Project 12 Report: Improving Protection of Privately Owned Critical Network Infrastructure Through Public-Private Partnerships

Project 12 Report: Improving Protection of Privately Owned Critical Network Infrastructure Through Public-Private Partnerships

Table of Contents

Project 12 Report: Improving Protection of Privately Owned Critical Network Infrastructure Through Public-Private Partnerships

Executive Summary

The United States relies on critical infrastructure and key resources (CIKR) for government operations and the health and safety of its economy and its citizens. The President issued National Security Presidential Directive 54 (NSPD-54)/Homeland Security Presidential Directive 23 (HSPD-23), which formalized the Comprehensive National Cybersecurity Initiative (CNCI). NSPD-54/HSPD-23 directs the Secretary of Homeland Security, in consultation with the heads of other Sector-Specific Agencies, to submit a report detailing the policy and resource requirements for improving the protection of privately owned U.S. critical infrastructure networks. The report is required to detail how the U.S. Government can partner with the private sector to leverage investment in intrusion protection capabilities and technology, increase awareness about the extent and severity of cyber threats facing critical infrastructure, enhance real-time cyber situational awareness, and encourage intrusion protection for critical information technology infrastructure."

Under the auspices of the Critical Infrastructure Partnership Advisory Council (CIPAC) and the National Infrastructure Protection Plan (NIPP) Partnership Framework, the Department of Homeland Security (DHS) formed a private-sector CIKR owner and operator working group to respond to this tasking. Private-sector input proved critical to appreciating the scale and scope of the task and in developing a set of actionable recommendations that reflects the reality of shared responsibility between the public and private sectors with respect to securing the nation's cyber assets, networks, systems, and functions.

The public and private-sector CIKR communities recognize that the challenges are significant, the threat is present and growing, and immediate proactive action must be taken. As such, this report includes short-term recommendations, often building upon accomplishments and activities already under way and existing trusted relationships with CIKR organizations. The report identifies an aggressive series of milestones that will result in tangible progress over the next year. For each recommendation, efforts should be made to investigate and leverage ongoing activities and, where appropriate, avoid creating new projects or working groups when one already exists.

Some recommendations within this report represent long-term objectives, with many requiring detailed legal and policy analysis, as well as advanced interagency planning and coordination. In some of these cases, feasibility studies, analysis, and additional investigation are needed. In addition, an integration and management process will need to coordinate efficiently among the various related efforts.

Building on the accomplishments of the NIPP framework, the U.S. Government and the private sector can improve CIKR cyber network and system security through partnership. Each has situational awareness that can inform the other's risk-based decisions. While existing public-private partnerships have facilitated information sharing and policy coordination to address these

obstacles, more can be done to improve the security and resilience of CIKR networks. A focus on partnering to assess and mitigate CIKR cyber risk would benefit both sides and provide for a more secure cyber infrastructure. Such a partnership could include the appropriate sharing of capabilities in addition to information. If solutions are to be found for securing the nation's CIKR networks against the complex, sophisticated, and growing cyber threat, industry and government must work as partners. Government must continue to consider private-sector value propositions when developing joint measures to improve the security of privately owned U.S. critical networks to ensure buy-in and active engagement.

This report represents a new level of cooperation between government and industry in identifying gaps in cybersecurity and information sharing and suggesting ways to address them. The U.S. Government should continue this work and jointly establish a clear value proposition with private-sector CIKR owners and operators for integrating cybersecurity into the enterprise risk management process. Such a value proposition, promulgated through outreach and awareness activities on threats and the importance of enterprise risk management from a cybersecurity perspective, as well as on market incentives where appropriate, can be used to encourage additional private-sector investment in cybersecurity.

The recommendations that follow provide a path to improve U.S. CIKR cybersecurity. A combination of planning and pilot programs is intended to build confidence over time and to allow course corrections to change with the dynamic cyber environment. These recommendations include:

- Develop a plan to identify specific goals and outcome metrics related to securing CIKR sector networks.
- Promote current public-private cyber information sharing efforts via the NIPP Framework by fostering trust through consistent and timely communications and consensus building.
- Develop a plan using the NIPP Partnership Framework to include the CIKR sectors into ongoing CNCI efforts.
- Leverage existing frameworks to develop, as appropriate, new vehicles, rules, and instruments between public and private sectors to improve sharing of actionable cyber information.
- Scope the requirements for implementing real-time cyber situational awareness.
- Evaluate the feasibility of sharing Federally developed technology capabilities with CIKR.

  - Expedite the TS/SCI clearance process for appropriate private-sector representatives for when "tear-line" unclassified cybersecurity documents are not available.
  - Enhance information sharing and analysis organizations, whether information sharing and analysis centers (ISAC) or other information sharing organizations (ISO), to make them the focal point of cyber operational activity with the 18 CIKR sectors.
  - Enhance information sharing mechanisms to provide an environment in which technological barriers do not impede cyber information sharing processes.
- Expand US-Computer Emergency Readiness Team (US-CERT)/National Coordinating Center for Telecommunications (NCC) joint operational capabilities to include private-sector CIKR participation to enhance CIKR real-time situational awareness.
- Establish a mechanism to give companies opportunities and incentives to invest in R&D and—based on legal, security, and investment-level criteria—potentially allow companies to obtain intellectual property rights to the results of government-funded or government-partnered cybersecurity R&D.
- Investigate new ways to drive improvement in the cybersecurity posture within the private sector in those cases where market forces yield an insufficient value proposition.
- Investigate methods to encourage cybersecurity across the business community nationwide similar to those used within private-sector CIKR.

Project 12 Report: Improving Protection of Privately Owned Critical Network Infrastructure through Public-Private Partnerships

I. Introduction

The United States relies on critical infrastructure and key resources (CIKR) for government operations, a vibrant economy, and the health and safety of its citizens. The President's July 2002 National Strategy for Homeland Security states:

> Government at the Federal, State, and local level must actively collaborate and partner with the private sector, which controls 85 percent of America's infrastructure. The nation's infrastructure protection effort must harness the capabilities of the private sector to achieve a prudent level of security without hindering productivity, trade, or economic growth.

With this strategy serving as a guiding principle, the President issued National Security Presidential Directive 54 (NSPD-54)/Homeland Security Presidential Directive 23 (HSPD-23), which formalized the Comprehensive National Cybersecurity Initiative (CNCI). This effort, referred to as "Project 12," responds to the direction in NSPD-54/HSPD-23 for a report detailing the policy and resource requirements for improving the protection of privately owned U.S. critical infrastructure networks.

Under the auspices of the Critical Infrastructure Partnership Advisory Council (CIPAC) and the National Infrastructure Protection Plan (NIPP) Partnership Framework, the Department of Homeland Security (DHS) formed a private-sector CIKR owner and operator working group. Private-sector input proved critical in enabling DHS to appreciate the scale and scope of the task and in developing a set of actionable recommendations that accurately reflects the reality of shared responsibility between the public and private sectors with respect to securing the nation's cyber assets, networks, systems, and functions. CIPAC members generously supported DHS with their time, expertise, and candid expressions of views.

The Risk Posture

Both public and private-sector information systems manage risk to their operations through constant monitoring and mitigation activities designed to prevent daily incidents from becoming significant disruptions; however, the growing threat requires a more thorough examination of risk to the cyber infrastructure and the associated implications for cybersecurity. As criminal exploits proliferate, nation states are realizing that criminal hacking tools, methods, and tactics offer asymmetric opportunities for espionage, countering military force, and for economic and geo-political advantage. This increasingly malicious and pervasive threat, coupled with insider threats and the spectrum of other threats facing critical infrastructures, illustrates the need for system-wide risk management, including enhanced threat information sharing by the U.S. Government and bi-directional vulnerability and incident reporting between the U.S. Government and the private sector to improve prevention, response, and recovery capabilities. Facilitating enterprise-wide cyber risk management practices and increasing the flow of timely, actionable cyber information will support increased cybersecurity for CIKR. Improved processes, new incentives, and possibly some changes in the legal environment will help the private sector and the U.S.

Government protect the nation's networks and assist the U.S. Government's efforts to leverage private-sector technology and expertise for the greatest mutual benefit. Realization of this goal through improved processes and new incentives will help the private sector and the U.S. Government protect and strengthen the nation's networks and assist the U.S. Government efforts to leverage private-sector technology and expertise for the greatest mutual benefit.

Overview and Scope

Project 12 asks one fundamental question: "How can government work with the private sector to enhance the security of the CIKR networks?" Some related topics are the primary focus of other CNCI areas and, therefore, are not discussed in detail here. In particular, the topics of cyber research and development (R&D) and cybersecurity "leap-ahead" technologies are the focus of other CNCI efforts.

