THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

Cybersecurity Collaboration Report

Strengthening Government and Private Sector Collaboration Through a Cyber Incident Detection, Prevention, Mitigation, and Response Capability

May 21, 2009

TABLE OF CONTENTS

EXECUTIVE SUMMARY

At the direction of the Executive Office of the President and following a comprehensive scoping effort, the President's National Security Telecommunications Advisory Committee (NSTAC) established the Cybersecurity Collaboration Task Force in November 2008 to explore the need for and feasibility of creating a joint 24/7 public-private operational capability focused on improving the Nation's ability to detect, prevent, mitigate, and respond to significant cyber incidents.

Protecting the United States' (U.S.) cyber and underlying critical infrastructures is essential to the Nation's homeland and national security, public health and safety, economic vitality, and way of life. Today's global economy, military operations, and public-private sector endeavors depend on the ability to operate in cyberspace. Meanwhile, the magnitude, nature, and sophistication of cyber threats pose increasingly greater consequences, highlighting an urgent need for protective action. Critical infrastructures such as banking and finance, communications, energy, information technology, and transportation are interdependent, with disruption of one having the potential to dramatically affect the others. As a result of these dependencies and interdependencies, the Nation's ability to operate with complete effectiveness in cyberspace is at serious risk. At the same time, the lines of responsibility between the public sector and the private sector for addressing cybersecurity and interdependency issues are blurred. Consequently, an urgent need exists for an overarching operational framework for coordination and response that more fully integrates the public and private sectors' efforts in this area. Development of a framework that can fully and strategically address the cyber threat must be a matter of national priority.

The Task Force's primary finding is that the integrated, operational information sharing and cyber response mechanisms needed to adequately address the cyber threat do not exist today. Given the threat environment, and the global reliance upon cyber technologies and networks, a national capability to prevent, detect, mitigate, and respond to cyber incidents of national consequence in a timely, effective manner is critical to national security. Although a variety of strategic, policy, and legal issues are associated with our Nation's ability to safely and effectively operate in cyberspace, the most significant gap is the lack of an operational mechanism for the Government and private sector to collaborate and coordinate during cyber events.

Based on the authorities and responsibilities established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, the NSTAC recommends to the President to direct the establishment of a joint, integrated public-private, 24/7 operational cyber incident detection, prevention, mitigation, and response capability to address cyber incidents of national consequence.

This recommendation proposes establishing a Government-sponsored Joint Coordinating Center (JCC) for public and private sector representatives from various critical infrastructures and key resources sectors following the aggressive, phased approach described in the report. Specifically, the JCC would initially build upon the current coordination/collaboration capabilities of the National Coordinating Center and the U.S. Computer Emergency Readiness Team, and incorporate other existing cyber incident monitoring and response public-private

entities. The JCC capability should be located in a Government facility with around-the-clock operations and supporting tools and collaboration capabilities. The JCC's primary mission would focus on robust information-sharing for developing and sharing cyber situational awareness, and would institutionalize the time-sensitive processes and procedures to detect, prevent, mitigate, and respond to cyber incidents of national consequence.

1.0 INTRODUCTION

1.1 Purpose

For many years, the President's National Security Telecommunications Advisory Committee (NSTAC) has recognized that, in today's converged environment, cyberspace is a strategic asset and protecting the Internet's integrity and availability is a national security priority.[1] In this report, the NSTAC examines national security and emergency preparedness (NS/EP) communications issues in a converged environment and provides recommendations to help ensure the Internet's integrity and availability now and in the future.

This report outlines the United States' (U.S.) need to develop a joint, integrated public-private, 24/7 operational cyber incident detection, prevention, mitigation, and response (DPMR) capability.[2] The cyber incident DPMR capability - the Joint Coordinating Center (JCC) - will consist of operational coordination and liaison functions, with the physical or virtual participation of the private sector critical infrastructure and key resources (CIKR) community. The capability is necessary to enable the Nation to defend itself from threats and vulnerabilities that jeopardize its ability to rely on cyber space. In addition, this operational capability will be a focal point for developing, monitoring, and creating a common situational awareness of threats and vulnerabilities in general and the operational impact of cyber incidents of national consequence in particular. Where feasible, the JCC would collect warning and threat information to enhance preparedness of both public and private sector cyber stakeholders through fostered collaboration and unity of effort. This may also include recommendations for protective measures or mitigations.

This report underscores the importance of creating a cyber incident DPMR capability. The single most critical improvement to the protection of both public and private sector cyber-based systems is the routine communication about new or evolving threats

DPMR Capability

Detection: Developing an understanding of normal network traffic volume and flow using independent sources will help the JCC participants detect anomalies. Stakeholders will work with partners to obtain external data on threats and vulnerabilities.

Prevention: Developing proper interdiction guidance for prevention activities. Prevention activities include bi-directional information sharing within the IT and communications sectors, and with government (Federal, State, and local) and international agencies.

Mitigation: Developing the mitigation tools and technology will help stakeholders to address cyber incidents, while ensuring stability within other unaffected networks.

Response: Organizing teams, processes, and procedures will help stakeholders to coordinate internal and external sources to respond to and recover from incidents.

[1] See: *Network Security Scoping Task Force Report: Report of the Network Security Task Force*. October 1990; *NSTAC Network Security Task Force Report*. July 1996; *The NSTAC's Input to the National Plan: An Assessment of Industry's Role in National Level information Sharing, Analysis, and Dissemination Capabilities for Addressing Cyber Crises.* November 2001; *Next Generation Networks Task Force Near Term Recommendations Working Group Report*. March 2005; *NSTAC Next Generation Networks Task Force Report.* March 2006; and the *NSTAC Next Generation Networks Implementation Annex Working Group Letter to the President.* November 2008.

[2] This report will refer to the joint, integrated public-private, 24/7 operational cyber incident detection, prevention, mitigation, and response capability simply as the "cyber incident DPMR capability." Each term (detection, prevention, mitigation, and response) is defined in Appendix A, Glossary of Terms.

and vulnerabilities (sometimes referred to as 'indications and warnings') among all key stakeholders responsible for protecting cyber networks and systems. In this report, the NSTAC presents a framework for initiating this comprehensive cybersecurity operational capability, identifies and analyzes policy considerations that may affect future capabilities, outlines parameters for the envisioned end state, and offers recommendations for phased implementation.

1.2 Background/Need

> *The reflection upon my situation and that of this army produces many an uneasy hour when all around me are wrapped in sleep. Few people know the predicament we are in.*
>
> General George Washington, 1776

Over the last 20 years, the Nation has become increasingly dependent on information technology (IT), interacting and communicating seamlessly across vast networks traversing the globe. This reliance on interconnected IT systems also exposes the Nation to significant cyber threats and vulnerabilities, placing our CIKR[3] at risk. Today, an adequate national operational capability to respond to the current growing cyber threat does not exist. Cybersecurity issues have been addressed piecemeal in varying ways by different government entities at the Federal, State, local, tribal, and territorial level; private companies and industry organizations; and academic institutions. Although these groups have initiated and sustained various levels of collaboration, cyber threat and vulnerability concerns require an even more systematic, integrated approach.[4] Recognizing the growing interdependencies between cybersecurity and CIKR, these groups are addressing cybersecurity from a national security perspective, rather than from a merely technology perspective. However, these efforts are works in progress; the need for an increasingly collaborative and systematic approach remains.

Today, an adequate national operational capability to respond to the current growing cyber threat does not exist.

CIKR Interdependencies and Threat Actors

The Nation's ability to function as a global leader depends on a variety of critical infrastructures and cyber technologies that enable the economy to operate within the global marketplace. For example, increased consumer access to electronic commerce has changed the face of the marketplace; migration to electronic medical records will improve the quality of healthcare; and power distribution systems are moving to a 'smart grid' delivery concept, which is highly dependent on cyber technologies. This critical reliance on cyber and communications networks is intensified by a growing interdependence among these networks and other CIKR.

