....	22
4. Build Industry Support for Proactive Positioning.....	22
5. Develop Policies and Mechanisms for Operation Under Mutual Suspicion	23

6.	Relational Trust Mechanisms (processes and tiering of effort/response.).....	23
7.	Education, Training and Human Resource	24
8	Summary.....	25
	Appendix A Mapping policy and technical recommendations to end states	27

Executive Summary

A Citizen-led National Cyber Defense Initiative (NCDI) has organized a number of workshops aimed at developing plans and input to the national discussion underway on Cyber Security. In November 2008, an NCDI Industry workshop was held. The workshop had representatives from the leading commissions and working groups chartered by various government organizations, and a balance of industry leaders and academic researchers. The workshop provided a forum for members of the computing and communication industry to contribute input to multiple planning and strategic efforts underway and to define actionable plans to take back to their organizations.

The workshop took a very focused and pragmatic view towards the recommendations and aimed to leverage partnership opportunities between government, academia, and industry. The results and recommendations from this workshop are consistent in many ways with those in other reports including “Securing Cyberspace for the 44th Presidency” by the Center for Strategic and International Studies and other commissions and panels. This is no surprise as there is overlap between key participants in these groups. However, the recommendations of this workshop reflect the participation of key industry leaders and the meta-level recommendations of an economics driven strategy.

The key recommendations from the workshop fell into two broad areas: strategic policy and technical mechanisms. Foremost in the strategic policy area, are specific recommendations to create national strategy, national response and recovery, and command authorities analogous to U.S. national strategies around nuclear defense during the height of the Cold War. These organizational strategic recommendations are supported through strategic recommendations for national-level cyber infrastructure measurement, economic based consequence analysis, and vigorous programs for the nation’s academic leaders and researchers. Again, analogies to the nation’s strategic initiatives during the cold war apply to the academic and research initiatives proposed here.

Balancing the strategic policy focused recommendations are technology focused recommendations. These are recommendations to research, develop, and implement technological approaches to the protection of information systems, approaches that must stay ahead of the competing, threatening technology that would exploit and corrupt those systems if it could. Key technology recommendations include mechanisms for modeling security, trust relations, attribution, techniques for supply chain assurance and techniques for quantifying problems and impacts. These technology recommendations are supported by recommendations for technical cultures and society that include proactive security management, an operational environment based on mutual suspicion and security technology as a key component of commercial products.

Taken together the recommendations of this workshop for policy, strategy, technology, mechanisms and a technical culture of security awareness have been mapped to the desired end-states that resulted from a previous NCDI workshop on defining end-states. The mapping is described in Appendix A. Thus, the results of these two workshops, Next Moves – 2007 and Industry – 2008 provide both a desired vision (for end-states in a secure world) and actionable recommendations that are under review by key government, industry and academic participants. These combined results provide an initial road map towards the goals of:

Over the next ten years transform

- **the cyber-infrastructure to be resistant to attack so that critical national interests are protected from catastrophic damage and society can confidently adopt new technological advances.**
- **the workforce and organizational culture aligned to design, develop, integrate, maintain secure critical infrastructure on an ongoing basis.**

1 Introduction

Large portions of our country's economic, industrial, social and governmental functions now depend upon a cyber infrastructure assembled from readily available commercial information system components. Much of this infrastructure is organized to tolerate random failures and outages but could fail catastrophically under malicious attack. Industry leadership is needed to substantially reduce this serious vulnerability. There are many efforts underway to begin to address these issues at the national level. A Citizen-led National Cyber Defense Initiative (NCDI) has organized a number of workshops aimed at developing plans and input to the national discussion underway. In November 2008 an NCDI Industry workshop was held. The workshop had representatives from the leading commissions and working groups chartered by various government organizations and a balance of industry leaders and academic researchers. The workshop provided a forum for members of the computing and communication industry to contribute input to multiple planning and strategic efforts underway and to define actionable plans to take back to their organizations.

The goal of the workshop was to develop a shared view of an attack-resistant and attack-tolerant cyber infrastructure and specific steps to be taken to reach that vision. The workshop charter was to identify how to achieve the vision of such an infrastructure through practical policies and courses of action by government-industry partnerships enabling an effective national research plan. During breakout sessions, four parallel working groups were asked to address following key questions:

1. **[Technology]** What particular technologies or processes are required to provide highly assured protection common to a broad group of critical infrastructures?
2. **[Roles and Market Forces]** What are the appropriate roles for industry relative to its investors, academia, and government in advancing the nation towards attack-resistant and attack-tolerant cyber infrastructure? Are there particular market issues that will help or hinder industry?
3. **[Research and Technology Transition]** As they become available, how can new research and technology be incorporated into commercial solutions more effectively? How can the research community and industry improve technology transition?
4. **[Education and Training]** How do we enlarge the pool of engineering talent available in the U.S. to develop the infrastructure we need? Should we refocus Computer Science and Engineering education to have a systems and infrastructure orientation? If so, how?