The public and private-sector CIKR communities recognize that the significant challenges and the growing threat require immediate and proactive action. This report includes short-term recommendations, often building on accomplishments and activities already under way and existing trusted relationships with CIKR organizations. The report identifies an aggressive series of milestones that will result in tangible progress over the next year. Where applicable, these activities should build on existing security and assurance efforts across the cyber infrastructure to increase resiliency and operational capabilities throughout the CIKR sectors. For each report recommendation, efforts should be made to leverage ongoing activities and, where appropriate, avoid creating new projects or working groups.

Some recommendations within this report represent long-term objectives that require detailed legal and policy analysis, as well as advance planning and coordination. In some of these cases, feasibility studies, analysis, and additional investigation are needed. In addition, an integration and management process will be needed to coordinate among the various related efforts.

Value Proposition for the Private Sector

Building on the accomplishments of the NIPP framework, the U.S. Government and the private sector can improve their CIKR cyber network and system security through partnership. Each has situational awareness that can inform the other's risk-based decisions. While existing public-private partnerships have facilitated information sharing and policy coordination to address these obstacles, more can be done to improve the security and resilience of CIKR networks. A focus on partnering to assess and mitigate CIKR cyber risk would benefit both sides and provide for a more secure cyber infrastructure.

Such a partnership could include the appropriate sharing of capabilities in addition to information. If solutions that do not undermine the primary functions of cyber infrastructure are to be found, industry and government must work as partners. Government must continue to consider private-sector value propositions when developing joint measures to improve the security of privately owned U.S. critical networks to ensure buy-in and active engagement.

This report represents a new level of cooperation between government and industry in identifying gaps in cybersecurity and information sharing and suggesting ways to address them. DHS believes that the U.S. Government should continue this work and jointly establish a clear value proposition with private-sector CIKR owners and operators for integrating cybersecurity into the enterprise risk management process. Such a value proposition, promulgated through outreach and awareness activities on threats and the importance of enterprise risk management from a cybersecurity perspective, as well as on market incentives where appropriate, can be used to encourage additional private-sector investment in cybersecurity. Throughout this report the value proposition for private-sector participation is used to guide realistic and actionable policy recommendations.

Desired End State of Public-Private Partnerships

The goal of this effort is to foster a level of cybersecurity commensurate with the associated risk to a critical infrastructure, with the understanding that a single approach will not satisfy the unique needs of all U.S. CIKR sectors. Information sharing mechanisms will facilitate this desired end state.

Increased CIKR cybersecurity can be achieved with two complementary approaches:

1. Strategic assessments of vulnerabilities, threats, and mitigation strategies; and

2. Focus groups to study and develop recommendations on sector-specific needs as well as technology specific needs, including R&D requirements.

Continuous bi-directional provision of threat information must afford CIKR sectors the opportunity to improve and measure their cybersecurity posture based on evolving threat information. Similarly, information on network activity and security issues passed from the CIKR sectors to government would enhance the threat information provided to the CIKR sectors. Cleared private-sector individuals representing each CIKR sector must have the ability to access and leverage the most recent relevant threat information through an information exchange mechanism that is not impeded by technological barriers and that is truly bi-directional. The U.S. Government must provide cyber threat and vulnerability information to industry at the lowest possible classification level while retaining the essential elements of actionable information necessary for information security purposes. The U.S. Government should institute a mechanism for CIKR sectors to provide feedback regarding the degree to which the threat information is timely, relevant, actionable, and leads to success (for example, blocked intrusion attempts). Likewise, industry should set up a mechanism to accept feedback from the U.S. Government and contribute to the U.S. Government's ability to produce meaningful and actionable threat information. In addition, recipients of threat information in the CIKR sectors must understand information flow across their business enterprises and exercise caution with respect to who will have access to that information.

Threat and vulnerability information sharing should include strategic and tactical analytic products by the homeland security, law enforcement, intelligence, and military communities that are relevant to the cybersecurity requirements of the nation's CIKR and are accessible to sector CIKR representatives, as appropriate.

The U.S. Government, in conjunction with the CIKR sectors, must establish criteria to measure the value of the information being shared. By establishing feedback mechanisms that determine whether shared information is making CIKR more secure, the U.S. Government can better manage the flow and improve the subsequent value of the exchange.

Long-term metrics and short-term metrics can be established to determine the value of both strategic and tactical information being shared. Strategic assessments may help shape policy and shift enterprise resources to prepare for anticipated cyber threats. In contrast, tactical assessments may help an organization make immediate changes to operations and its security posture.

The recommendations that follow provide a path to establish mechanisms to improve U.S. CIKR cybersecurity. A combination of planning and pilot programs is intended to build confidence over time and to allow course correction to change with the dynamic cyber environment.

Enduring Security Framework

This report focuses on both near- and long-term actions specifically focused on the task of identifying policy and resource requirements for improving the protection of privately owned U.S. critical infrastructure networks. Other critical aspects of the CNCI and the nation's cybersecurity strategy require partnership with industry, including those that focus on strategic long-term issues. To address some of these

long term issues, and building upon the frameworks and recommendations outlined in this report, as well as in the Supply Chain Risk Management Plan, the Deputy Secretaries of Homeland Security and Defense along with the Director of National Intelligence, established the "Enduring Security Framework (ESF)." The ESF will engage industry leaders under the DHS NIPP structure, leveraging the CIPAC framework. Under the ESF, the U.S. Government and corporate executive and operations officers from the Defense Industrial Base and Information Technology Sectors will discuss problems that impact national security and the ability of the U.S. industry to maintain their competitive advantages in world markets including technology, architecture, and policy issues. Membership in the ESF may be extended to other sectors as it matures. These discussions will culminate in the development of policy recommendations.

II. Short Term Recommendations (less than 1 year)

Recommendation ST-1: Develop a plan to identify specific goals and outcome metrics related to securing CIKR sector networks.

Finding meaningful ways to measure cybersecurity across a sector, let alone across the nation, is extremely complex. Under the NIPP, each sector must develop risk metrics in 2009 that include cybersecurity. These metrics will be used to help quantify this complex problem and drive and track progress for the recommendations in this report. DHS intends to use the Cross Sector Cyber Security Working Group (CSCSWG) to work with and across the sectors to develop cybersecurity metrics to meet this need. The CSCSWG will work with other government departments and agencies to ensure that risk metrics are comprehensively defined and measurable from an interagency perspective. Discussions will address both industry concerns on the sensitivities of shared data and government difficulties to establish steady-state security goals and measures.

Milestones:

- Convene a CSCSWG subgroup to address this issue (October 2008).
- Identify sector-specific measures for inclusion in the 2009 Sector Annual Reports (June 2009).
- Begin to collect and report data against those measures in the 2010 Sector Annual Reports.

Resource Requirements: CIKR sector cooperation and engagement.

Recommendation ST-2: Promote current public-private cyber information sharing efforts via the NIPP Framework by fostering trust through consistent and timely communications and consensus building.

Private-sector companies and industry associations worked side-by-side with their government counterparts to write the NIPP, published in June 2006. The NIPP institutionalized the Sector Partnership Model—built around Sector Coordinating Councils (SCC) and their Government Coordinating Council (GCC) counterparts—enabling government and private-sector entities to collaborate on CIKR protection.

These councils of experts have gone on to develop and implement Sector-Specific Plans (SSP) for CIKR protection, and CIKR owners and operators are investing significant time and resources into their SCCs as well as SSP implementation activities. In addition, many sectors rely on information sharing and analysis centers (ISAC), designated information sharing organizations (ISO), or other established processes designed specifically to facilitate information sharing within the sector and with other trusted entities. As a result, SCCs and ISAC/ISOs have evolved into rich resources of operational, strategic, and policy-related expertise, adding value to other sectors and government partners at all levels. In addition, the Sector Partnership Model has resulted in trusted relationships between SCCs, GCCs, ISACs, and other security partners.

The NIPP Sector Partnership Model has promoted private-public partnerships and will be used as the primary method for information sharing between partners for CIKR protection activities. Public and private-sector security partners should continue to work together to raise the NIPP partnership model to a higher level of maturity. Information sharing partners under the NIPP framework will rely on the SCCs or sector-designated ISACs/ISO to address cybersecurity. The U.S. Government will rely on the SCCs for their sector-specific CIKR expertise, while the ISAC Council, the Partnership for Critical Infrastructure Security (PCIS), and the CSCSWG will be leveraged for expertise on cross-sector issues such as interdependencies, incentives, common sectoral issues, and information sharing. Within this NIPP structure, both government and industry partners recognize that the individuals who address cybersecurity within an organization may differ from those with physical security responsibility and expertise. Working within the NIPP structure, DHS and the Sector-Specific Agencies are working to ensure cyber communication and coordination is taking place with the correct individuals.