Such interdependence was demonstrated and highly visible during the August 2003 Northeast

[3] *Critical Infrastructure: the assets, systems, and networks, whether physical or virtual, so vital to the U.S. that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof. Key Resources: publicly or privately controlled resources essential to the minimal operations of the economy and government. (http://www.dhs.gov/xprevprot/programs/gc_1189168948944.shtm).*

[4] *The NSTAC does not formally comment on pending legislation, but the NSTAC acknowledges that the U.S. Congress is considering many of the issues discussed in this report through proposed legislation. Given the changing nature of bills during the legislative process, the NSTAC notes these developments and will track their progress.*

blackout. Immediately before the blackout, a computer worm disrupted an Ohio power plant's indications and warnings system, degrading its ability to receive critical data regarding the health of the power plant and grid. Although the worm did not directly cause the blackout, it created confusion and prevented the plant owners and operators from receiving warnings that would have alerted them to the failures in the grid so they could have taken measures to protect the power plant. This failure within the energy sector disrupted cyber and communications networks throughout the Northeastern United States and areas in Canada, underscoring the interdependencies between cyberspace and other CIKR sectors.[5] Potential adversaries have undoubtedly noticed these vulnerabilities and the United States' disjointed incident response.

In addition to these growing interdependencies, the United States has witnessed the rise of a diverse and aggressive range of threat actors and various entities carrying out cyber attacks against cyber systems and underlying infrastructures. These threat actors include: agents of nation-states, lone wolf hackers, cybercrime organizations, and terrorists, among others. These malicious actors are relentlessly exploiting the complexity of the interconnected environment and the anonymity of the Internet to access communications and data networks, presenting new risks to U.S. cyber and national security. Future concerted cyber attacks against U.S. national infrastructures could be severe or catastrophic.

Various entities have carried out cyber attacks against cyber systems and underlying infrastructures.

Future concerted cyber attack against U.S. national infrastructures could be severe or catastrophic.

These looming threats came to fruition in incidents such as the 2007 cyber attacks against Estonia, the 2008 cyber attacks against Georgia, and the 2008 cyber attacks against the Department of Defense (DoD). In 2008, the World Bank suffered a series of Internet attacks that penetrated at least 18, and perhaps as many as 40, of the bank's data servers. In March 2009, the *New York Times* reported on a world-wide cyber espionage network known as GhostNet. This network targeted organizations and individuals in 103 countries and used malicious software to steal sensitive information.[6]

Most recently, since November 2008, malicious code known as Conficker spread to more than 12 million computers worldwide. In response to this threat, a number of private sector and government representatives informally joined together to form the Conficker Working Group to develop mitigation techniques to respond to the evolving threat. The working group conducted its activities in an ad hoc and self-organizing manner, and was instrumental in reducing the impact and infection rate of U.S. computers.[7] However, Conficker continues to pose challenges and risks for the global Internet community. The depth and breadth of Conficker's spread highlights the value of public-private sector cybersecurity collaboration and how a joint, integrated capability would more likely offer an established and secure place to coordinate these kinds of efforts.

International geopolitical events, such as the cyber attacks against Estonia and Georgia, demonstrate that the Federal Government would benefit from immediate, expert, and

[5] "Blaster worm linked to severity of blackout," *ComputerWorld*, August 29, 2003.

[6] "Vast Spy Systems Loots Computers in 103 Countries," *New York Times*, March 28, 2009.

[7] http://www.confickerworkinggroup.org/wiki/.

authoritative private sector involvement in response to such events. Public-private cooperation provides a valuable mechanism for subject matter experts to contribute to protecting America's cyber infrastructure.

Beyond their susceptibility to cyber-specific threats, the complex interdependencies of the various infrastructures, cyber and communications networks are also subject to the threat of natural disasters (for example, hurricanes, floods, earthquakes, and wildfires) and physical events (for example, train derailments, undersea cable cuts, and bombs), as documented in the NSTAC's 2006 *Global Infrastructure Resiliency (GIR) Report*.[8] The threat of natural disasters and disruptive physical events can significantly impact the cyber environment with long term effects. In addition to being vulnerable to physical and cyber threats, these networks are also vulnerable to electromagnetic pulse attacks.[9]

The threat of natural disasters and disruptive physical events, such as cable cuts or train derailments, can significantly impact the cyber environment with long term effects.

Disruptive events in any of these areas can significantly impact the cyber environment with long-term effects. Consequently, current DPMR activities associated with the physical protection and restoration of CIKR cannot be subordinated to cyber response. Rather, physical and cyber DPMR activities must be approached in conjunction with each other, and cannot be treated as separate processes or functions.

The Need for an Operational Solution

There is no operational mechanism across all sectors for a coordinated and unified effort to detect, prevent, mitigate, and carry out a real-time response to significant cyber issues affecting the Nation. Government and private sector subject matter experts recognize the urgent need for and value of a public-private sector collaborative DPMR capability. Previous reports, such as the 2003 President's *National Strategy to Secure Cyberspace*,[10] the Department of Homeland Security (DHS) *2007 Tiger Team Report*[11] and the 2006 NSTAC *Next Generation Networks Task Force Report*, recommended establishing a joint coordination center where the public and private sectors could share cybersecurity information. The NSTAC issued the following recommendation:

Government and private sector subject matter experts recognize the urgent need for and value of a public-private sector collaborative DPMR capability.

> *A joint coordination center for industry and Government should be established. This would be a cross-sector industry/Government facility with a round-the-clock watch, and would be brought up to full strength during emergencies. Such a center would improve communications between industry and Government as well as among industry members, and would incorporate and be modeled on the NCC.*

[8] *NSTAC Report to the President on Global Infrastructure Resiliency*, October 2006.

[9] Electromagnetic pulse (EMP) attacks present a less significant direct threat to telecommunications than it does to the National Power grid, but would nevertheless disrupt or damage a functionally significant fraction of the electronic circuits in the Nation's telecommunications systems in the region exposed to EMP (which could include most of the United States). EMP attacks could damage a functionally significant portion of the Electric Power Grid, resulting in prolonged power- and synergistic system-outages. Dr. William R. Graham, Chair, Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. July 10, 2008. (http://armedservices.house.gov/calendar_past_hearings.shtml).

[10] *The President's National Strategy to Secure Cyberspace*, Executive Office of the President (2003).

[11] *Tiger Team Report*, Department of Homeland Security (2007).

> *The center should be a Government-funded, appropriately equipped facility, manned jointly by experts from all key sectors. In a fully converged (Next Generation Network [NGN]) environment, everything will be interconnected and interdependent to a greater degree, and thus means of coordinating among all key sectors must exist. Physically collocated, joint manning is vital to achieve the high level of interpersonal trust needed for sharing sensitive specific information and to achieve the level of mutual credibility required in a fast-paced decision-oriented environment. It should provide the full set of planning, collaboration, and decision-making tools for those experts to work, whether together as a whole or in focused subgroups.*[12]

Previous reports recommended establishing a joint coordination center where the public and private sectors could share cybersecurity information.

The proposed cyber incident DPMR operational capability is envisioned to address disruptions and attacks to national CIKR that occur via the U.S. cyber infrastructure.[13] A variety of entities currently have defined and limited responsibilities; there is no overall entity responsible for cross sector coordination and response during time-critical cyber incidents of national consequence. The National Coordinating Center (NCC) has coordinated a variety of activities between the Federal Government and the private sector for more than 25 years. Although the NCC's charter does not preclude coordinating cyber incidents, it has historically focused on issues associated with the physical side of the Nation's telecommunication infrastructure. Information sharing within the Network Security Information Exchanges (NSIE) focuses on cyber vulnerabilities and threats, but does not focus on immediate, operational activities. The U.S. Computer Emergency Readiness Team (US-CERT) is charged to provide outreach to the private sector, but could benefit by broadening its interaction with NCC Industry Members and other private sector participants. There are other examples of joint private-public collaboration, primarily in the post-incident cyber domain. However, these are not focused on early indications and warnings, but rather on post-incident investigations, some of which have law enforcement aspects. In addition, organizations have made little progress in assessing the threat environment and aligning cyber incident management efforts. In short, despite the existence of a number of coordination mechanisms and capabilities, there is currently no overarching, integrated public-private, 24/7 operational cyber incident DPMR capability.

Many factors have contributed to this situation, such as shifting priorities, budget constraints, and the blurred lines of ownership and jurisdiction over these issues. These factors affect both the Government and the private sector. Nonetheless, the NSTAC believes a critical first step in implementing some of these recommendations is establishing an initial operational capability that allows all appropriate players to share information, establish a baseline understanding of the threats to our Nation's critical infrastructures, and take action to detect, prevent, mitigate, and respond to cyber threats.