Industry participants in the workshop included representatives from major hardware and software vendors, and computer services that produce critical components and systems that underlie the critical information infrastructures of major sectors of our Nation's enterprise (such

as electrical power generation and distribution, banking, and telecommunications). Participants were chosen who brought a deep understanding of the technologies involved and also have significant influence over business decisions within their companies. To assure focus and productivity, the meeting was limited to 35 participants. The workshop was co-chaired by Terry Benzel, of USC-ISI and a member of the National Cyber Defense Initiative steering committee, and Mary Ann Davidson, of Oracle and a leader from industry with support from the National Science Foundation.

2 Workshop Charge

The paragraphs below are a verbatim recitation of the charge to the workshop attendees.

The goal of the workshop is to develop a shared view of an attack-resistant and attack-tolerant cyber infrastructure and specific steps to be taken to reach that vision. We will begin the workshop with a discussion in plenary session to describe the "What" in terms of a vision. Then in smaller working groups sessions we will address the "How" in terms of how to achieve this vision of such an infrastructure through specific steps, practical policies and courses of action.

In previous workshops we established the high level vision statement: Over the next ten years transform the nation's cyber-infrastructure to be resistant to attack so that critical national interests are protected from catastrophic damage and our society can confidently adopt new technological advances.

This should be accomplished by transforming technology, laws, education, societal norms, software and hardware so that strategic attacks can be resisted preventing, deterring, tolerating, surviving, and recovering quickly. Specific threats of concern are threats to government continuity and general welfare.

In preparation for the workshop we are asking you to bring your three ideas of "how" we can realistically achieve this vision, through adjustments to existing markets or through extra-market activities. We will spend the first 30 minutes of the working groups discussing these initial ideas and focusing the groups. The working groups are tasked as follows:

The first charge is to produce an actionable, triaged set of recommendations. That is, if there are things we can do near term to either effect immediate and positive change or lay the seeds for future improvements, we should put those recommendations in a Do Now bucket (as opposed to a Do Later bucket). We ask that you tranche: in relative importance (X is more important than Y) and in time (do X in the next 2 years, Y in 2-5 years, Z in 5-10 years).

The second charge is that we ask you all to consider the actors involved with a view towards including actors in the recommendations (e.g., "the government should do X to improve Y"). You should consider such factors as "who owns the problem?", "who can fix the problem?", "who can create a solution?" and perhaps "who can influence a solution?" For example, consider could the government adopt a particular standard or require it through acquisition regulations to help create a market demand for industry? While attendees are not (primarily) public policy experts or economists, our recommendations may be more actionable to the extent we can include the "who" of a recommendation and not just the "what."

3 Context

This workshop is the result of a sequence of activities initially triggered by a Defense Science Board study delivered in the summer of 2006. Prior reports addressing cybersecurity shortfalls can be found in every decade since 1970, but as the magnitude of the problem has become increasingly apparent over the last two years, a plethora of workshops have been convened and studies issued addressing hard problems, research agendas, organizational issues, and more. The accompanying chart depicts many of the current activities and indicates their origins and intended consumers. Although many of these efforts appear to be parallel and potentially uncoordinated, there is generally some significant overlap among the individuals involved, so there is perhaps less duplication of effort than it might appear. It is also worth noting that in each case there is usually some intended audience for the result – a specific government department, for example, which may have a particular mission and threat model. The resulting reports typically reflect these concerns.

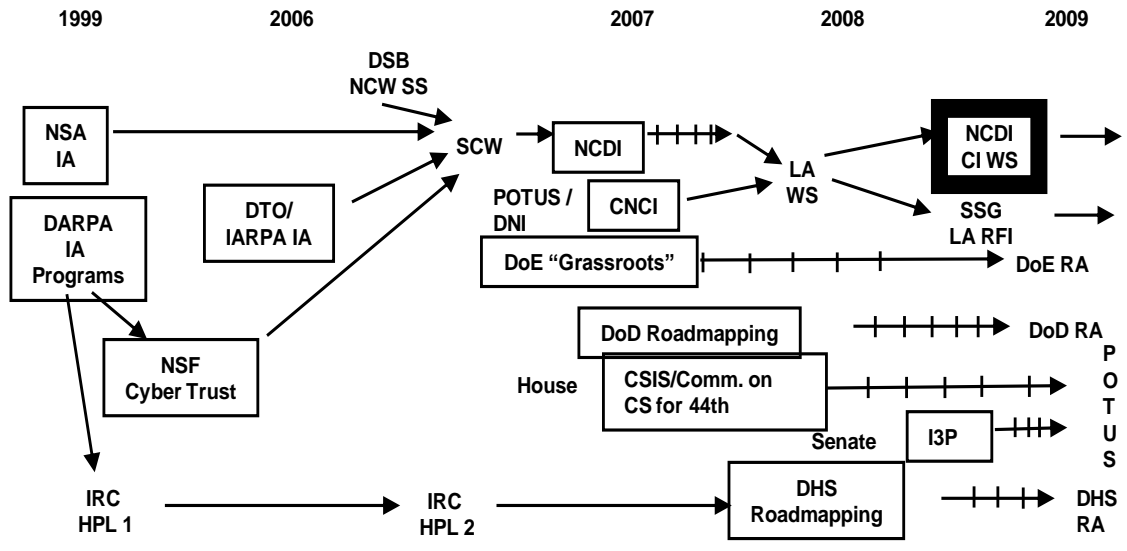


Figure 1: Relationship of NCDI with other security related initiatives.