Other mature government-sponsored cyber information sharing mechanisms, such as the Federal Bureau of Investigation's (FBI) regionally based InfraGard program and the United States Secret Service regional Electronic-Crimes Task Forces (ECTF) will be assessed for coordination with the NIPP information sharing process.

Milestones:

- Finalize cyber information sharing mechanism mapping across CIKR sectors already begun under the CSCSWG (October 20,2008).

- Develop mapping and identify constituencies of other CIKR cyber information sharing mechanisms such as InfraGard and the ECTF (November 30,2008). Once this mapping is complete, it will be used by DHS organizations Intelligence & Analysis (I&A) and US Computer Emergency Readiness Team (US-CERT) to improve cyber information sharing with the sectors and will provide input for Recommendation ST-3 (vehicles and rules to improve information sharing).

Resource Requirements: To complete this task, each sector must recognize the need for a cyber information sharing mechanism and must acknowledge that cyber and physical security information may need to reach different individuals within the sector. Sectors vary in levels of organization, maturity, and funding for activities such as this one. Recommendation ST-7 (assess and enhance information sharing and analysis organizations) addresses this issue in more detail; however, engagement and buy-in from all sectors and government entities is a necessary resource to complete this task. At a minimum, this effort will seek to identify success stories from each of the sectors and make recommendations about whether best practices can be adopted and applied across different sharing mechanisms.

Recommendation ST-2a: Develop a plan using the NIPP Partnership Framework to include the CIKR sectors into ongoing CNCI efforts.

Some of the issues raised under Project 12 are primarily addressed through other efforts.

- Initiative 4 focuses on R&D for cybersecurity technologies. The R&D coordination report indicates that greater public-private coordination is needed to facilitate rapid identification and continuous evolution of cyber R&D priorities.

- Initiative 8 focuses on cyber education and training.

- Initiative 9 seeks to establish increased public-private coordination and cooperation in the development and deployment of "leap-ahead" technologies.

- Initiative 11 focuses on the need for a strong partnership with the private sector and supply chain operators to address vulnerabilities and risk management of the information technology supply chain.

There is a need for a plan in which the CIKR sectors, working through the NIPP Partnership model, can engage in appropriate activities across the CNCI, beyond those explicitly included within the scope of Project 12. Industry has equities and expertise that should be understood and incorporated across the CNCI. In particular, DHS will work with the Office of Science and Technology Policy as the leader for Initiatives 4 and 9 to ensure that OSTP receives the inputs, perspectives, and requirements identified in this report and can benefit from NIPP partners' expertise. DHS also will work with the various private-sector entities responsible for complying with information security statutes (i.e. financial, healthcare) that include an information security training component. The ESF, outlined in the introduction to this report, will provide an important venue for collaboration with NIPP partners under the CIPAC framework, to address long term strategic issues related to globalization.

In accordance with NSPD-54/HSPD-23, DHS intends to use the NIPP Partnership Framework to engage with CIKR on all aspects of the CNCI where CIKR input is relevant, feasible, and appropriate. DHS will work with its Office of General Counsel and consult with DOJ to ensure legal issues are considered. DHS has developed an engagement plan to include initial briefings on CNCI to PCIS/Federal Senior Leadership Council, all SCC/GCCs, and the ISAC Council to provide a baseline understanding of CNCI. Once a baseline has been established, work will begin to incorporate CIKR sector input into appropriate CNCI activities. DHS will work with the FBI and the Secret Service to provide briefings and engage as appropriate with InfraGard and ECTF members.

Milestone:

- Provide an updated engagement plan to Initiative leads for reference and coordination (November 15, 2008). The engagement plan will be updated as required. Briefings on CIPAC and NIPP framework will be provided to interagency partners as requested.

Resource Requirements: The NIPP Sector Partnership framework and CIPAC provide the needed mechanism for this interaction. The DHS Office of Infrastructure Protection and Office of Cybersecurity and Communications are resourced to support this interaction. The engagement plan will identify potential industry engagement in CNCI projects and propose a framework for that engagement. The full stand-up and operation of the ESF will require federal staffing, legal,

policy, and logistical contract support resources. DHS is prepared to dedicate the resources required for creation of an Executive Secretariat to support this effort.

Recommendation ST-3: Leverage existing frameworks to develop, as appropriate, new vehicles, rules, and instruments between public and private sectors to improve sharing of actionable cyber information.

For information sharing to be effective and actionable, clear policies and processes are necessary to determine how, when, and what information is shared between security partners. While many accomplishments have been made in developing a framework under the NIPP to communicate with industry, current operational capabilities do not uniformly support satisfactory cyber information sharing across the sectors. As such, it is imperative that government and private-sector security partners develop and implement agreements to facilitate effective cyber information sharing, leveraging existing frameworks, such as the NIPP or the Protected Critical Infrastructure Information (PCII) Program. At the most basic level, government and private sector must identify what information is needed by each party, how and when it will be shared and protected (in terms of both security and privacy protections), and what kind of feedback or response can be expected.

Information Sharing Requirements Collected from CIPAC Members:

These requirements reflect the views offered by private sector officials to DHS and should not be attributed to, or considered the official perspective of the U.S. Government.

For the selected vehicle to succeed, several key concerns and criteria for successful implementation must be considered, including:

- **Value Proposition.** Develop concrete benefits (such as advance notice of a threat, broader awareness of asset vulnerabilities, and opportunity to shape national policy) to encourage businesses to provide critical security information in real-time.

- **Formal Criteria.** Formal criteria for what and when information is shared, particularly relating to incident response and handling, is necessary to standardize sharing of information across government and private-sector security partners.

- **Criteria for Accountability.** Clear criteria are vital to assure that policy and procedural lapses are shown to have clear and certain consequences. These criteria must address the way information is collected, stored, moved, and retired throughout the data life cycle.

- **Unauthorized Sharing.** Che **U.S.** Government and private sector must prevent the passing of information, beyond the boundaries established by the original provider of the data.

- **Competitive Posture.** The private sector must be able to compete in the marketplace. A private-sector owner and operator routinely balances its need to remain competitive with the need to share sensitive information, aligned with the need to protect its own intellectual property, market competition, its customers, and its shareholders, as well as with regulatory obligations. Global organizations may encounter additional complexity.

- **Reach.** Cyber infrastructure permeates each of the **18** 6IKR sectors and sub-sectors, but the **U.S.** Government has differing levels of reach into each sector. As a result, not only is awareness of some sectors' cybersecurity posture inconsistent, inconsistent breadth and depth of information sharing occurs between industry and government in each sector. Not all sectors may require the same level of sharing, but some sectors still lack the operational ability to receive cyber threat information or to pass relevant data to the **U.S.** Government in a secure manner.

- **Continuous Feedback.** Both the **U.S.** Government and private-sector CIKR owners and operators need input on the value and use of the information being provided. This is an important component of the value proposition of information sharing. The NIPP risk management framework includes a feedback component for continuous improvement that should be used to promote information sharing effectiveness,

- **The Business Imperative.** Businesses exist in an environment of competition, a very different environment from that of most public-sector organizations. Consequently, businesses will behave very differently from public entities, gpr example, jeducing certain risks may be too costly for a business in a highly competitive environment, and the U**.S.** Government must understand that some risk will simply be accepted by most businesses. This creates a dynamic challenge of managing the risk dialog between government and private-sector organizations.

- **Legitimate "Need-to-Know" Restrictions.** The private sector must balance competitive issues with the need to share sensitive mfornation. Conversely, government organizations must also consider when it is necessary to restrict information to protect intelligence sources and methods.

- **Adherence to "Need-to-Share" Principles.** As indicated in the ***United States Intelligence Community Information Sharing Strategy,*** the U.S. Government, led by the Office of the Director of National Intelligence, is attempting to develop a culture supportive of responsible information sharing. The U.S. Government will need to provide a transparent process for explaining how it balances the "responsibility to share" with continued protection of sensitive intelligence sources and methods.

- **Relevance.** Some organizations may be further along than others in adopting newer techniques, operating models, or technologies. Therefore, what may be considered new and critical information by some companies may be "old news" or too basic for others. These differing experiences,, challenges, and maturity levels make it necessary for the U.S. Government to tailor the information to be shared.

- **Actionable Information.** Many industry representatives have articulated a need for actionable information to help them counter threats identified via the information sharing process. Without actionable information, private industry is leffein a quandary, having knowledge of potentially serious threats and increased risk without the ability to mitigate the risk.