Since 1991, the NSTAC has recommended creating a cyber collaboration capability, and recognizes progress such as the creation of the IT and Communications Sector and

An urgent and growing need exists to improve upon coordination of existing U.S. and international cyber incident capabilities in both public and private sectors.

[12] *NSTAC Next Generation Networks Task Force Report* (March 28, 2006).

[13] Like the physical infrastructure of roads, bridges, power grids, telephone lines, and water systems that support modern society, 'cyber infrastructure' refers to the distributed computer, information, and communication technologies combined with the personnel and integrating components that provide a long-term platform to empower the modern scientific research endeavor. (http://www.nsf.gov/od/oci/reports/toc.jsp).

Government Coordination Councils.[14] Although these achievements have improved cybersecurity collaboration, the NSTAC believes that operational collaboration and coordination between the Federal Government and private sector must improve. An urgent and growing need exists to improve upon coordination of existing U.S. and international cyber incident capabilities in both public and private sectors.

The NSTAC has further recommended to the Government that the private sector should be elevated to the status of a trusted partner, and that the public and private sectors should share critical and time-sensitive threat information to strengthen the threat and warning architecture.[15] The Federal Government has the tools and abilities to gather information on the capabilities and intentions of adversaries in cyberspace, but does not adequately share this data with the private sector. Without jeopardizing its sources and methods, the Government must share this data with the private sector, including information regarding planned attacks and the assets that may be in danger. This advanced information will give the infrastructure owners and operators more time to take protective measures to deflect attacks or minimize their impact. Such measures can limit negative effects both on the private sector and its immediate customers, as well as the extended, interdependent CIKR.[16]

Elevating the private sector to trusted partner status is the foundation for any future collaboration effort, and is a policy decision that should be made and supported at the highest levels of Government. The Federal Government and the private sector should improve their awareness of shared risk, consequences, dependencies, and cascade effects; they must also clarify decision-making authority and their respective response and reconstitution roles. The desired outcome of these improvements is clear guidance and an enhanced ability to rapidly execute national-level decisions for response options to sophisticated attacks against our shared information infrastructure.[17] This outcome can only be accomplished by first acknowledging that the risk associated with partnering with the private sector outweighs the consequence of not doing so.

1.3 Charge

At the request of the Executive Office of the President (EOP) to examine the issue of cybersecurity collaboration, NSTAC established the Cybersecurity Collaboration Task Force (CCTF) in November 2008 to explore the need for and feasibility of creating a joint public-

[14] See: *Network Security Scoping Task Force Report: Report of the Network Security Task Force*. October 1990; *NSTAC Network Security Task Force Report*. July 1996; *The NSTAC's Input to the National Plan: An Assessment of Industry's Role in National Level information Sharing, Analysis, and Dissemination Capabilities for Addressing Cyber Crises.* November 2001; *Next Generation Networks Task Force Near Term Recommendations Working Group Report*. March 2005; *NSTAC Next Generation Networks Task Force Report.* March 2006; and the *NSTAC Next Generation Networks Implementation Annex Working Group Letter to the President*. November 2008.

[15] See: *Network Security Scoping Task Force Report: Report of the Network Security Task Force*. October 1990; *NSTAC Network Security Task Force Report*. July 1996; *The NSTAC's Input to the National Plan: An Assessment of Industry's Role in National Level information Sharing, Analysis, and Dissemination Capabilities for Addressing Cyber Crises.* November 2001; *Next Generation Networks Task Force Near Term Recommendations Working Group Report*. March 2005; *NSTAC Next Generation Networks Task Force Report.* March 2006; and the *NSTAC Next Generation Networks Implementation Annex Working Group Letter to the President*. November 2008.

[16] *NSTAC Response to the Sixty-Day Cyber Study Group.* Section 3.1. March 12, 2009.

[17] Ibid. Section 4.5.

private, 24/7 operational cybersecurity collaborative DPMR capability. The CCTF also examined the opportunities and challenges to developing this cyber incident DPMR capability.

The report examines the feasibility of developing a new cyber incident DPMR capability or expanding the operational focus of existing cyber watch functions, and identifies the issues that may impede or preclude achieving this objective. Moreover, the report also proposes recommendations for resolving these issues.

1.4 Process

The CCTF identified issues that may affect the development and deployment of a cyber incident DPMR capability, including trust issues between the public and private sectors and policy considerations. Section 3.0 describes these issues.

The Task Force conducted a gap analysis of existing collaboration models and capabilities to determine mechanisms that may be developed or enhanced to establish a national cyber incident DPMR capability. The data-gathering included interviews with subject matter experts and internal discussions among Task Force members. Based on its findings, the Task Force then developed recommendations.

During interviews with the CCTF, key public and private sector subject matter experts identified existing operational capabilities that may serve as a basis for a cyber incident DPMR capability.[18] The CCTF posed the following questions to all presenters regarding public-private cyber incident DPMR capabilities:

- Can the capabilities be provided under the current contractual, legal, and regulatory framework? If not, what would need to change to support any given capability?
- Are the capabilities currently technically feasible? If not, what would be necessary to move in that direction?
- Assuming the desired capabilities are lawfully and technically feasible, what operational and/or business model would best suit participation by the private sector CIKR in this initiative?
- What cultural/trust issues must be addressed?

[18] See Appendix C for a list of Government officials and private sector representatives who met with the CCTF.

2.0 DESIRED END STATE: 24/7 CYBER INCIDENT DPMR CAPABILITY

2.1 Joint Coordinating Center (JCC)

To achieve the desired end state of a joint, integrated public-private, 24/7 operational cyber incident DPMR capability, the NSTAC recommends that, under the direction of a Federal department or agency identified by the President, members from both the public and private sectors build upon current NCC and US-CERT capabilities and integration efforts and extend these capabilities to develop a JCC capability. The principal feature of the JCC is rich, timely, bi-directional sharing of information between the public and private sectors that ensures their ability to detect, protect, mitigate, and respond to cyber threats.

> *The principal feature of the JCC is rich, timely, bi-directional sharing of information between the public and private sectors that ensures their ability to detect, protect, mitigate, and respond to cyber threats.*

Governance – Clarity of Mission, Roles, and Responsibilities

To achieve success and maximum value, the proposed JCC capability requires clearly defined authorities, oversight, management, responsibilities, roles, and resources. There is a lack of clear authority and budget responsibility for a public-private cyber collaboration capability; cyber collaboration capabilities currently exist, but are largely uncoordinated. In addition to approving this JCC capability, the NSTAC recommends that the President should:

> *There is a lack of clear authority and budget responsibility for a public-private cyber collaboration capability; cyber collaboration capabilities currently exist, but are largely uncoordinated.*

- Designate the Executive Branch organizations that will participate as members of the JCC and contribute personnel and other resources;
- Designate a lead organization or sponsor; and
- Direct budget and authority provisions to properly implement, operate, maintain, and evolve the proposed JCC capability.

The lead organization or sponsor should convene a working group, leveraging the membership and expertise of existing organizations such as NSTAC member companies and members from appropriate Government and Sector Coordinating Councils, and task the working group to develop the initial concept of operations (CONOPS) to govern the JCC. The CONOPS will refine the JCC's:

- Mission and purpose;
- Membership requirements and eligibility;
- Designated leadership (to consider private sector co-chairs);
- Desired operational capabilities and coordination and liaison functions;
- Governance structure; and
- Other details necessary for its establishment.

The CONOPS will identify actions required to implement the JCC. The NSTAC understands that Phase I activities will be the most urgent, specific, and immediately actionable tasks.

Given this matter's sense of urgency and its link to national, homeland, and economic security, it is imperative to establish an achievable but aggressive timeline to execute an implementation plan for the JCC. The NSTAC recommends that the working group complete the CONOPS and launch the JCC soon thereafter.[19] Upon approval, the JCC would be implemented through a phased approach, as described in Sections 2.2 and 2.3. A phased implementation approach will allow enhanced capabilities to be established in an affordable and efficient manner. The NSTAC offers an implementation timetable for consideration in Appendix B.

A phased implementation approach will allow enhanced capabilities to be established in an affordable and efficient manner.