Time ordering is approximate. Initiation of activity corresponds roughly to right hand edge of box with activity title. Vertical lines indicates workshops/meetings and are approximate

Although this chart includes many relevant activities, it is not complete picture of activities in cyber-security R&D during this period. The choice of 1999 as a starting point corresponds to the creation of the first IRC Hard Problems List.

CIWS	Cyber Industry Work Shop
CNCI	Comprehensive National Cybersecurity Initiative
CS	Cyber Security
CSIS	Center for Strategic and International Studies
DARPA	Defense Advanced Research Projects Agency
DHS	Dept of Homeland Security
DNI	Director of National Intelligence
DoD	Dept of Defense
DoE	Dept of Energy
DSB	Defense Science Board
DTO	Disruptive Technology Office
HPL	Hard Problems List (versions 1 and 2)
I3P	Institute for Information Infrastructure Protection
IA	Information Assurance
IARPA	Intelligence Advanced Research Projects Activity
IRC	Infosec Research Council (informal govt coordinating group)
LA	Leap Ahead
LA WS	Leap Ahead Work Shop
NCDI	National Cyber Defense Initiative
NCW	Network Centric Warfare
NSA	National Security Agency
POTUS	President of the United States
RA	Research Agenda
RFI	Request for Information
SCW	Safe Computing Workshop (Albuquerque, Nov/Dec 2006)
SS	Summer Study
SSG	Senior Steering Group (of the National Coordination Office (NCO)'s Cyber Security and Information Assurance Interagency Working Group)

Table 1: List of acronyms used in Figure 1.

4 A Vision

Previous workshops organized by the National Cyber Defense Initiative reached two important conclusions: (1) major cyber defense strategic investments could address the urgent need to reduce vulnerability to national information infrastructure within 5-10 years, and subsequently, that (2) There are promising strategic moves toward achievable end-states that can reduce risk. More planning is needed, with emphasis on market and quantification. These conclusions were motivated by a real and growing strategic threat, a view that current research activities are insufficient, and a realization that a focused research agenda in close partnership with industry is essential to succeed.

The vision statement stemming from the analysis of the previous workshops is as follows:

Over the next ten years transform the cyber-infrastructure to be resistant to attack so that critical national interests are protected from catastrophic damage and society can confidently adopt new technological advances.

The transformation called for is pervasive and includes not only technology but law, education, policy and even societal norms. The attack resistance refers not only to traditional prevention and detect-respond methods, but also to strategic deterrence, damage tolerance, critical function survival, and quick recovery. The reference to critical national interests suggests a strong focus on threats to government continuity and the public general welfare. In the end, the goal is to weave a secure cyber space fabric that enables quick and safe advances and economic strides in the information age.

Although the vision is specific and compelling, it is not prescriptive. Achieving it will be no small task and will require concerted effort of the nation's top talent. Toward breaking down the vision into more manageable goals, the NCDI workshop series identified key end-states which would characterize how we would expect to operate as a nation when our vision is realized. These end-states can then form top-level goals that can be accomplished by specific actions or programs that we called "moves" in recognition of the complex game we find ourselves in. These end-states are enumerated below and formed a starting point for this workshop in which we began how the government in partnership with industry might achieve the lofty goals toward the shared vision.

Desired End-States

- **Continuity of Critical Information Infrastructure Operations is assured.** A transformed, resilient US cyber infrastructure that we know will sustain critical functions in the face of attack.
- **Critical Assets are Protected/Defended from Strategic Damage.** Make it economically prohibitive for an adversary to cause strategic damage to the US critical infrastructure.
- **Infrastructure Providers can Maintain Local/Global Cyber Situation Awareness.** Know what is on critical system platforms, what is connected to the network, who is on the network, and the traffic flowing over it.
- **Cyber Early Warning Systems are in Place.** Early warning of cyber-attacks can be provided.
- **Infrastructure Systems Don't Leak Data (Data-Tight Systems).** Prevent unauthorized leaks or exfiltration of critical information and intellectual property. Ensure accountability for information flows.
- **Infrastructure Systems can be extended safely to embrace new technology.** New functions can be confidently added without compromising existing function or assurance.
- **Infrastructure Systems can provide continuous, quantified reports of their security and dependability.** Where possible, new metrics and measurement technology will permit security and dependability to be quantified based upon realistic assumptions.

5 Potential Costs of Cyber-Attacks on Critical Infrastructure Industry

To help establish a context for discussions, an economist with a background in measuring the cost of potential cyber attacks was invited as a key note presentation. The information presented here is a summary of the keynote presentation and is drawn from published reports and a soon to be published book by Scott Borg and the U.S. Cyber Consequences Unit, a non-profit organization. www.usccu.us.

The losses that our country could suffer as a result of cyber-attacks on our industries are enormous. The overall scale of the destruction is determined by four factors¹:

1. the difference between level of need satisfied by the operation under attack and the normal costs of meeting that need,

¹ This analysis is explained in detail in Scott Borg, *Cyber-Attacks: A Handbook for Understanding the Economic and Strategic Risks* (forthcoming).

2. what substitutes for the operation under attack,
3. the duration of the effects produced by the attack, and
4. the extent to which other operations depend on the operation under attack.