- **Ability to Protect Sensitive Data.** Many industry representatives have expressed concern that government may not be able to protect sensitive private-sector information (such as details on vulnerabilities and compromises) under existing statutes and frameworks, resulting in exposure of data to competitors, the media, and adversaries. Private-sector entities may not have aeeess to or the ability to handle or store government sensitive information (intelligence, threat), resulting in delays in ttansrnitting specific threat information to the people that need it in the private sector. Such gaps should be considered under current frameworks or any future vehicles contemplated by this recommendation. Finally, both the U.S. Government and private sector may have specific privacy protection responsibilities which must be addressed as part of any policy and practice of sharing information.

- **Multinational Nature of the Private Sector.** Businesses operate in a global economy. Consideration*must be given to how best to share information when the private-sector organization is multinational, the recipients of information are not necessarily U.S. persons, and the corporation has offices and Operations in other countries.

Sector-specific agreements will vary to accommodate differing business models. These agreements should be developed to address the above requirements and considerations and to enable trusted information sharing under the auspices of the NIPP framework. In addition, each agreement should recognize that information of varying levels of sensitivity will be shared and may require different categories of security marking and dissemination controls. Agreements, once developed, will incorporate reference to the Controlled Unclassified Information (CUI) directive but must also recognize and provide rules of engagement for information sharing before the CUI program is fully defined and implemented. For example, the Defense Industrial Base Cybersecurity/Information Assurance (DIBCS/IA) Program's framework agreement establishes processes for trusted information sharing between government and industry and provides signatories with detailed handling and marking guidance in the accompanying DIB/CS/IA Security Classification Guidance. Rules of engagement will need to acknowledge the international nature of industry and must address not only the presence of non-U.S. persons working within CIKR but also foreign-owned businesses operating U.S. CIKR and U.S. corporations operating internationally. This process must include identification and shared understanding of what individuals in the private sector have a legitimate "need-to-know" and an explanation of what those individuals would be expected to do (and not do) with the information they receive.

Finally, since cyber information sharing is an evolving process, any agreement should contain feedback mechanisms on the usefulness of the bi-directional information exchange process and the actual information that is shared between security partners. Feedback from CIKR security partners will help ensure they receive actionable information, advanced notifications of threats, and a broader awareness of vulnerabilities, providing a tangible benefit and increasing the value proposition for security partner participation.

Milestone:

- Develop dissemination guidance for DHS cyber products that may be used by other agencies or sectors, defining in layman's terms how, when, and if those products may be further distributed within a company, association, or ISAC/ISO (November 30, 2008).

- Establish pilot agreements for bi-directional cyber information sharing with two sectors (ideally one with an established ISAC and one without) (December 31,2008).

- Develop a concept of operations (CONOP) between DHS and the 18 CIKR sectors for bi-directional, operational cyber information sharing (December 31,2008).

Resource Requirements: This effort will require legal counsel support within both government and industry. Work on these activities is already under way through the CSCSWG Information Sharing Subgroup.

Recommendation ST-4: Scope the requirements for implementing real-time cyber situational awareness.

Existing collaborative cyber situational awareness mechanisms offer limited real-time interaction between the private sector and Federal, State, and local governments on response, recovery, and training. In addition, a common CIKR real-time situational awareness for cyber is not available across these disparate domains. This would be especially critical during major cyber attacks that propagate quickly and require real-time threat information sharing and response coordination.

The U.S. Government must identify the classes of information that it needs from the various infrastructure sectors to discharge government responsibilities to protect them, identify the classes of information it is not currently obtaining from industry, and determine how it will reliably obtain that information from industry in the future. The U.S. Government also needs procedures for protecting industry information that it shares with other private-sector entities.

CIPAC Member Input

This input reflects the views by private sector officials to DHS and should not be attributed to, or the official perspective of the U.S. Government.

Seven main barriers have prevented the U.S. Government and private sector from establishing CIKR common cyber situational awareness:

1. No clear criteria between parties as to what information needs to be shared;
2. A lack o f trust between the U.S. Government and private sector;
3. Little incentive for some private-sector entities to develop common situational awareness because they already have their own mechanisms in place;
4. Little agreement on the format or delivery method for shared information;
5. No environment (either virtual or physical) available to host the fused data needed to develop common situational awareness on the scale proposed;

6. A paucity of releasable, actionable, government information because of classification, and distribution limitations; and
7. Lack of jprivate-sector clearances or approved facilities needed to fully participate in developing common CIKR situational awareness.

The distributed and complex nature of the decision-making environment for CIKR cybersecurity makes development of common real-time situational awareness a logistically and financially daunting task. Many sectors have thousands of institutions, all with competing business models, differing perceptions of customer service, and varying trust relationships. A single picture would have to accommodate such realities—multiplied across all 18 sectors—and would have to be built upon an architecture capable of handling massive amounts of information at the high speeds required for real-time awareness. Designated industry representatives would have to be selected to represent their sectors as a whole and would have to be trusted to uphold security markings and classifications, answering to the U.S. Government as well as to the company that employs them. The cost of scoping and building a tool that meets the requirements for cyber real-time situational awareness is likely to be significant and would be a high-risk investment of Federal funding. Before making that investment, the U.S. Government and its information sharing security partners must define a clear scope and mission for the development of common situational awareness and should evaluate a variety of interim or simplified solutions.

Common CIKR real-time cyber situational awareness is not a "single" view or a unanimous agreement on the details of specific events but is instead a series of related processes and

disciplines that seek to provide a shared understanding of events within and among various stakeholder organizations. These include:

- A framework of indications and warnings built over time;
- Threat data, including information about attackers, techniques, methods, prevalence, or targets;
- Strategic analysis examining attacks and intrusions in a broader context rather than on an enterprise or case-by-case basis;
- Pattern analysis enabling enterprise owners to understand their normal flow of data and locate anomalies;
- Enforcement of policies via network monitoring and ensuring that basic defense-in-depth technologies and processes are in place;
- Real-time insight into attacks during specific incident response events; and
- Multiple perspectives and degrees of resolution of the data, including the U.S., State, local, and tribal governments, the private sector, the CIKR community, and individual CIKR sectors.

Figure 1 provides a notional illustration of how different activities can contribute to situational awareness. The concepts presented in Figure 1 can be used as a starting point for defining how an operational model incorporating the US-CERT, NCC, and other CIKR private-sector security partners could be constructed.

As a key part of this task, DHS will need to consider how this common real-time cyber situational awareness will support and integrate with the National Cybersecurity Center (NCSC) and CNCI Initiative 5 "Connect Current Centers To Enhance Cyber Situational Awareness" for increased situational awareness and opportunities for enhanced collaboration. In addition, the role of the National Infrastructure Coordination Center (NICC) and its relationship with US-CERT and the NCC should be addressed.

Milestone:

- Develop a scoping document for the development of common CIKR, real-time situational awareness (December 31,2008).

Resource Requirements: Applicable legal concerns will be scoped and assessed by concerned Federal entities. All other resource requirements will be determined in the scoping process.

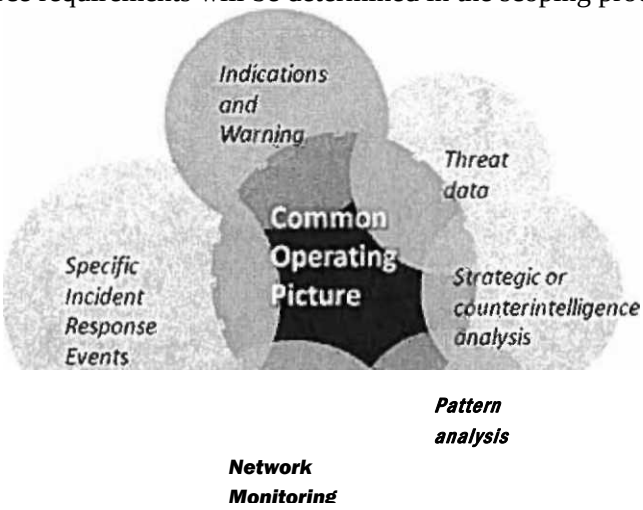

Figure 1: Elements of common cyber situational awareness or "common operating picture"

Recommendation ST-5: Evaluate the feasibility of sharing Federally developed technology capabilities with CIKR.