The NSTAC recommends that the JCC be housed in a Government-funded and appropriately equipped facility. The facility should be based in the Washington, DC, area to leverage the expertise and existing collaboration centers located in this region; however, NSTAC believes that a back-up facility should be based in another part of the United States to provide resiliency and ensure continuity of operations. In a fully converged, networked environment, JCC functions would be interconnected and interdependent to a greater degree, enabling all key sectors to coordinate with each other.[20] In turn, representatives from all key sectors will jointly operate the JCC. In some cases, representatives will be physically collocated; in other cases, they will be virtually connected. Physical collocation and joint operations are vital elements to achieve the interpersonal trust and level of mutual credibility required for sharing sensitive, detailed information in a fast-paced, decision-driven environment.[21] In addition, there is a need for controlled communications mechanisms to enable sharing information among all those authorized to access the information.[22]

Finally, the NSTAC notes that these recommendations are consistent with the objectives and recommendations of the President's Comprehensive National Cybersecurity Initiative (CNCI). Although Initiative #5 focuses on linking certain Federal cyber operations centers to improve cyber threat awareness and incident response actions, it focuses exclusively on the U.S. Government. Some of these centers are also critical components in our recommended joint public-private sector capability. Initiative #12 recommended expanding the joint operational capability of the US-CERT and the NCC to include private sector CIKR sector participation, to eventually incorporate voluntary participation from all 18 CIKR sectors.

[19] As a result of the 2007 DHS *Tiger Team Report*, DHS has efforts underway to develop a collocated, coordinated operational capability. The NSTAC envisions that its proposed cyber incident DPMR capability may build on these efforts.

[20] The term "key sectors" refers to the banking and finance, communications, energy, and IT sectors.

[21] "If the partnership between the Federal Government and private sector is to be successful, another key requirement is establishing a permanent physical location or forum so that critical and non-critical sectors can interface with one another and their Federal counterparts. This is essential to developing and maintaining long-term collaborative relationships." *A Review of the Top Officials 3 Exercise*, DHS OIG Report OIG-06-07, p. 24 (Nov. 2005).

[22] The term 'controlled communication mechanisms' refers to real-time, managed bridges and Web tools for information sharing.

2.2 Operations

Successful models of public-private sector collaboration currently exist in practice, such as the long history of the NCC for communications-related matters. The NCC model operates within the existing legal and policy frameworks, and should be leveraged as an integral element for future public-private cyber security collaboration. Leveraging both the NCC and the US-CERT, as well as other capabilities, a fully-developed JCC capability can allow public and private sector representatives to share information, which will improve cyber incident DPMR. The JCC will have a 24/7 watch and warning capability, with surge capacity during emergencies. To expedite the implementation of this capability, the NSTAC recommends a phased approach.

Successful models of public-private sector collaboration currently exist in practice, such as the long history of the NCC for communications-related matters. The NCC model operates within the existing legal and policy frameworks, and should be leveraged as an integral element for future public-private cyber security collaboration.

The first phase will leverage existing collaboration models within the public and private sectors and establish a foundation for extending collaboration capabilities. The key elements associated with the first phase are:

- Extending the current presence of communications company representatives to the physical/virtual presence of Information Sharing and Analysis Center (ISAC) representation from the communications, financial services, IT, and power sectors;
- Establishing the baseline information needs of both private sector and Government partners;
- Creating an initial CONOPS predicated on those baseline information needs; and
- Testing that CONOPS for a period of time to ensure that the approach is sound.

Follow-on phases will improve on these existing models and develop more robust information sharing to achieve enhanced cyber incident DPMR capabilities. These phases would include expansion of U.S. Governmental and international participation, extended private sector participation, and enhanced training and exercise support.

Appendix B provides a phased-approach implementation of the JCC. The table suggests an aggressive implementation timeline commensurate with the urgency of addressing this need. The complexities of this effort require sustained high-level attention to ensure success.

2.3 Membership

Planning and executing national cyber incident DPMR capabilities requires joint participation of many domestic public and private sector organizations, in addition to international entities. Presently, organizations involved in cyber incident efforts are physically separated, functionally disjointed, and lack efficient communications capabilities. Combining all stakeholders into a single Government-funded/equipped physical location, with the capability for virtual participation, is necessary for full cybersecurity planning and execution.

Planning and execution of national cyber detection, prevention, mitigation, and response capabilities requires joint participation of many domestic public and private sector organizations, in addition to international entities.

Although the CONOPS will outline longer-term membership requirements, core Phase I JCC membership should include, but not be limited to, the U.S. Government, the private sector, and the international community. Examples are provided in the table below.

TABLE 1 – CORE PHASE I JCC MEMBERSHIP	
Federal Government	Department of Homeland Security US-CERT NCC Watch National Cyber Security Center (NCSC)
	DoD Joint Task Force Global Network Operations' (JTF-GNO) Security Center Defense Cyber Crimes Center (DC3)
	Department of Justice's National Cyber Investigative Joint Task Force (NCIJTF) within the Federal Bureau of Investigation (FBI)
	Federal Communications Commission (FCC)
	Department of Commerce
Private Sector	Carriers
	Internet Service Providers (ISP)
	Security companies
	Content providers
	Hardware/software vendors
	Owners/operators representatives
	Representatives from the Banking and Finance, Communications, Electric, and IT ISACs
International Community	Key allies, such as Australia Canada New Zealand United Kingdom
	Other international organizations, such as Forum of Incident Response and Security Teams International Watch and Warning Network, North Atlantic Treaty Organization Interpol

The NSTAC notes that work is currently underway to better align the Government's own operational centers for better situational awareness, through the CNCI. Listing the Government centers above is not meant to interfere with the Government's own organizational activities. Rather, by naming these centers, we are acknowledging that their capabilities may be critical components in our recommended joint public-private sector capability, and making known our desire to coordinate and collaborate with those capabilities.

Presently, organizations involved in cyber incident efforts are physically separated, functionally disjointed, and lack efficient communications capabilities.

During the JCC's subsequent development phases, additional cybersecurity-focused departments, agencies, and private sector groups may participate to improve the depth of information sharing. These groups could provide additional subject matter expertise and operational experience to further the JCC's capabilities. Such members could include:

- Other ISACs;
- Intelligence Community Incident Response Center (IC-IRC);
- National Security Agency Threat Operations Center (NTOC);
- SANS Internet Storm Center (ISC);
- National Cyber-Forensics Training Alliance;
- North American Network Operators Group; and
- Carnegie Mellon University's Computer Emergency Response Team Coordination Center.

For security purposes, all members should be required to hold a clearance at a level to be determined in the CONOPS. In addition, the CONOPS will identify any special security clearance considerations for the core members (including international partners) to facilitate their participation in a secure environment.

Combining all stakeholders into a single Government-funded and equipped physical location, with the capability for virtual participation, is necessary for full cybersecurity planning and execution.

The NSTAC recommends that a mechanism for rapidly and effectively coordinating among all key sectors be established to address security needs in the new cyber environment. Incident response, including response planning, requires a joint public-private sector effort to improve coordination and establish an inclusive, comprehensive, and effective response capability.[23]

2.4 Information Sharing to Enable Operational Collaboration

The JCC's core function is operational collaboration enabled by strong, effective information sharing, which is vital in a cyber threat environment that is relentless and increasing in scope. The JCC's success depends on the extent to which public and private sector members acquire, use, share, and act upon information. This sharing must be bi-directional and timely. The U.S. Government and the private sector must establish mechanisms to protect sensitive information (e.g., proprietary information, personal information, and intellectual property) and to address antitrust concerns.

In an effort to design a robust, effective, and legally-protected information sharing environment for the proposed cyber incident DPMR capability, the NSTAC examined a number of considerations, specifically:

- Cultural/trust and technological considerations; and
- Legal, regulatory, and international considerations.

[23] In response to the President's 60-day Cyber Review, the NSTAC provided input and recommendations; the recommendations in this report are consistent with those recently provided in the NSTAC's support of the 60-day Cyber Review.

The cultural and technological considerations are addressed below; the regulatory, legal, and international considerations are addressed in Section 3.0.

Cultural/Trust Considerations

Cultural challenges arise in creating a cyber incident DPMR capability because the Government and the private sector have different organizational objectives, which may conflict with coordinated, integrated, and seamless information sharing. The Government's mission focuses primarily on protecting the Nation's security; the private sector focuses on serving and protecting its customers. These objectives themselves may not be mutually exclusive, but they can result in incompatible information sharing practices. Consequently, the Government and the private sector must examine and overcome such difficulties and reach common ground to productively share cybersecurity data.