These four factors make the destruction that can be caused by attacks on critical infrastructure industries especially great. We have a very great need for things like electricity, oil and gas, telecommunications, financial services, water, and transportation. Yet the cost of these things, relative to our need for them, is relatively low. Hence, the difference between the level of need satisfied by these critical infrastructure industries and their costs is very large. If we are deprived of these critical supplies and services, there are hardly any substitutes. Most of the things we accomplish with electricity, oil and gas, telecommunications, water, and so on, can't be readily accomplished without them. Cyber-attacks are capable of physically destroying much of the equipment utilized by critical infrastructure industries. This equipment generally takes many months to repair or replace. Hence, if these industries were attacked, the duration of the effects would be potentially long. Finally, almost every activity we carry out in our economy depends on these critical infrastructure industries. Even businesses that can manage for extended periods without electricity, oil and gas, telecommunications, water, or other such basics, will still depend on other businesses that are unable to do without them. Since many of the cyber-attacks that threaten critical infrastructure industries could be automated and are scalable, the portion of the country that could be affected by a given wave of cyber-attacks is very great and could easily encompass many states.

The U.S. Cyber Consequences Unit has been able to produce tentative estimates of the extent to which all economic activity would be shut down as a result of cyber-attacks on critical infrastructure industries. If the shutdown lasted for three days or less, the losses would be minimal. Despite lean supply chains and just-in-time delivery, most parts of the economy have at least three days worth of extra inventory. Despite efficient utilization of facilities, most parts of the economy also have enough extra capacity to make up three days of lost production before the end of the quarter and usually before the end of the month. But after three days, the losses begin to climb rapidly. If electricity is shut off over a region that is large enough so that it can't be serviced from outside, after eight to ten days, about 72% of all economic activity as measured by GDP will shut down. If oil and gas supplies are shut down, it could take up to three weeks before the full effects would be felt, but then about 71% of all economic activity will shut down. Without telecommunications, the portion of the economy that will shut down is about 62%. Without any banking and financial services, the portion is about 59%. Without water and sanitation, the portion is about 40%. Without air transport, the portion is about 24%. All of these estimates assume that people are extremely ingenious in employing every substitute operation they can find. Despite this ingenuity, the loss of essential services and supplies would inevitably result in many people dying. No modern economy has ever suffered this level of

damage. The only plausible scenarios that would produce a similar scale of destruction involve nuclear exchanges.

6 Roles and Market Forces

The workshop was oriented towards contributions from and to industry participants from major hardware and software vendors, and computer services that produce critical components and systems that underlie the critical information infrastructures of major sectors of our Nation's enterprise. An early discussion in the workshop was around the question of roles and market forces, briefly summarized here and representing the views of some participants.

Market Failure: There is an argument that the market has failed for "secure software" in that the security-worthiness of commercial software (even commercial software used in critical national security applications) is not readily ascertainable by the customer. That is, customers do not know what they are getting in terms of IT products they buy; in particular, they do not know how secure the product is or what their lifecycle "costs to secure" are likely to be. There are multiple remedies available to correct market failures which range from using customer purchasing power to change the demand side of the market, up to and including regulation.

Before immediately jumping to the regulatory end of the spectrum, however, the following questions must be considered:

- What, specifically is it that needs "fixing?" (Regulations tend to focus on outcomes, so desired outcomes should be clearly formulated.)
- Are there other alternatives available?
- What will the cost side of a regulatory solution entail and is it commensurate with benefit?
- Will the regulation actually achieve the desired affect?
- Will the regulation be implemented in a way that does not overlap or conflict with other regulations?

Regarding the last point, a nightmare regulatory scenario is one in which

- each domain in which a company does business imposes slightly different regulatory constraints on products
- the regulatory remedy becomes an expensive compliance exercise that only benefits auditors or testing entities and

- security is not actually better, or money is actually diverted from security to focus on compliance with a duplicative and wasteful regulatory structure

(For example, while drug approval is a necessary step before introducing a new drug into the market, having *each* of 50 states require a separate drug testing process prior to acceptance will likely not lead to safer drugs, just more expensive ones.)

Focus Demand: On the other end of the solutions spectrum - using market forces to correct the market - a large customer sector, such as the US federal government acting collectively, can move the market by demanding more secure software. "Demand more secure software" can occur by a number of means. One of these is asking for more transparency from suppliers in terms of their secure development practices. The benefit or "market remedy" of this approach is that:

- customers can make better risk-based procurement decisions if they know what the vendor did and did not do in terms of secure development practices, including disclosing the governance structures the vendor has in place to validate that they do what they say they do²
- the mere fact of asking suppliers for more transparency in secure development processes (especially with specificity around those practices) will "signal the market" that security is a purchasing criteria and likely increase the focus on security among suppliers to the Federal government
- suppliers who improve their security practices for the Federal government will not deprecate those practices for other market sectors

Incentivize Suppliers. Another means of correcting market imbalance and raising the bar on security are programs that put systemic and repeatable costs back on suppliers, such as the Federal Desktop Core Configuration program. That is, if a supplier can do once (provide a secure configuration out of the box) what customers would otherwise do repeatedly (securely configure multiple instances or installations of products), the cost argument is all in favor of the vendor "securing once," and consumers "consuming securely" multiple times. Note that FDCC-like programs also require governance structures to make sure secure configurations are developed

² If vendors are not honest about their secure development practices (e.g., on RFPs) the penalty for this could include fines or being banned from future procurement. Extensive "development practice" audits are a possible verification mechanism too, but there is no structure or entity capable of this at present. Greater transparency may raise the overall "security worthiness" bar on commercial software but will likely not raise the bar to the assurance level required for most classified systems, since that is a small market segment within the overall Federal government market and there is otherwise insufficient market demand for high assurance systems.

multilaterally instead of bilaterally, have change control on fixed schedules, allow phase-ins (and are not applied retroactively), and so on.