In many cases, CIKR owners and operators have significant and sophisticated technical capabilities for protecting their own networks; however, owners and operators within some sectors could improve their cybersecurity posture by leveraging Federally developed technologies (such as advanced Intrusion Detection System technologies). Sharing Federally developed technology capabilities also might enhance industry's value proposition for engagement with government and might increase situational awareness capabilities for both CIKR and government. Steps would be taken to ensure that the technology is widely available avoiding favoring one company over another. This concept will be considered in the common cyber situational awareness scoping document described in ST-4 and its feasibility will be analyzed under this recommendation.

Milestone:

- Conduct a feasibility analysis of sharing Federally developed technical capabilities with two interested CIKR owners and operators (December 31, 2008).

- Based on the results of the analysis, potentially devise a plan for a pilot program to share technology with two CIKR owners. The plan for a pilot program will need to include clear roles and responsibilities for both the U.S. Government sponsor and the CIKR owner, including engaging the private sector to determine R&D requirements and sharing Federally developed technology with

the private sector. These roles would include providing hardware and software, operation and maintenance, and reporting of incidents detected by the technology. The technology would be considered for piloting with a

CIKR owner only after the PCC determines the technology had been successfully deployed in a ".gov" environment and has met required performance standards.

Resource Requirements: Applicable legal concerns will be scoped and assessed by concerned Federal entities. All other resource requirements will be determined in the feasibility analysis process.

Recommendation ST-6: Declassify as much intelligence as possible to improve private-sector situational awareness and expedite the TS/SCI clearance process for appropriate private-sector representatives for when ^tear-line" unclassified cybersecurity documents are not available.

DHS provides secret-level clearances for SCC members and has made significant progress in providing secret-level classified briefings to these cleared individuals. With a top secret, sensitive compartmentalized information (TS/SCI) clearance, CIKR sector representatives could access more sensitive intelligence information and thereby help ensure a more comprehensive analysis of cyber risk. Cleared private-sector security partners also would be able to obtain the classified details associated with cybersecurity threat data. In addition, the review of information by sector representatives—even though information could not be shared further—could add to the weight and validity of assessments of cyber threat. If CIKR industry representatives affirm to their colleagues the assessments provided by DHS, it would help build the case for action. A draft plan to obtain these clearances for selected private-sector representatives is already in the DHS chain-of-command approval process. Representatives would be nominated by their SCC to receive higher-level clearances and access.

While clearances would alleviate some information sharing barriers, DHS obviously does not have the resources, nor is it logistically feasible or desirable, to clear everyone in the CIKR sectors. As a result, the U.S. Government should continue to improve upon processes for crafting classified threat information into "tear-line" products that convey sensitive information to trusted partners without compromising sensitive sources and methods.

The U.S. Government must make a commitment to distill actionable threat information proactively down to a level where it can be used to take action. The U.S. Government could leverage cleared private-sector representatives to help distill classified materials down to only what is needed for action without compromising intelligence equities. Access to such information would provide private-sector CIKR owners and operators with a broader picture of sophisticated threats and, more importantly, of the advanced capabilities of various adversaries. Relaying actionable intelligence down to the correct audience requires appropriate processes and technologies. For instance, an effective filtering process is required for delivering tactical information to CIKR owners and operators so that they can defend their networks.

The benefit of disclosing specific classified or CUI information should be weighed against the potentially adverse impact on national security. Such balancing requires ongoing interagency involvement of multiple communities, a robust set of protocols for obtaining input from those communities, and a coordination mechanism for the timely resolution of information sharing conflicts.

Milestones:

- Initiate a TS/SCI clearance process with CIKR sectors (October 31, 2008).
- Develop a plan and timeline for DHS to work with the Intelligence Community on tear-line criteria and processes for sharing information with CIKR sectors (December 31, 2008).

Resource Requirements: Funding and staff resources to process CIKR TS/SCI clearances. Buy-in from the Intelligence Community to work with DHS to produce more timely and actionable tear-line information.

Recommendation ST-7: Enhance information sharing and analysis organizations, whether ISACs or other ISOs, to make them the focal point of cyber operational activity with the 18 CIKR sectors.

Under the NIPP, each sector was to designate an operational information sharing arm. Some CIKR Sectors rely on ISACs, while others rely on ISOs or other established processes designed specifically for a sector or company for the immediate exchange of operational information. Among the CIKR sectors and sub-sectors, eight have functioning ISACs—Communications, Information Technology, Financial Services, Electricity, Water, Emergency Response, Public Transit, and Surface Transportation (rail)—operating at varying levels of maturity and with differing focus on cyber versus physical security issues. Other sectors have additional mature operational cyber information sharing mechanisms or have designated distinct ISOs to analyze and disseminate threat and vulnerability information throughout the sector. The U.S. Government should continue to recognize and use these entities for cyber information sharing and collaborative analysis on behalf of their respective sectors.

Because the business models of ISACs, ISOs, and other processes vary widely across sectors, baseline support is required to ensure each is capable of providing basic cyber information sharing services to CIKR owners and operators. This recommendation seeks to review current support and identify any needs for modification or expansion based on identified requirements to address cyber information sharing needs. Contracting mechanisms and resources will be assessed to cover administration and coordination requirements. In addition, DHS will explore offering more robust functionality via Homeland Security Information Network (HSIN), US-CERT portal or another tool to ISAC and ISO participants to support cyber information sharing. This support could include vetting potential participants, maintaining membership lists, and obtaining and managing content for sector portals. DHS offers analogous contractor secretariat support to the SCCs and has offered information sharing requirements gathering and limited content management support to SCCs/ISACs/ISOs in the past.

To ensure an effective model, the U.S. Government should pursue the following actions:

- Streamline processes with existing organizations;
- Examine the requirements for these services in sector designated ISOs and ISACs;
- Evaluate available contractual models to support provision of these services if requested;
- Identify performance measures to accompany provision of support; and
- Work with private-sector leadership through PCIS, SCCs, and the ISAC Council to establish baseline functionality that each private-sector ISAC/ISO and counterpart government entity needs to provide in order to serve as a focal point of cyber operational information and analysis.

Milestones:

- Collect ISO/ISAC operational and resource requirements (December 3**1**,2008).
- Evaluate available contract support models (December 31,2008).
- Agree on initial baseline functionality sets to support operational activity (June 30, 2009). Review and adjust functionality sets based on experience, continuing with explicit status reviews annually on the anniversary of each initial baseline.

Resource Requirements: To be determined in the requirements analysis listed above.

Recommendation ST-8: Enhance information sharing mechanisms, whether the Homeland Security Information Network or other information sharing technologies, to provide an environment in which technological barriers do not impede cyber information sharing processes.

The HSIN was designed to facilitate the real-time exchange of information to government and CIKR partners at the Controlled Unclassified Information (CUI) level. DHS developed a pilot program for communicating with the CIKR sectors, referred to as HSIN-Critical Sectors (HSIN-CS). According to CIPAC members, while this pilot enjoyed limited success with a few sectors, in general the legacy HSIN system was unable to meet CIKR functional requirements and was not broadly adopted.

DHS is working with its CIKR partners to identify requirements and options for information sharing using HSIN. Providing CIKR security partners with the opportunity to shape HSIN requirements and functionality provides a clear value proposition for security partners and should result in a product that will be more useful to all parties for cyber information sharing. Sectors could then leverage HSIN for use in and with their sector-specific information sharing mechanisms to create a consistent approach to cyber information sharing. This approach gives sectors the flexibility to use existing and familiar systems and tools on top of a common HSFN platform.

In addition to planned HSIN updates, DHS should expand efforts to connect cleared private-sector security partners with nearby cleared Federal facilities to enable use of secure video teleconference (SVTC), secure telephone equipment (STE), and Homeland Secure Data Network (HSDN) e-mail capabilities for remote participation in cyber threat briefings and discussions. In this way, CIKR sectors can participate as full partners in the intelligence analysis and sharing process. DHS increasingly is receiving feedback from CIKR partners that increasing travel costs

are precluding in-person attendance at government events. This proposed step would work to mitigate technical and financial barriers to cyber threat information sharing and collaborative cyber risk analysis with industry experts outside of the Washington, D.C. area. In addition, DHS should explore the current need for equipment use or purchase to be tied to a government contract, limiting the ability of many entities to obtain these devices.

Milestones:

- Develop a plan for CIKR requirements gathering for HSIN (August 31,2008).
- Brief the private sector on industry and government requirements (Sept 29, 2008).
- Develop a plan for vetted security partners to have increased access to SVTC, STEs, secure e-mail, HSDN, and local Federal facilities (November 30, 2008).

Resource Requirements: The HSIN effort is already resourced and plans include the CIKR community. The SVTC, STE, and HSDN plan will require research into venue options and cooperation with local Federal facilities.