As a result of a lack of guidance and clarity regarding these considerations, the private sector has been reluctant to offer the Government cybersecurity data relating to critical infrastructure. A long-term approach to overcoming these barriers and alleviating liability concerns is to develop a protected and legally acceptable process to secure, use, and share cybersecurity data with the Government, without jeopardizing the privacy of the private sector and its customers.

Another concern is the issue of mutual trust between the Government and the private sector. For instance, the Intelligence Community (IC) currently classifies information to protect the sources and methods of its intelligence collection activities. The IC is therefore reluctant to share detailed cybersecurity threat data, fearing that the private sector may not adequately protect the sources of this information. Exposure of classified data could clearly hamper the IC's ability to effectively gather further information, but failing to share threat data with the private sector could also lead to a distorted or incomplete view of the common operating environment. The IC's reluctance to share cybersecurity threat data exacerbates the trust issue between the Government and private sector.

To ameliorate this problem, the Government and the private sector can gradually establish mutual trust by working closely together on their common goal to detect, prevent, mitigate, and respond to future cyber attacks. For example, the Government can develop tearline procedures to protect the IC's classified sources and methods, and still provide sufficient information about the threat itself to allow the private sector to take mitigation measures.[24] This early, advance information will give the infrastructure owners and operators more time to take protective measures to deflect attacks or minimize their impact.

Technical Considerations

Tools, techniques, methods, and procedures must anticipate and keep pace with a rapidly evolving threat.

The JCC will require tools for monitoring cyber infrastructure data, developing situational awareness, and coordinating response activities among all key sectors. In a collocated environment with a virtual collaboration capability, experts will need the best supporting tools to successfully prevent and manage the evolving attacks. The most significant threats are the attacks that have not yet been predicted

[24] This issue is currently being addressed through the Project 12 activities under the Comprehensive National Cyber Initiative.

by security experts, such as those involving innovative strategies and techniques. The increased speed and scope of attacks, and the complexity of coordinating remediation efforts, exceed human capacity for manual analysis and response in a timely and effective manner. Tools, techniques, methods, and procedures must anticipate and keep pace with a rapidly evolving threat. Investment in research and development will produce tools to support advanced cyber incident DPMR activities.

Another technical challenge to establishing a cyber incident DPMR capability is secure communications. The JCC requires a robust, resilient and secure communications system with the CIKR owners and operators to facilitate the cyber incident detection, prevention, mitigation and response capability. Such a communications system will allow Government and private sector participants (both physical and virtual) to communicate and coordinate if the JCC primary communications system is disrupted. Additionally, using robust logging and encryption technologies to protect the confidentiality and the integrity of the communications is essential to prevent adversaries from intercepting the JCC participants' cyber incident response communications. The NSTAC recommends that the JCC cyber incident DPMR capability include a redundant and secure communications system to facilitate public-private collaboration.

The JCC requires a robust, resilient and secure communications system with the critical infrastructure and key resources owners and operators to facilitate the cyber incident detection, prevention, mitigation and response capability.

3.0 LEGAL CONSIDERATIONS

The successful creation and execution of the JCC mission requires public-private sector information sharing, which raises legal, liability, antitrust, and privacy issues for all parties involved. Phase I of the JCC capability is predicated on sharing information to the extent feasible in today's legal environment. However, to move beyond the immediate capabilities and achieve the end-state envisioned for the JCC, the Task Force evaluated aspects of the current legal environment – including regulatory issues, case law, and contractual provisions – that must be addressed to expand information sharing capabilities in the JCC context.

3.1 Current Legal Environment

In its 2003 *Legislative and Regulatory Task Force Report*, the NSTAC analyzed legislative and other impediments to information sharing.[25] Although the information sharing environment has evolved since then, legal provisions regulate information acquisition, use, and sharing.

With respect to antitrust issues, the proposed 24/7 JCC envisions the participation and collaboration of private sector competitors across a number of sectors. Collaboration among competitors raises antitrust concerns, warranting a review of antitrust legislation. The *Sherman Antitrust Act of 1890*[26] precludes any collective activity that has the probable effect of lessening competition in the marketplace.[27] Because the NCC model currently operates within the existing legal and policy frameworks, the NCC framework offers a relevant template to use to initiate the Phase I capability, and should be leveraged for future public-private sector cybersecurity collaboration. To eliminate any ambiguity, the NSTAC recommends that an antitrust review be conducted to include activities planned in the second and later phases of the JCC's development.

Several complex statutory provisions *may* impact the ability of all interested parties to acquire, use, and share information relevant to cybersecurity threats. While not a comprehensive list, the laws listed below set the parameters for cybersecurity collaboration and could limit near real-time, public-private, operational cybersecurity collaboration.[28] Table 2 depicts the law that applies to content in both real-time interception and in stored communications.

[25] NSTAC LRTF Report. *Barriers to Information Sharing,* September 2003.

[26] *Sherman Antitrust Act of 1890*, July 2, 1890, ch. 647, 26 Stat. 209, 15 U.S.C. § 1–7.

[27] *The proposed JCC could be modeled on the NCC. The NCC participants share real-time information about communications networks. For the NCC, the Department of Justice issued a letter ruling stating that NCC's collaborative activities do not violate antitrust laws. Specifically, the letter ruling determined that the NCC collaborative activity was one which "would enable the industry to provide collectively that which each member of the industry could not provide individually, i.e., a nationwide, interoperable system of independent carrier networks in which the resources of all are available to meet this Nation's NS/EP needs." See Letter from the Office of Attorney General*, June 1, 1983, to Lt. Gen. William J. Hilsman, Manager, NCS.

[28] In the future, effective coordination of information sharing would be solidified if specific legal protections were enacted for cyber defense activities designed to acquire, use, and appropriately share relevant information, including through measures designed to monitor, intercept, use and disclose aspects of Internet and other IP communications.

Table 2 - Incident Response: Monitoring Communications During an Incident[29]		
Timeliness of Information Accessed	**Access to Communications Content**	**Access to Communications Metadats (Headers, Logs, and Other Information)**
Real-time interception of communications	Wiretap Act (18 USC §§2510-22) FISA (50 U.S.C. §§ 1801 et seq.)	Pen Register Statute (18 USC §§3121-27) FISA (50 U.S.C. §§ 1801 et seq.)
Access to stored communications	ECPA (18 USC §§2701-12) FISA	ECPA FISA

- The *Wiretap Act* (1968) broadly prohibits the intentional interception, use, or disclosure of wire and electronic communications unless a statutory exception applies. Although some statutory exemptions arguably allow cybersecurity initiatives, privacy advocates and others may disagree with some of the applications of these exceptions to cybersecurity activities, which may create uncertainty that could discourage parties from comprehensive information sharing related to cyber defense. As described in Section 3.2 below, the *Communications Act of 1934* also regulates divulging certain communications and information pertaining to communications.

- The *Electronic Communications and Privacy Act of 1986* (ECPA) amended the Wire Tap Act in a variety of ways.[30] For example, it added statutory protections for stored electronic data in the *Stored Communications Act*, and for data derived from "pen registers" and "trap and trace devices" that pertains to the origin and destination (but not the content) of certain communications in the *Pen Register Statute*.[31] Those provisions

[29] Table 2 is based on information taken from Joel M. Schwarz, DOJ, and was modified by the NSTAC Task Force. Joel M. Schwarz, DOJ, Computer Crime and Intellectual Property Section, Criminal Division. *Cyber Security—the laws that Govern Incident Response.*

[30] Section 2701 (5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; and USC 2511 (2) (a) (i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

[31] *§2701 – The Stored Communications Act of 1986* focuses on unlawful access to 'stored wire and electronic communications and transactional records.' According to the statute, anyone who *intentionally accesses without authorization a facility through which an electronic communication service is provided or… intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system* is subject to prosecution. *§3121 – The Pen Register Act of 1986* governs real-time monitoring, but not collection, of communications traffic data. Carriers and ISPs are required to provide content if served with a court order. This statue was designed to apply to traditional telecommunications networks and to enable law enforcement officers to capture the originating

set forth the procedures by which governmental authorities may obtain access to such communications and communications-related data, and also include exceptions for certain service providers and other activities that apply in the cybersecurity context.