7 Results and Recommendations

Working groups were asked to focus on identifying specific actionable steps: the “how” to achieve the vision. While the workshop was divided into four working groups, there was no attempt to subdivide the problem space or artificially constrain any one group. The use of parallelism around several postulated questions and topics allowed for maximum creativity while developing results while providing a unifying framework for all involved.

Working groups were tasked with creating two types of recommendations initially framed as direction to create a set of capabilities or functions, and then to map the “capabilities” into the end states. Working group results tended to fall into one of two high level sets of recommendations. 1) those in the area of high level strategic or policy recommendations and 2) those of a more technical nature.

Below we provide the summary of policy and strategy recommendations followed by discussion of technical approaches and mechanisms necessary to achieve our vision.

7.1 Policy and Strategy Recommendations

The United States must develop a set of top-down cohesive strategies involving national agencies and departments as well as the private sector to address the issues associated with its reliance on computer systems. It must also include its effect on the global economy. This strategy must force a paradigm shift to address the motivations of an attacker not simply define security techniques. Focusing on techniques leads to point solutions that may not be applicable to the diversity of systems that need to be protected. Recovery must be part of the plan. These policies may be regulated, but must involve a public-private sector due to ownership, expertise and since the private sector will be an affected party. The strategy must also provide boundaries within the cyber realm and create a new set of guidelines for acceptable cyber behavior. This strategy would create a foundation we can build upon. To achieve this vision, the working groups recommended new policies and strategies for the nation and described how they contribute to the elements of a national cyber-security plan.

1. National Cyber Recovery Plan

The Federal Government should develop a National Cyber-Recovery Plan to define how the nation will recover from large-scale cyber-attacks on critical infrastructure. This plan would be similar in scope to the civil defense plans developed during the Cold War to define the response to a nuclear attack. The plan would be a living document; a small, task-oriented organization would be charged with developing it and keeping it up-to-date. Extensive industry involvement

would be required to assure the realism and effectiveness of such a plan. The plan would describe the successive phases of action to be carried out by the Federal Government and by the key critical infrastructure corporations in the event of a massive cyber-attack. It would outline how the various government departments and industry sectors would work together to restore vital supplies and services as rapidly as possible. An important component of the plan would be actions to provide adequate information to the public and to restore public trust. The plan would include guidelines for the general public, providing them with advice on how to cope with shortages and other problems such an attack could cause. It would also tell people how they could best help their fellow citizens in such an emergency. The development of this cyber-recovery plan would require only modest funding, but it could potentially suggest ways to improve responses that would eventually require additional resources. The overall planning effort would need to be accompanied by a mandate for distributing the plan and for carrying out exercises that would help the country learn how to apply the plan.

2. Presidential Cyber-Response Plan

The White House should develop a Presidential Cyber-Response Plan for dealing rapidly with a major cyber-attack. Unlike the “National Cyber Recovery Plan”, the “Cyber Response Plan” is tactical in nature and is expected to take effect immediately following the detection of a large scale cyber attack. It is very important that the response to a large scale cyber-attack be worked out in advance in considerable detail, so that the necessary emergency actions could be carried out extremely rapidly. The response plan would need to define the successive stages of action and information gathering, and the deciding factors at each juncture. The response scenarios would need to incorporate assessments of the degree of confidence that could be placed on the developing situational awareness. There would need to be specific measures for coordinating with industry. The plan would need to describe the application of emergency powers, possible martial law, and potential military actions. It would need to take account of relations with allies and with other foreign powers. The overall response plan would not be effective if it were developed in a manner that was piecemeal, ad hoc, and secret. To truly serve the country, the cyber-response would need to be policy-based and to some degree a matter of public declaration.

3. National Cyber Command and Authority

The President should create a new high level Cyber Command Authority that will direct national cyber-security measures. This should be a new entity supported in law and by executive order, with the required budgetary control and executive power to effect changes and implement policies related to strategic and operational aspects of cyber-security. It should operate outside of the old nuclear planning agencies and the existing federally funded research and development centers. The National Cyber Command and Authority should maintain a permanently funded and routinely re-constituted think tank composed of distinguished members with extensive experience in industry, academia well as various branches of the government, to receive inputs on operational and strategic policies. The National Cyber Command and Authority should also

provide industry with an expert group, midway between the government and the private sector, with whom they could have high-level, but actionable discussions.