III. Long Term Recommendations (1 to 3 Years)

Recommendation LT-1: Expand US-CERT/NCC joint operational capabilities to include private-sector CIKR participation to enhance CIKR real-time situational awareness (builds on Recommendation ST-4).

As experts and advisors have noted in previous studies—such as the Early Warning Task Force of the 2003 National Cybersecurity Summit and the President's National Security Telecommunications Advisory

Committee in 2006—the pervasive nature of cyber infrastructure throughout the 18 CIKR sectors creates the need for co-location (either within a virtual or physical environment) of industry and government resources into a single expanded US-CERT/NCC operation center.

The physical or virtual operations center would allow the CIKR sectors and sub-sectors to volunteer operational subject matter experts to coordinate with each other and the U.S. Government on a variety of cross-sector cyber incident-related efforts. A fundamental goal of the co-location would be to collect and analyze cyber-related information and then escalate that analysis through appropriate channels. Co-location would integrate the analysis generated by industry participants, government partners, US-CERT, and NCC staff and would allow such information and analysis to be compared with results from commercially available services, CIKR-provided information, and information sources. This information would provide an important source of data for fusion in the National Cybersecurity Center (NCSC). It also would provide the needed vehicle for CIKR input into National Cyber Response Coordination Group (NCRCG) decision-making process. Physical or virtual co-location would maximize the U.S. Government's investment in network protection by facilitating collaborative analysis and coordinated protective and response measures and by creating a feedback loop to increase value for private-sector and government participants. Another key outcome would be stronger institutional and personal trust relationships among security practitioners across multiple communities.

US-CERT and NCC Watch were co-located to the same floor in 2007 but are not physically co-located in the same operations center. DHS plans to co-locate US-CERT and the NCC and could expand the successful NCC model that includes communications industry representatives and invite the 18 CIKR sectors to have representation, focused on cybersecurity situational awareness, within the joint operations center (either physically or virtually). A limited pilot with a few sectors that have had previous experience with two-way information sharing would help refine operational concepts prior to inviting all 18 CIKR sectors to join. This expansion of capacity available to CIKR sectors as US-CERT grows and matures would increase the value proposition for private-sector participation and data submissions. If private-sector submissions of intrusion data and vulnerabilities were met with timely and valuable information from US-CERT, the private sector would be likely to increase submissions of data.

This effort would eventually include voluntary participation from all 18 CIKR sectors, as determined appropriate by each of the sectors, but it would be most effective to extend participation in the project in phases, building on the co-location of US-CERT and the NCC. Several private-sector partners have expressed concern over the costs of providing representatives to a joint operational capability, especially considering the potential for

significant downtime between incidents. Previous efforts to co-locate industry and the U.S. Government have had challenges that hindered effectiveness; however, greater participation could result from further efforts to:

- Enhance the value proposition for private-sector participation and input;
- Fully integrate private-sector participants (as determined by the sector);
- Fully use the expertise of those participants through ongoing collaboration on analysis and exercise planning;
- Defray costs of participation, in part through the use of "virtual co-location." **Milestones:**
- Ensure operational integration of US-CERT and NCC (in progress).
- Develop a plan for the physical co-location of US-CERT and NCC (January 1, 2009).

- Execute initial operating capability for the physical co-location of US-CERT and NCC (October 1,2010).

- Develop a plan, including legal analysis, to integrate all 18 CIKR sectors either virtually or physically into a facility, including interim strategies to engage the private sector for NCRCG coordination prior to co-location (June 30, 2009).

- Obtain a formal legal opinion, non-disclosure agreement, and privacy impact assessment as necessary, detailing the maximum extent of information sharing that is permitted and expressing any limitations on the ability to combine data within and amongst government and industry (June 30, 2009).

- Develop a CONOP, in coordination with the NCSC CONOP (October 31, 2009).

- Define metrics and oversight mechanisms to monitor response mechanisms and remediation efforts (October 31,2009).

- Ensure the CIKR virtual or physical co-location is fully operational (October 1,2010).

Resource Requirements: Key requirements will include identifying a suitable facility and funding, and consideration of privacy and legal implications. CIKR partners will need to provide personnel resources.

Recommendation LT-2: Establish a mechanism to give companies opportunities and incentives to invest in R&D and—based on legal, security, and investment level criteria— potentially allow companies to obtain intellectual property rights to the results of government-funded or partnered cybersecurity research and development

An important first step in leveraging investment in cyber is to understand and define that investment. Over the past 20 years, the U.S. Government has allocated significant R&D funding for information security. That data should be reviewed to assess the results of R&D activities in order to identify further R&D requirements and locate previous research that might solve current cybersecurity problems. In addition, implementation of this recommendation should include coordination with Initiatives 4 and 9 (on R&D coordination and leap-ahead technologies, respectively) of the CNCI. Current efforts by OSTP, the Networking and Information Technology Research and Development (NITRD) program, and the Special Cyber Operations Research and Engineering (SCORE) Interagency Working Group to analyze government-wide R&D should be performed and coordinated in tandem with the proposed activities in this recommendation. Each sector should be brought in to identify desired capabilities or requirements in conjunction with the DHS Science and Technology Directorate in a collaborative manner to achieve eventual buy-in from all 18 CIKR sectors.

Under the NIPP framework, the Information Technology (IT) Sector has begun to examine its current R&D priorities. In its 2007 Sector-Specific Plan (SSP), the IT Sector identified nine R&D priority areas:

1. Cyber situational awareness and response;

2. Forensics;

3. Identity management: authentication, authorization, and accounting;

4. Intrinsic infrastructure protocols security;

5. Modeling and testing;

6. Control systems security;
7. Scalable and composable secure systems;
8. Secure coding, software engineering, and hardware design improvement; and
9. Trust and privacy.

In addition to these priorities outlined by the IT Sector, the protection of intellectual property and securing against the insider threat are general priorities for private-sector CIKR owners and operators. While IT Sector R&D efforts can be applied in cross-sector efforts, unilateral development of requirements by one sector is not recommended. Each sector should be brought in to develop R&D requirements in a collaborative manner to achieve eventual buy-in from all 18 CIKR sectors, leveraging sector SSP implementation activities and efforts such as the Control Systems Security Roadmaps developed in the Energy and Water sectors. Since publication of the IT SSP in May 2007, the IT Sector has been working to characterize these priorities and catalogue existing government, private sector, and academic research in these areas. The IT Sector is planning an R&D exchange to identify companies that are either performing R&D activities or have expertise in each identified R&D priority area. This analysis will yield a list of private-sector security partners (including government-owned, contractor-operated labs and Federally funded R&D centers) with whom the U.S. Government can partner for specific cybersecurity R&D issues. Steps will be taken to ensure DHS is not prejudging the competitive acquisition process.

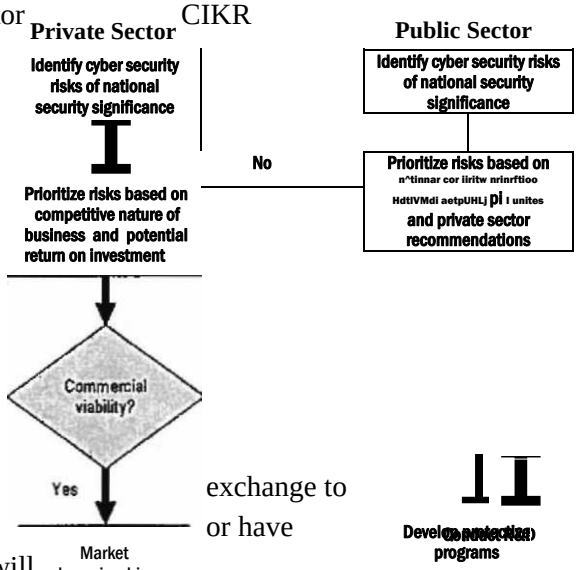

Figure 2: R&D Process for Risks of National Security Significance

The IT Sector's Protective Programs and R&D Working Group (PPRD WG) is developing an R&D Information Exchange Framework to promote parallel, but not overlapping, processes across government and private-sector R&D activities. As Figure 2 illustrates, the private sector will continue to invest in R&D initiatives for which there is commercial viability, and the U.S. Government should minimize its investment in the areas for which significant commercial investment is already occurring. Alternatively, across the nine priority areas defined above, some areas present significant commercial risk or no commercial viability at all yet are still very important to the protection of private and public sector CIKR. These areas deserve the greatest amount of investment from government R&D sources. The challenge comes when trying to identify the areas that need investment. Commercial entities are unlikely to share their internal R&D priorities because of proprietary concerns but are more likely to indicate those areas in which they are not willing to make investment or are only willing to make an investment in partnership with the U.S. Government. The R&D Information Exchange framework under development ideally will allow the public and private sector to identify those areas that require government R&D investment prioritization without compromising the competitive advantages of the commercial entities conducting R&D.