- The *Foreign Intelligence Surveillance Act* (FISA) imposes criminal penalties upon and authorizes civil suits against any person who intentionally *engages in electronic surveillance under color of law* in the absence of statutory or other authorization and against persons who intentionally use or disclose information so acquired.

- Various states have enacted laws that may limit the interception of electronic communications and the use or disclosure of such intercepted communications. Some may argue that these laws and related judicial doctrines restrict the ability of carriers, ISPs, and others to act as part of a coordinated cyber defense effort.

- The *Privacy Act of 1974* prevents Federal Government departments and agencies from releasing personally identifiable information (PII). Specifically, the Privacy Act states, *No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains*. Certain sector-specific privacy laws may also restrict public-private information sharing, such as the *Gramm-Leach-Bliley Financial Services Modernization Act*, which focuses on the financial services sector, and the *Health Insurance Portability and Accountability Act*, which focuses on the health sector.

3.2 Regulatory Considerations

Under Section 222 of the *Communications Act of 1934*, as amended, and the FCC's implementing regulations, telecommunications carriers and providers of interconnected Voice over Internet Protocol (VoIP) service have a duty to protect the confidentiality of customer proprietary network information.[32] Telephone companies and providers of interconnected VoIP service may use, disclose, or permit access to customer information in these circumstances:

- As required by law;
- With user approval; and
- In providing the service from which the customer information is derived.

and terminating telephone numbers of phone calls made to and received by an individual, but not the content of those calls. The FCC expanded the scope of the *Communications Assistance for Law Enforcement Act* to include the interception of information provided over the Internet. The Pen Register Act has since been applied to Internet technologies, allowing law enforcement officers to monitor the source and destination of Internet Protocol traffic. CALEA was intended to preserve the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities. *Telecommunications carriers are identified as common carriers, facilities-based broadband Internet access providers, and providers of interconnected Voice over Internet Protocol (VoIP) service. (http://www.fcc.gov/calea/).*

[32] *In the Matter of Implementation of the Telecommunications Act of 1996; Telecommunications Carriers; Use of Customer Proprietary Network Information and Other Customer Information*; IP-Enabled Services, 22 FCC Rcd 6927 at ¶ 54.

The FCC requires telecommunications service providers and interconnected VoIP providers to file certification stating whether or not they are in compliance with the FCC's Customer Proprietary Network Information rules. The certification must include a statement demonstrating compliance in specific categories.

Contractual Considerations

Telecommunications service providers, ISPs, and other IT companies may face contractual barriers that prevent them from sharing cybersecurity data with the Government. For example, contractual provisions might be interpreted in some circumstances as barring service providers from sharing detailed cybersecurity data that reveals the identity of the providers' customers. If a service provider inadvertently divulges proprietary or other information that may damage a customer's reputation, the service provider might be sued for breach of contract for damages allegedly suffered by the client or others. Major Government customers, however, may wish to modify their contracts with owners and operators and develop contractual provisions that would allow owners and operators to share cybersecurity data within the proposed JCC capability.

3.3 Current Case Law

Theory of Negligent Enablement

Various Federal and state laws and regulations, tort law, international law, evidentiary requirements, and contractual commitments contribute to the legal standards for maintaining information security. Through case law, courts are establishing a 'negligent enablement' legal precedent, which finds liability for companies that neglect to protect data in their custody. For example, if a company neglects to patch a known vulnerability in its network within a timely manner, and customer data is vulnerable, lost, or stolen, the company may be liable.[33] As a result of this legal precedent, owners and operators are increasingly hesitant to share cybersecurity data that may reveal known vulnerabilities in their networks; nor are they eager to share information regarding the company's actions or inactions in addressing the vulnerability. As envisioned during Phase I, sharing aggregated and anonymized cybersecurity data will not expose companies to liability concerns of this type because specific network vulnerabilities will not be revealed. However, as more detailed information is shared in the JCC's subsequent development phases, such as threat and vulnerability data, owners and operators may have liability concerns arising from the 'negligent enablement' precedent.

[33] *In 2003, the State of California was the first state to pass a law mandating that companies or other organizations maintaining personally identifiable information (PII) must notify affected citizens if their data has been lost, stolen, or shared without proper permission. Regulators and enforcement agencies must also be notified following a data breach. Following California's example, 34 other states have passed similar data breach notification laws that impose a 'duty to warn' on companies and organizations that maintain PII.*

3.4 Models for Liability Protection

Before implementing Phase II, the Government should consider adopting legislation that would clearly provide liability protection for acquiring, using, and sharing more detailed cyber data, or that would, at a minimum, clearly state that the existing statutory exceptions apply to such activity. As to the former, there are at least three statutes that serve as models for such liability protection:

- The *Support Anti-terrorism by Fostering Effective Technologies Act of 2002* (SAFETY Act);[34] and
- The *Year 2000 (Y2K) Readiness and Responsibility Act of 1999.*[35]

The SAFETY Act provisions provide Federal procurement credits and a safe harbor from civil liability for those companies who can demonstrate compliance with market generated best practices for cyber security. Industry organizations such as the Internet Security Alliance have recommended that Congress adopt a "Cyber Safety Act" based on the Safety Act model. They believe this new act would provide a coherent and comprehensive approach to liability, creating explicit Federal support for incentives that encourage private sector investment in improved security and protection of the Internet.

Another model for cyber security liability protection concerns is the *Y2K Readiness and Responsibility Act of 1999.* This law established protections for companies from potential unfounded or frivolous lawsuits stemming from 'millennium glitches.' Specifically, the law requires a 90-day notification period, places caps on punitive damages, establishes proportional liability, and encourages alternative dispute resolution. The JCC capability may require liability protection similar to those found in both laws.

3.5 International Issues

As a result of the borderless nature of cyberspace and the instantaneous communications it creates, the JCC must engage with members of the international community, including multinational organizations and foreign-owned network service providers. Moreover, private sector entities that operate in foreign countries must ensure that all of their cybersecurity activities conform to applicable foreign legal requirements.

Prior NSTAC Recommendations

In its 2007 *NSTAC Report to the President on International Communications*, the NSTAC reviewed the legal and policy framework underpinning international communications.[36] The existing legal framework consists of treaties, conventions, bilateral dialogues, Mutual Recognition Agreements, Federal Trade Agreements, memoranda of operations, national plans, and other legal instruments. The NSTAC concluded that adequate cyber defense could only

[34] *Support Anti-Terrorism by Fostering Effective Technologies Act of 2002,* 6 U.S.C. §§ 441-44 (2006).

[35] *Year 2000 (Y2K) Readiness and Responsibility Act of 1999,* Public Law 106-37.

[36] *NSTAC Report to the President on International Communications,* August 16, 2007.

occur through international cooperation. The NSTAC considers the recommendations in that report to be crucial in developing the JCC capability.

With respect to natural disasters and physical events having cyber consequences or effects, the NSTAC noted in its 2006 *Global Infrastructure Resiliency Report*[37] that the undersea cable infrastructure carries approximately 95% of the international traffic, including Internet traffic, and that restoration of that infrastructure requires international cooperation. The NSTAC believes that the Federal Government should review these recommendations and consider its appropriate role in the protection and security of that infrastructure.

Implications in Europe

Analysis and response to cross-border cyber incidents requires sharing information among countries. However, some countries have legal restrictions on the acquisition, use, and sharing of this data, particularly if the country considers the data to be PII.

Article 25 of the European Union (EU) *Data Protection Directive* permits the transfer of PII to a non-EU country only if the European Commission has determined that the non-EU country ensures an adequate level of protection. As a whole, U.S. privacy and information protection law does not meet the Commission's standards. However, EU PII can still be shared with the United States under certain contractual arrangements by which the receiving U.S. entities agree to data processing and sharing constraints that meet the *Data Protection Directive's* requirements. For example, air carriers operating flights to or from the United States or across U.S. territory have contractual agreements that permit the carriers to share EU passenger name records (PNR) data with U.S. customs authorities. In addition, U.S. entities that voluntarily certify to the U.S.-EU Safe Harbor Framework may receive EU PII. Many non-EU countries – such as Australia, Argentina, Canada, and Switzerland – have adopted privacy laws similar to the EU's law.