4. Cyber Security Rating Institution

The Federal Government should establish an official institution, possibly with some legal protection, for rating the cyber-security of commercial over-the-counter software. The ratings provided by this institution would be analogous to automobile crash ratings, energy efficiency ratings, and nutritional ratings. The ratings should be supported by scientific measurement technologies, including automated tests, that would evolve and be constantly improved over time. The ratings would be acknowledged to be partial, but still useful as broad indicators. The testing and the publication of the results would initially be implemented gradually or in phases, so that the market consequences could be gauged and adjusted. The ratings should be expressed in a simple, numerical scale, easy for consumers to understand. Publishing the ratings on software labels and packaging would be mandatory. Product ratings would be voluntary, but unrated software would have to be labeled “cyber-security unrated.”

5. Economics and Cyber Security Planning

The Federal Government should make the economic context of cyber-security innovations a part of all planning and R&D. This means that all proposed technologies, regulations, and cyber-security policies should be considered from the standpoint of cost-effectiveness and possible market forces. It means that all cyber-security metrics should consider economic consequences before being used as a guide for action. It means that the causes and remedies for cyber-security market failures should be investigated and considered wherever these are a component of the existing problems. If economics is made a component of cyber-security planning, one consequence is that more consideration would be given to changes in production processes that could reduce the consequences of cyber-attacks. This would allow cyber risks to be reduced by making industries more resilient, rather than simply by deploying more cyber-security tools. The broader consequence is that the most cost-effective (and *only* the most cost-effective) cyber-security measures would be developed and applied.

6. Academics and Cyber Security

The Federal Government should offer sustained funding to academic programs that help to meet national cyber-security needs. In particular, certain urgently needed types of cyber-security awareness education, and training should be mandatory within all academic institutions that receive Federal support. Academic institutions should be incentivized to include secure coding practices into the curriculum of every computer science degree program. Inclusion of business context and business uses of information systems, as a part of curriculum of all computer science and cyber-security programs should be strongly encouraged and incentivized. Secure system engineering, including system failure analysis, should be a recognized discipline in every institution providing computer science education and training. Finally, as a complement to these

educational initiatives, the Federal Government should provide employment incentives that will increase the portion of American citizens in computer science and cyber-security graduate programs.

7. Advanced Research in Cyber Security

The Federal Government should fund advanced research in cyber-security that augments defensive as well as offensive capabilities and its policies of use. This should not only include innovations in hardware and software that would enhance defensive capability, but also research into offensive actions that could be carried out to stop or reduce the consequences of cyber-attacks, despite the likelihood of causing collateral damage. These offensive measures would not be intended as tools for retaliation or deterrence, but as a practical option for preventing further damage and value destruction due to an ongoing cyber attack.

The next section provides a list of necessary technical approaches and mechanisms that need to be developed in order to achieve the goal of cyber-security at a national level.

7.2 Recommended Technical Approaches and Mechanisms

Working groups recommended new technical approaches and mechanisms and described how they contribute to the elements of a national cyber-security plan. Below is a list of necessary high-level classes of approaches and technical mechanisms that need to be developed in order to achieve our vision are described.

1. Supply Chain Security Assurance

Hardware, firmware and software are the building blocks for cyber systems, and these building blocks must be developed and managed so that it is possible to have confidence in their integrity, not only as delivered, but also as they evolve. Throughout the lifecycle of each product and system, from inception through retirement, there are opportunities for the introduction of exploitable flaws and unintended functionality. Techniques to mitigate lifecycle threats posed through reliance on an untrusted supply chain must be adopted to improve product development, delivery and updates. A set of processes and policies focused on lifecycle assurance should be used to lessen and mitigate intentional and unintentional harm. In many cases, a hardware-based root of trust could enable detection of tampered software. Additional methods to provide tamper resistance and tamper detection for hardware, firmware, software, and services need to be identified, formalized through international standards, and automated. These methods, combined with cyber-security-focused courses and curricula, will teach and train the OEM workforce to develop systems in the supply chain that are more difficult for adversaries to exploit.

2. Security Modeling (unclassified technology).

To secure critical systems, we must understand and measure the security characteristics of their components and their connections as well as the security principles the overall system must

uphold. In the past, industry has successfully measured the functionality, performance and reliability of products. Today, that is not enough. Security understanding and measurement can be achieved through defining and modeling a system and its components as well as how they are used. Testing components can always be done in an unclassified way. Measuring a system's security characteristics can use similar techniques but the results may be sensitive if they reveal residual vulnerabilities of a critical system. When critical systems are constructed, the results of modeling and testing the system as a whole may be sensitive. The techniques used for the modeling and testing, however, can often remain unclassified.

There are at least three levels of modeling to consider: (1) Systems modeling; (2) Sub-systems modeling; and (3) product modeling. Product modeling is completed by the originating vendor(s). It tests the product to see if it works as designed and assures its resistance to known vulnerabilities and attacks. Sub-systems modeling is undertaken by either industry sectors collectively or in partnership with government. Sub-systems are tested for interaction and exploitable vulnerabilities resulting from compositions of products. This means addressing the boundary cases where attackers often find vulnerabilities. Systems modeling is a scaled version of a fully working process for an industry that tests the entire system to determine interdependencies and systems weaknesses.

Each model level should be tested as the system is built or integrated. The earlier in the life-cycle of the systems development such testing is conducted, the more likely the results will be unclassified. We intend that the model testing methodologies remain unclassified, yet we would allow models and analyses of specific systems and properties to be classified as needed.