The value of a strong public-private partnership cannot be overestimated. The public sector already gets tremendous benefit from existing investments by IT Sector participants. Services, operations, facilities, technologies, and real systems that industry can supply for R&D initiatives might otherwise be unavailable, unaffordable, or unfeasible for one area within the R&D community. Likewise, industry participants can learn from collaboration with government, and academic researchers and can use those lessons learned for potential real-world applications.

In addition, companies are developing technologies that may not demonstrate immediate commercial viability but may necessitate government involvement to allow for near-term technological development and enhancement in advance of general availability. The U.S. Government often recognizes different security needs than does the commercial marketplace; therefore the U.S. Government requires a mechanism

to identify necessary near-term technologies and support commercialization for deployment throughout CIKR.

The U.S. Government should leverage the IT Sector's PPRD WG and the activities under way in Initiatives 4 and 9 to analyze and address the following key questions:

1. What key information elements are required in a public-private information exchange framework to prioritize public-sector R&D funding related to cybersecurity while protecting the commercial viability of private R&D efforts?

2. How should the public-private partnership leverage risk assessment and threat identification in the prioritization of R&D initiatives?

3. In what areas should government R&D investments focus?

4. How will needs and capabilities be identified and prioritized?

5. What are the principal characteristics of the cybersecurity marketplace and how should they affect this model? How do they differ from other CIKR sectors, and how can the other sectors benefit from the IT Sector's R&D initiatives?

The value proposition for the public sector will be an optimization of R&D resource expenditure to those activities that most require non-commercial intervention. The private sector will gain unique insights stemming from R&D efforts and will use them to address emerging threats and risks through the commercialization of technology. All CIKR owners and operators stand to benefit from IT Sector R&D efforts that result in cost-effective tools and practices that they need to secure their cyber infrastructures. While the IT Sector's R&D efforts were used within this recommendation to illustrate the need for public-private coordination, all sectors are required to develop R&D priorities, per the NIPP guidance. While R&D in many sectors focuses on physical security, many cross-sector R&D efforts focus on cybersecurity, especially for supervisory control and data acquisition (SCADA) systems. Thus, any plan to integrate private-sector input into Federal R&D programs should leverage not just the IT sector but also work done by other sectors on cyber R&D.

Milestones:

- Provide a briefing on PPRD efforts and findings to initiatives 4 and 9 leaders (November 30, 2008).

- Use the PPRD WG and CSCSWG to address the aforementioned "key questions" and work with Initiatives 4 and 9 leaders to develop a CONOP for integrating the private-sector input into Federal cybersecurity R&D efforts (June 2009).

Resource Requirements: Requires coordination with Initiatives 4 and 9 leaders. This also an important long-term, strategic topic that should be considered for study and recommendations by ESF.

Recommendation LT-3: Investigate methods for leveraging capabilities of cleared IT and communications product and service providers.

Information sharing improves the ability of the public and private sectors to assess threats against their respective networks. Companies can use government information to develop a more complete picture of their security environments and to take appropriate protective measures. The U.S. Government—by

analyzing the relationship between intrusions, tactics, and vulnerabilities—can in turn judge whether malicious activity targeting Federal networks is pertinent to critical infrastructure. Increasing the quality of shared information serves to improve the overall level of network security. Two major obstacles identified above hinder this effort:

- Government concern about broadly sharing classified and sensitive threat information (including signatures and vulnerability data) that may jeopardize intelligence sources and methods; and

- Industry concern about sharing proprietary or private information with government.

Given that these issues have persisted for decades, it would be useful to evaluate alternative approaches. DHS should explore the feasibility of entering into agreements to share information with cleared IT and communications service and product providers who are increasingly important intermediaries in the security of government and CIKR networks. These firms design, build, and integrate hardware and software and also provide tools and services to protect their clients' networks. Because many of these firms contract with the U.S. Government, they already possess the facilities and clearances necessary to receive and hold classified information. These same firms could leverage this capability and information provided by the U.S. Government to improve protection of CIKR networks without the need to share the details of often highly classified data with those CIKR facilities directly.

By partnering with these producers and providers, the U.S. Government could streamline the sharing of actionable threat information and extend coverage to a broader critical infrastructure audience than addressed through existing mechanisms. Such an effort would supplement existing mechanisms such as the sector ISACs, which will also be enhanced through the other activities described in this report. While some CIKR owners and operators would still not be reached, presenting some challenges to ensure equitable implementation, this concept presents an opportunity to reach a broad range of firms across the sectors. In addition, the multinational nature of many companies warrants careful implementation of any classified information sharing.

When the U.S. Government observes malicious activity on its networks or has information about a threat or an impending cyber attack, it could share that information with those producers and providers that have been cleared to receive information. Routing threat-specific data through these cleared firms could help ensure that information is not mishandled or compromised, in part because end-user companies would not be required to handle and protect sensitive security information. As a part of any agreement, the firms would be required to provide feedback to DHS on the information, including anonymized data on attack trends in CIKR networks, which in turn would support the common operating picture.

A pilot/study would examine legal and policy implications surrounding this concept, funding requirements, how it would complement other mechanisms (ISACs, ISOs), and how CIKR entities that do not use these firms could be equitably supported. To ensure fairness, the U.S. Government could consider assistance to small businesses to meet security requirements. Risks could be mitigated by making clear that the U.S. Government is prepared to share information with all qualified companies that are willing to meet security requirements.

Milestones:

- Develop feasibility analysis leveraging experience and lessons learned of the Defense Department's pilot with the Defense Industrial base and the United Kingdom's "Consultancy Model" (February 28,2009).

- Develop a pilot program plan (June 30,2009).

- Commence execution of an approved program plan (FY 10).

Resource Requirements: To be developed during feasibility analysis and pilot program planning. These plans will require legal and policy expertise and input.

Recommendation LT-4: Investigate new ways to drive improvement in the cybersecurity posture within the private sector where market forces yield an insufficient value proposition.

The U.S. Government's ability to assist the CIKR owners and operators to strengthen their level of cybersecurity throughout all CIKR is limited in part by the diversity of CIKR owners and operators, the international nature of CIKR, the extraordinarily dynamic nature of the IT industry, and the rapid evolution of cyber threats. Owners and operators of CIKR must weigh cybersecurity costs against other business and operational requirements on the basis of their particular market environment and within existing fiscal or operational regulatory boundaries. Some CIKR owners and operators are subject to regulation that stipulates risk management or security measures, such as the Chemical Facilities Anti-Terrorism Standards. Other sectors have significant regulation not related to security or resilience goals, and yet others are unregulated.

Regardless of the level of regulation, many CIKR owners and operators are security conscious and employ methods of network protection to mitigate the risks to their business model. Others, however, are unable to develop a compelling business case for enhanced cybersecurity because of insufficient knowledge of the threats facing their organization, a lack of consistent risk and vulnerability measurement tools and methodologies across CIKR sectors, or a lack of

understanding of the potential impacts to their organization or to the nation. The heavy CIKR dependence upon communications and the interconnected network models within and between businesses could result in a successful cyber attack against an unsecured and unprepared organization having repercussions within and across multiple sectors.

Establishing incentives and additional drivers for sound cybersecurity practices would create value for companies that would not otherwise make the requisite security investments, thereby creating an efficient and sustainable mechanism to upgrade the security of the entire system. Establishing and incentivizing sound cybersecurity measures to mitigate evident risks, while accounting for differences in business models, would enable CIKR companies to apply value drivers consistently within and across diverse sectors and sub-sectors (such as the Oil and Natural Gas and Electricity sub-sectors within the Energy Sector). The U.S. Government should leverage the expertise and reach of the CSCSWG to conduct a sector-by-sector analysis and identify a menu of incentives. This work should leverage the National Infrastructure Advisory Council's (NIAC) *Best Practices for Government Intervention* report as well as other documented best practices for improving cybersecurity. The U.S. Government should evaluate the array of incentive options before establishing a plan to provide incentives to the private sector. The following text box lists some options identified by the private sector that the U.S. Government should evaluate during its analysis of incentives.

1&PACMember Input:

Tthis input reflects the views offered by private sector officials to DHS and should not be attributed to, or considered the official perspective of, the U.S. Government.