The NSTAC believes that any future legal review and assessment of foreign laws governing the acquisition, use, and exchange of data and PII would facilitate the success of the JCC. The review may determine that the JCC requires a safe harbor provision similar to the PNR Agreements.

3.6 Legal Conclusions

To facilitate information sharing without violating these legal requirements, many service providers have developed policies and procedures to sanitize and aggregate cybersecurity data so that it can be shared with the Government without disclosing PII. The NSTAC believes that these procedures to remove the source and content of IP traffic are an intermediary step that can improve collaboration between the Federal Government and the private sector. Although the JCC's desired end state includes the ability to share the full contents of malicious Internet traffic, the NSTAC recognizes the need for explicit legal authority to share more detailed cybersecurity data with the Federal

No new legal authorities are required for Phase I implementation. However, follow-on phases may require additional legal guidance or authorities.

[37] *NSTAC Report to the President on Global Infrastructure Resiliency*, October 2006.

Government because this increased information sharing may expose PII. For the JCC's Phase I build-up, sanitized and/or aggregated data is sufficient to accommodate the center's initial needs. No new legal authorities are required for Phase I implementation. However, follow-on phases may require additional legal guidance or authorities.

4.0 FINDINGS AND CONCLUSIONS

The NSTAC recommendations presented in Section 5.0 are based on the CCTF's findings with respect to the need for a coordinated cyber incident detection, prevention, mitigation, and response capability and the CCTF's approach for addressing that need. The NSTAC finds that:

- Today, an adequate national operational capability to respond to the current growing cyber threat does not exist.

- Various entities have carried out cyber attacks against cyber systems and underlying infrastructures. Future concerted cyber attacks against U.S. national infrastructures could be severe or catastrophic. The threat of natural disasters and disruptive physical events, such as cable cuts or train derailments can significantly impact the cyber environment with long term effects.

- Government and private sector subject matter experts recognize the urgent need for and value of a 24/7 public-private sector collaborative cyber incident detection, prevention, mitigation, and response capability. A phased implementation approach will allow enhanced capabilities to be implemented in an affordable and efficient manner.

- There is an urgent need to improve upon coordination of existing U.S. and international cyber incident capabilities in both public and private sectors. The need for this capability is growing over time.

- Previous reports recommended establishing a joint coordination center where the public and private sectors could share cybersecurity information.

- The principal required feature of the Joint Coordinating Center must be rich, timely, bi-directional sharing of actionable information between the public and private sectors to detect, protect, mitigate, and respond to cyber threats.

- There is a lack of clear authority and budget responsibility for a public-private cyber collaboration capability; cyber collaboration capabilities currently exist, but are largely uncoordinated. This is the central issue that must be addressed.

- Successful models of public-private sector collaboration currently exist in practice, such as the long history of the NCC for communications-related matters. The NCC model operates within the existing legal and policy frameworks, and should be leveraged as an integral element for future public-private cyber security collaboration.

- Planning and execution of national cyber incident detection, prevention, mitigation, and response capability requires joint participation of many domestic public and private sector organizations, as well as international entities. Presently, organizations involved in cyber incident efforts are physically separated, functionally disjointed, and lack efficient communications capabilities. Combining all stakeholders into a single Government funded/equipped physical location, with the capability for virtual participation, is necessary for full cybersecurity planning and execution.

- The JCC requires a robust, resilient and secure communications system with the critical infrastructure and key resources owners and operators to facilitate the cyber incident detection, prevention, mitigation and response capability.

- Tools, techniques, methods, and procedures must keep pace with and anticipate a rapidly evolving threat.

- No new legal authorities are required for Phase I implementation. Follow-on phases may require additional legal guidance or authorities.

5.0 RECOMMENDATION

1. Based on the authorities and responsibilities established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, the NSTAC recommends to the President to direct the establishment of a joint, integrated public-private, 24/7 operational cyber incident detection, prevention, mitigation, and response capability to address cyber incidents of national consequence.

To establish this capability, the NSTAC recommends the following:

- **Create a Joint Coordinating Center (JCC) as the authoritative place for operational coordination with the private sector critical infrastructure and key resources owners and operators.**
  - Assign Government and private sector representatives to develop the initial JCC CONOPS.
  - Provide full JCC functionality on a phased implementation timeline.
  - Build on the National Coordinating Center model integrated with the U.S. Computer Emergency Readiness Team model and create a joint, integrated public-private, 24/7 operational cyber incident detection, prevention, mitigation, and response capability to address a full range of cybersecurity needs.
  - Provide a dedicated interagency management structure to govern Federal involvement, including designation of a single, authoritative, and accountable office within the Executive Office of the President. This office should have budgetary and management authority across the Federal cybersecurity enterprise.
  - House the JCC in a Government-funded and equipped facility.
  - Establish mechanisms for the U.S. Government and the private sector to protect proprietary information and intellectual property, and to mitigate anti-trust concerns.
  - Provide resilient, redundant, and secure communications to coordinate across all engaged entities and sectors.
  - Before Phase II implementation, conduct antitrust review.

- **Recognize the private sector as a trusted partner.**
  - Conduct a joint public-private sector review to identify any existing mechanisms for robust information sharing.
  - Fully integrate private sector participants into the JCC operational capability on the same basis as government participants.
  - Develop a mechanism and procedures to conduct full, bi-directional information sharing among all JCC participants.
  - Provide tools and system access to all JCC participants to establish a fully collaborative working environment.

APPENDIX A:

Glossary of Terms

APPENDIX A: GLOSSARY OF TERMS

- ***Critical Infrastructure:*** The assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on national, homeland, or economic security, public health or safety, or any combination thereof

- ***Cyber Infrastructure:*** The distributed computer, information and communication technologies combined with the personnel and integrating components that provide a long-term platform to empower the modern scientific research endeavor

- ***Detection:*** Developing an understanding of normal network traffic volume and flow using independent sources will help the JCC participants detect anomalies. Stakeholders will work with partners to obtain external data on threats and vulnerabilities.

- ***Key Resources:*** Publicly or privately-controlled resources essential to the minimal operations of the economy and government

- ***Mitigation:*** Developing the mitigation tools and technology will help stakeholders to address cyber incidents, while ensuring stability within other unaffected networks.

- ***National Security and Emergency Preparedness (NS/EP) Communications:*** Communications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the national security or emergency preparedness posture of the United States.[38]

- ***Next Generation Networks:*** The NGN will logically consist of applications that deliver services, the services provided to users, and the underlying transport networks. … The NGN itself is a capability that will enable many services and applications. Some services will be provided by the network; other services may be external to it, but will depend on it. NGN user-centric services will be delivered over various networks, some of which (such as private customer premises networks and mesh networks) lie outside the wide scope of the Public Network. However, there is no single, universally accepted definition of the NGN exists. … The term NGN is not intended to represent any single configuration or architecture. Instead, it represents the set of converged networks … expected to arise that will transparently carry many types of data and communications and allow delivery of services and applications that are not coupled to the underlying network. However, it is possible to note several key NGN elements or attributes over which there is little, if any, dispute.[39]

- ***Personally Identifiable Information (PII):*** Information that can be used to distinguish or trace an individual's identity (such as their name, social security number, or biometric

[38] NCS Directive 3-1, *Telecommunications Operations Telecommunications Service Priority (TSP) System for National Security and Emergency Preparedness.*

[39] *NSTAC Report to the President on Next Generation Networks*, March 28, 2006.

records), either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

- ***Prevention:*** Developing proper interdiction guidance for prevention activities. Prevention activities include bi-directional information sharing within the IT and communications sectors, and with government (Federal, state and local) and international agencies.

- ***Response:*** Organizing teams, processes, and procedures will help stakeholders to coordinate internal and external sources to respond to and recover from incidents.