To accomplish security assurance through modeling, at least four capabilities are essential. All exist today and can be used, though advancement in these capabilities would likely bear significant fruit. These four areas are (1) theory, (2) simulation/emulation, (3) health modeling—functionality, and (4) and predictive what-if scenario analysis. For theory, there exists a significant body of work that needs to be collected and applied for establishing near term capabilities, modeling advances are needed for more sophisticated modeling, including an algebra for composition of security properties. Simulation and emulation capabilities are needed because designs need to be analyzed in the abstract before the expense of implementation and because the systems to be analyzed are too complex to understand without the abstractions that simulation and emulation provide. Because security properties depend on the health of the system, particularly to measure denial of service and to measure the functioning of the security components, system health modeling and continuous assessment is a key capability. Knowing exactly what to model and the best way to respond to ill-health are hard issues that need further investigation. To use modeling and simulation technology effectively, designers and operators must be able to explore possibilities with minimum cost and calendar time. A few isolated models exist today to begin to allow this type of predictive analysis as part of a design process

for limited properties. These capabilities should be expanded and techniques such as strategic attack scenario analysis and operational counter-measure defense scenarios should be supported.

3. Quantifying Problems/Impact

There is not a common basis for understanding how bad things can become during a cyber attack. Expert testimony in various fora varies widely in the assessment of damage and value destruction due to cyber attacks. If the government wants private sector help, it must work to articulate with high credibility specific strategic damage levels that are possible to critical information-dependent infrastructures and how the private sector can best help mitigate these risks. The responsibility to make this case clear is not the private sector's, but rather one for which the government needs private sector input and response on. A program to address these vulnerabilities includes government funding for research on how to provide this quantification as well as government provision of materials for academia, to instruct students can learn from these case studies and are better prepared to defend the country

4. Build Industry Support for Proactive Positioning

Today, cyber defense is largely a matter of reaction -- installing firewalls, patches, antivirus signatures, intrusion detection/prevention systems. To reach our goals, defense must assume a more active role. The steps required to accomplish this center around fostering businesses to profit from security capabilities and a strong culture of protecting proprietary customer information. Such a culture drives technology and policies around anonymity services and policies that protect privacy (no over-exposure of information) and require technical advances in the development of trustworthy and unspoofable identities. It will be necessary to change user expectations for minimally invasive security mechanisms to a market for identity assurance.

In this environment, value creation will stem from identity assurance and attribution and companies will gain reputation through cyber-security conscious behavior and associations. In addition to these cultural changes it will be necessary for industry and government to develop dual-use standards (defense and offense) so that cyber technology can be used to inform a defense though better understanding of the offense. This may require legal relief for government access to needed information and dual use capabilities.

To prepare for the possibility of a catastrophic large scale cyber attack, it is recommended that we explore models for using the industrial base for fighting back. In this instance it would be necessary to find a way for the government to disclose certain information so that the industrial base can help. In this context, there are questions to investigate associated with what industry needs to do to help explicitly rather than implicitly. It must be noted that one of the great challenges for any sort of offense includes attribution. Attribution is multi-faceted and must include:

- Traffic History/Traffic Analysis to figure out who is doing what

- Understanding of the flow of resources and information and dependencies
- Ability to create a map of how resources are interdependent in order to determine critical dependencies

It is necessary for large scale systems to be designed based on the application of policies based on identity and reputation that are designed for resilience and active response. Along with policy, cultural and technical advances in these areas, comes the need to create models and metrics for proof of trust among entities.

5. Develop Policies and Mechanisms for Operation Under Mutual Suspicion

Globalization has led to a world in which more and more components of the critical infrastructure, including software, and hardware, during design, development, manufacture and operations interact at various phases of the infrastructure lifecycle, with entities that may not be entirely trustworthy. There exists a tussle between economic incentives and security goals. Hence it is necessary for segments of critical infrastructure to change their orientation to one of operating under mutual suspicion. In order to do this it will be necessary to strengthen the private sector interactions (e.g., supply chain, collaboration), define privacy policies for controlled information sharing, define requirements for coalition in operations and develop dynamic policies for information, infrastructure, and identity.

6. Relational Trust Mechanisms (processes and tiering of effort/response.)

We must develop the institutions, policies and mechanisms to enable information sharing, coordination and collaboration between organizations, people and systems. This will allow more situational awareness within our infrastructure as well as across organizations needed to support our infrastructure. Not all ‘players’ are actors in responding to issues because most are users (consumers, implementers) of IT vice actors (creators, designers, OEM) of IT / services. Interaction ranging from sharing to collaboration is based on levels of relationships. Relationships over the course of time increase and/or decrease the amount trust accorded to the group based on necessity, value and experience within and through the relationship. Following is a list of mechanisms ranked from basic to more complex:

- Information sharing – is normally the transfer of information from one entity to others towards a common goal, with almost no engagement between the parties involved
- Coordination – is the give and take usually between two or more entities for a common goal or situation, usually of short duration
- Collaboration – is the processing and analysis of information and/or data to solve common issues while achieving long-term goals over a longer time. Collaboration requires an automated collection of data to support the collaboration (not necessarily

shared between all parties). This automated collection develops the real technical basis of normal to above/below normal trends and the collaboration on what it means leads to the interpreted (synthesized) meaning of the automated collections.