1. ***Leverage the purchasing power of the U.S. Government to provide enhanced levels of cybersecurity for private-sector entities that do business with the U.S. Government.*** Because many critical infrastructure companies do business with the U.S. Government— selling products or sendees that meet Federal needs—the contracts that govern these relationships, such as the General Services Administration's Networx contract, offer a useful vehicle for requiring enhanced cybersecurity measures. A more unified approach to procurement that places a higher value on

security in comparison to cost would enhance the U.S. Government's market influence and would allow it to set contract requirements that promote broader adoption and implementation of better cybersecurity measures by its vendors and contractors. The creation of standardized contract language embracing sound cybersecurity would further dissemination of good practices throughout the economy and possibly assist State and local governments as they work to enhance their cybersecurity. The model could he offered as best practices to international standards bodies responsible for establishing certifications and other industry norms.

2. ***Extend protection to private-sector entities that develop and deploy effective and innovative cybersecurity technologies to remove any market "barrier to entry" caused by legal liabilities in the event of the products failing to perform.*** The U.S. Government should work toward developing legal protections for the development and deployment of network security technologies or practices that support CIKR protection. The Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act of 2002 was designed to encourage companies to field new anti-terrorism technologies by lintiting

liability and even granting full immunity against third-party claims brought against qualified anti-terrorism technologies for damages resulting from terrorist acts. The U.S. Government could explore ways to use SAFETY Act protections to encourage cybersecurity technology enhancements.

3. ***Streamline compliance of multiple regimes.*** Regulatory and legislative mandates and compliance frameworks—such as Sarbanes-Oxley, Gramm-Leach-Bliley, and the Health Insurance Portability and Accountability Act, as well as other general privacy best practices—should be analyzed together and any overlaps highlighted. As compliance reporting requirements are already burdensome in some sectors, care should be taken to ensure efficient implementation ofethese types of controls and to measure the performance of the incentives. Due to the rapid evolutionary pace of technology and cyber threats, any stipulated control should be regularly reviewed for adequacy and efficiency.

4. ***Include cybersecurity in regulatory rate base.*** The U.S. Government should consider a dialogue with relevant Federal regulatory agencies, State public utility commissions (SPUC) and the Council of Mayors to explore ways to implement early rate-based, recovery of appropriate and effective cybersecurity investments in the rate base for affected CIKR services. Tfais exemplifies the true cost of service for these CIKR owners and operators to provide safe and reliable service to the rate payers. Facilitated by the U.S. Government, regulators and mayors could evaluate with their utility service providers the effectiveness of existing cybersecurity controls and could work with those service providers to prioritize the early implementation of appropriate and effective cybersecurity measures. As part of this program, mayors and SPUCs would need to be educated on cyber threats to increase their awareness and strengthen the argument to incorporate cybersecurity into the rate base.

5. ***Educate the public on cybersecurity.*** An informed consumer will be able to personalize the "value" of a more secure and resilient service or product, thus enabling market forces to be driven by the consumer rather than by government.

6. ***Develop mechanisms to expand use of cyber insurance to promote corporate investment in the use of effective standards and practices of cybersecurity.*** Insurance traditionally has been one of the most effective motivators in fields as diverse as good health practices and safe building standards; however, the cyber insurance market has not developed to the point where it can be used as a sufficient motivator for improved corporate behavior. The U.S. Government traditionally has developed mechanisms, such as crop and flood insurance, which transfer the risk of major events to both government and industry. These mechanisms might be adapted to the cybersecurity field. Cyber insurance, if more broadly used, could provide a set of uniform and constantly improving standards for corporations to adopt and be measured against while simultaneously transferring a portion of risk the U.S. Government might face in

the case of a major cyber event. Cyber insurance that provides incentives for compliant actions (i.e., lower premiums) provides a "return on investment" instrument for security professionals to show value of investment.

This list is by no means inclusive, is subject to further government analysis (including legal review), and not all items would be applicable for all sectors. Other concepts suggested by industry participants included social contracts, qualification for Federal grants, and awards programs for cybersecurity in CIKR. A sector-by-sector study should explore how much of the cybersecurity issue is a problem that requires government intervention and what can be driven by market forces. The CSCSWG will convene a working group to work with the individual sectors to conduct this review.

Milestones:

- Complete a sector-by-sector (and sub-sector where appropriate) study, which at a minimum will include key judgments for each sector as to whether market forces yield an insufficient value proposition to implement and maintain appropriate cybersecurity measures (March 31, 2009).

- Develop and execute a plan based on the sector study (FY 10).

Resource Requirements: Will be developed in the sector-by-sector study that includes an implementation schedule focusing upon the most critical sectors first. It is likely that the initial study results will yield long-term, complex policy issues that could be explored though the ESF.

Recommendation LT-5: Investigate methods to encourage cybersecurity across the business community nationwide similar to those used within private-sector CIKR.

Based on the discussion of cybersecurity return on investment, industry and government should work to establish a clear value proposition for integrating cybersecurity into the enterprise risk management process where it does not exist already. Such a value proposition, promulgated through outreach and awareness activities on threats and the importance of enterprise risk management from a cybersecurity perspective, can be used to encourage additional private-sector investment in network security for small and medium-sized businesses.

DHS collaborates with organizations such as the National Cybersecurity Alliance (NCSA) to reach target audiences for cybersecurity awareness programs, activities, and initiatives including public awareness campaigns, events, and public service announcements. The small-business community is one such target audience. DHS is also working with NCSA to prepare for National Cybersecurity Awareness Month, which is held every October to increase cybersecurity awareness across the country and help Americans prepare for and respond to cyber-related threats and attacks. Since its inception, National Cybersecurity Awareness Month has been formally recognized by Congressional Resolution, Federal, State, and local governments, and industry leaders.

As part of its Ready Business Initiative, DHS has been working closely with the U.S. Chamber of Commerce to encourage the private sector to take steps to prepare for a range of emergencies. Through a series of town hall-style meetings, officials from the DHS Private Sector Office— working closely with representatives from the Chamber as well as Federal, State, and local government partners—are coming together to discuss the role of the business community in

addressing a myriad of threats, including natural disasters, terrorist attacks, and pandemic influenza outbreaks. Leveraging this model, DHS will collaborate with the Chamber to increase cybersecurity awareness and encourage cybersecurity investment by the private sector. The partnership enables DHS to

bring cybersecurity practices to the wide audience of private-sector organizations outside the Washington, D.C., area, including the diverse set of small and medium-sized businesses that the Chamber represents. Through its network of local chambers, the Chamber will coordinate a series of five regional events across the nation for business owners and operators, incorporating participation from State and local government. The partnership will also increase awareness of the potential consequences from a cyber attack, and it will stress the importance of integrating cybersecurity into broader enterprise risk management and incident response planning.

Furthermore, DHS and the Chamber hosted a Chief Security Officer (CSO) Summit during the 2008 National Cybersecurity Awareness Month to highlight the importance of integrating cybersecurity into enterprise-level risk management and incident response plans. Such efforts encourage private companies to view cybersecurity as an integral investment to their business operations.

DHS will also present this as a topic for ESF study and recommendations and will encourage the industry leaders active in that framework to leverage their expertise and influence to increase heightened awareness and focus of cyber security within the business community,

Milestones:

- Complete all five regional cyber events (March 31, 2009). The first event is planned for October 20, 2008.

- Complete a suite of outreach efforts related to National Cybersecurity Awareness Month that will reach a national audience, including the business community (October 31, 2008).

Resource Requirements: Requires support from the Chamber, other awareness organizations, and State and local partners. May require coordination with Federal partners, such as the Departments of Defense and State to ensure synchronization with other efforts.

IV. Conclusion

In order for these recommendations to succeed, ***the U.S. Government must work with the CIKR sectors in a true collaborative partnership as must industry with the government, both realizing each other's essential cultural and operational differences.*** After developing these new processes, policies, and tools, we must exercise them together with government and industry CIKR partners to ensure they are successful. Resources will need to be committed from both government and industry. Complex legal and policy implications inherent in many of these recommendations will require active engagement across the interagency community as well as legal counsel from within industry and government. The CIPAC mechanism and NIPP sector partnership structure provide the framework needed to work with the spectrum of CIKR partners; however, significant engagement, commitment, and labor investment will be needed from these partners. DHS will provide OMB with Federal funding resource requirements for FY 10 by December 1, 2008. DHS will continue engagement on short- and long-term recommendations through the NIPP framework and will provide regular status updates to both CIKR and Interagency partners. The DHS National Cyber Security Division (NCSD) will be the lead for implementing all of the recommendations in this report, in coordination with the DHS Offices of Policy, Privacy, Civil Rights and Civil Liberties, Private Sector, Intelligence and Analysis, Infrastructure Protection, and General Counsel. NCSD also will coordinate extensively with interagency partners leading other CNCI projects, the Sector-Specific Agencies, State, local, and private-sector partners.