- Situational Awareness – situational awareness is what you gain from information sharing through collaboration over a period of time. Situational awareness is more useful and productive in collaborative activities than those involving coordination or sharing as the interpreted meaning of data extracted by collaborative networks may encode early warning indicators future cyber-attacks and trigger points for coordinated action.
- Early warning/pre-attack reconnaissance – is enabled through situational awareness and collaboration to ensure fuller knowledge and unique partner expertise. No one organization can or should have full knowledge.

7. Education, Training and Human Resource

With commercial products being designed, manufactured, integrated, deployed and maintained by an international work force, and with security as a global property of systems, all the organizations and people involved with IT products must understand, appreciate and maintain a level of security assurance commensurate with the requirements these products are intended to meet. To maintain this competence requires training and retaining an international workforce and dispelling the perception that the offshore development thus enabled, threatens US engineering jobs. Early systematic education at the national and international levels about security design principles, security versus usability tradeoffs, in combination with security research and implementation methods to develop secure systems, would build from the ground up a workforce that can appreciate, understand and construct secure systems. Frequent re-examination of professional certification programs would enable cyber-security professionals to keep up with the ever changing security landscape and rewards for professionalization would incentivize people to keep their certifications up to date. In a global supply chain, assurance guidelines for COTS products based on how they were developed rather than who or where they were developed would be easier to enforce, thus bringing global supply chain assurance one step closer to reality.

Overclassification limits the quality and benefits of research, because it limits both the pool of researchers available to pursue it and the range of systems to which it can be applied. The government should foster sustained, unclassified joint Government (e.g., CAEIAE) and industry (e.g., SafeCode) partnership programs with educational institutions. Such programs help align university curricula and research with dynamically changing national needs.

8 Summary

A Citizen-led National Cyber Defense Initiative (NCDI)-Industry workshop was held in November 2008. The workshop had representatives from the leading commissions and working groups chartered by various government organizations, and a balance of industry leaders and academic researchers. The workshop provided a forum for members of the computing and communication industry to contribute input to multiple planning and strategic efforts underway and to define actionable plans to take back to their organizations. The recommendations of this workshop reflect the participation of key industry leaders and the meta-level recommendations of an economics driven strategy.

The key recommendations from the workshop fall into two broad areas: strategic policy and technical mechanisms. Foremost in the strategic policy area are specific recommendations to create national strategy, national response and recovery, and command authorities analogous to U.S. national strategies around nuclear defense during the height of the Cold War. These organizational strategic recommendations are supported through strategic recommendations for national-level cyber infrastructure measurement, economic based consequence analysis, and vigorous programs for the nation's academic leaders and researchers. Again, analogies to the nation's strategic initiatives during the cold war apply to the academic and research initiatives proposed here.

Complementing the strategic policy-focused recommendations are technology-focused recommendations. These are recommendations to research, develop, and implement technological approaches to the protection of information systems, approaches that must stay ahead of the competing, threatening technology that would exploit and corrupt those systems if it could. Key technology recommendations include mechanisms for modeling security, trust relations, attribution, techniques for supply chain assurance and techniques for quantifying problems and impacts. These technology recommendations are supported by recommendations for technical cultures and society that include proactive security management, an operational environment based on mutual suspicion and security technology as a key component of commercial products.

Mapping the recommendations of this workshop for policy, strategy, technology, mechanisms and a technical culture of security awareness to the desired end-states recommended by a previous NCDI workshop, provide an initial road map towards the goals of:

Over the next ten years transform

- **the cyber-infrastructure to be resistant to attack so that critical national interests are protected from catastrophic damage and our society can confidently adopt new technological advances.**

- **the workforce and organizational culture aligned to design, develop, integrate, maintain secure critical infrastructure on an ongoing basis.**

Appendix A Mapping policy and technical recommendations to end states

Section in document		Continuity of Critical Information Infrastructure Operations	Protect/Defend Critical Assets from Strategic Damage	Local/Global Cyber Situation Awareness	Data-Tight Systems	Extensible systems that safely embrace new technology	Quantifiable security and dependability (D =dependency)
Section 7.1	1. National Cyber Recovery Plan	X	X	X	X	X	X
	2. Presidential Cyber-Response Plan	X	X	X			X
	3. National Cyber Command and Authority	X	X	X			X
	4. Cyber Security Rating Institution				X	X	D
	5. Economics and Cyber Security Planning		X			X	X
	6. Academics and Cyber Security				X	X	X
	7. Advanced Research in Cyber Security	X	X	X	X	X	X

Section 7.2		Continuity of Critical Information Infrastructure Operations	Protect/Defend Critical Assets from Strategic Damage	Local/Global Cyber Situation Awareness	Data-Tight Systems	Extensible systems that safely embrace new technology	Quantifiable security and dependability (D =dependency)
	1. Supply Chain Security Assurance				X	X	X
	2. Security Modeling (unclassified technology).			X			
	3. Quantifying Problems/Impact			X			X
	4. Build Industry Support for Proactive Positioning		X	X		X	D
	5. Develop Policies and Mechanisms for Operation Under Mutual Suspicion	X	X	X	X	X	D
	6. Relational Trust Mechanisms (processes and tiering of effort/response.)	X	X	X	X		X
	7 Education, Training and Human Resource	X	X		X	X	D