APPENDIX B:

Suggested Phased Approach Implementation

APPENDIX B: SUGGESTED PHASED APPROACH IMPLEMENTATION

The table below depicts a possible implementation process for the phased approach:

Suggested Phased Approach Implementation

Phase	Timeframe	Activity
Phase 0	Within 60 Days	Complete initial CONOPS.
Phase I	Within 90 days of CONOPS approval	Implement Phase I joint CONOPS to provide cyber situational awareness and a common operational picture.
		Integrate core Phase I JCC members.[40]
		Deploy controlled communication mechanisms for information sharing and collaboration.
		Identify, develop, and integrate capabilities to establish an operating environment. Some capabilities include rapid collaboration, mitigation, trend analysis, monitoring via watch functions, and shared products.
		Accept/procure data inputs/feeds from other organizations – SANS Internet Storm Center (ISC), Symantec Corporation, McAfee, and others as necessary.
		Ensure legal considerations in Section 3.0 are aligned with future planned activities.
		Establish/review Phase I metrics to measure progress and inform the development of further phases.
Phase II	Within one year of CONOPS approval	Establish training and exercise functions.
		Integrate with other organizations – National Security Agency Threat Operations Center (NTOC), Intelligence Community Incident Response Center (IC-IRC), State/local, tribal, international partners.
		Invite representatives from remaining 18 CIKR sectors.
		Define requirements for additional operational capabilities, including more robust information sharing between the public and private sectors; gather additional legal guidance as needed.
		Update and enhance CONOPS based on experience.
		Ensure legal considerations in Section 3.0 are aligned with future planned activities.
		Establish/review Phase II metrics to measure progress and inform the development of further phases.

[40] Core Phase I JCC members include those entities listed in Section 2.3.

Suggested Phased Approach Implementation

Phase	Timeframe	Activity
Phase III	After one year of CONOPS approval	Define requirements for additional operational capabilities, including more robust information sharing between the public and private sectors; gather additional legal guidance as needed.
		Update and enhance CONOPS based on experience.
		Ensure planned activities are consistent with legal considerations in Section 3.0.
		Establish metrics to measure progress and inform the development of further phases.

Important factors for success include:

- Adequate and appropriate resources (for example, funding, personnel, and collaboration tools);
- Core physical facility with appropriate security and resilient communications and utilities;
- Voluntary private sector representation initially from the banking and finance, communications, energy, and IT sectors with full physical access to the facility; virtual access initially for other sectors;
- Extended virtual participation from both the Government and the private sector over time; and
- Controlled communications mechanisms for information sharing among the private sector and government partners.

APPENDIX C:

Studies and Reports

APPENDIX C: STUDIES AND REPORTS

NSTAC Reports

2008 Next Generation Networks Implementation Annex Working Group Letter to the President
In this letter, the NSTAC stated it had re-examined the previous 2006 Next Generation Networks (NGN) Report to: identify and review current Federal Government efforts that address issues in the report's recommendations; and identify gaps among the 2006 *Report* recommendations, current NGN needs related to the provisioning of NS/EP communications, and existing Federal Government activities, and to provide follow-up recommendations to ongoing work and to enhance future Federal NGN NS/EP activities and implementation actions.

2007 NSTAC Report to the President on International Communications
A key recommendation of the *NSTAC Report to the President on International Communications* was for *DHS to coordinate international planning and development with the appropriate Federal Agencies for adoption of a global framework incorporating operational protocols and response strategies*. This report specified that this framework should *examine, with the help of private sector partners, existing U.S. laws and policies that could prevent service providers and other stakeholders from taking the necessary proactive measures to restore service and prevent harm to NS/EP users for government essential operations during a crisis*.

2006 NSTAC Report to the President on the National Coordinating Center (NCC)
Key recommendations from the NCC report include requesting expanding *the NCC to include both communications and IT companies and organizations. This would be a cross-sector public-private sector facility with a round-the-clock watch, and would be brought up to full strength during emergencies*. Additionally, the report recommended engaging *the private sector in critical infrastructure protection activities by increasing the flow of threat information to the private sector, facilitating private sector participation in impact analyses, and clarifying policies for the protection of private sector information*. Finally, the report concluded by improving *the Federal Government's cyber response strategy to delineate roles and responsibilities of Government and the private sector in the National Response Plan, aligning communications and cyber operations centers, and enhancing relationships with international computer emergency readiness teams*.

2006 Next Generation Networks (NGN) Task Force Report
A key recommendation of the NGN Report was the creation of *an inclusive and effective NGN incident response capability that includes a Joint Coordinating Center, incorporating and modeled on the National Coordinating Center (NCC), for all key sectors, but particularly both the Communications and IT Sectors*.

2005 Next Generation Networks Task Force Near Term Recommendations Working Group Report
This report focuses on convergence and how the Federal Government will meet its needs for national security and emergency preparedness (NS/EP) communications. The report discusses how the Government can meet NS/EP requirements and address emerging threats using the NGN. Many of the recommendations focused on cross-government coordination to track NGN

activity, collaborating with the private sector, and providing greater support to private sector efforts to determine NS/EP risks during convergence.

2003 Legislative and Regulatory Task Force Report on Barriers to Information Sharing
The Legislative and Regulatory Task Force *Report on Barriers to Information Sharing* produced a series of recommendations for the Federal Government action designed to improve information sharing between the public and private sectors.

2001 The NSTAC's Input to the National Plan, *An Assessment of Industry's Role in National Level Information Sharing, Analysis, and Dissemination Capabilities for Addressing Cyber Crisis.*
This report focuses on the need for a recognized, authoritative, national-level capability to disseminate warnings and facilitate response and mitigation efforts for cyber crises across the Nation's infrastructures. Key elements of such a capability spanning public and private sectors should include information collection and sharing, information analysis, dissemination of alerts and warnings, and post-event analysis and dissemination.

1990 Network Security Scoping Task Force Report: Report of the Network Security Task Force
Recommendations from this report include identifying a mechanism for security information exchange and providing steps for Government agencies to improve intelligence information sharing to the private sector and led to the creation of the National Security Information Exchange.

Department of Homeland Security (DHS) Reports and Plans

2009 National Infrastructure Protection Plan (NIPP)
The NIPP addresses the requirements set forth in Homeland Security Presidential Directive 7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection*, and provides the overarching approach for integrating the Nation's many CIKR protection initiatives into a single national effort. It sets forth a comprehensive risk management framework and clearly-defined roles and responsibilities for DHS; Federal Sector-Specific Agencies; and other Federal, State, regional, local, tribal, territorial, and private sector partners implementing the NIPP.

2008 *Comprehensive National Cybersecurity Initiative's* Project 12 Report
A key recommendation from the Project 12 Report, *Improving Protection of Privately Owned Critical Network Infrastructure Through Public-Private Partnerships*, recommended expanding the joint operational capability of US-CERT and NCC to include private sector CIKR sector participation. This effort would eventually include voluntary participation from all 18 CIKR sectors, as determined appropriate by each of the sectors. Co-location of private sector partners could be physical or virtual. DHS is currently implementing the co-location of the NCC and US-CERT.

2007 Department of Homeland Security *Tiger Team Report*
This report was developed in 2007 by Government representatives from NCS and NCSD and industry representatives from the NCC/Communications and IT Information Sharing and Analysis Centers following the NSTAC 2006 Next Generations Report. The 2007 report provided guidance and recommendations on why and how DHS could lead the government and industry in building a fully integrated operational capability to perform cyber and communications security missions in an environment characterized by the convergence of the IT and Communications sectors. The report outlined a three-phased implementation: Phase I called for collocating US-CERT and NCC Watch in a common facility; Phase II called for integrating the operational capabilities of the US-CERT and NCC Watch to create a single 24/7 operational entity that incorporates the current missions of US CERT and NCC Watch, and met CS&C's National-level mission requirements; and Phase III called for inviting other sectors to send representatives to the joint operations center. Phase I was implemented in late 2007/early 2008. The recommendations associated with the Tiger Team's Phase II are consistent with this report's Phase I capabilities.

2007 Information Technology (IT) Sector Specific Plan (SSP)
The IT Sector Specific Plan notes that *public and private sector security partners have an enduring interest in assuring the availability of the infrastructure and promoting its resilience. The IT SSP represents an unprecedented partnership and collaboration between the IT public and private sectors to address the complex challenges of CIKR protection. Public and private sector organizations each represent and bring unique capabilities to the partnership, and derive value from the exchange. Successful CIKR protection is the commitment of IT Sector public and private sector security partners to share information and provide the tools and capabilities necessary for an effective partnership*.

<u>Other Reports</u>

2009 Congressional Research Service Report: *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations*
This report discusses the legal issues and addresses policy considerations related to the Comprehensive National Cybersecurity Initiative, specifically focusing on legal authorities for Executive Branch response to cyber threats, Congressional constraints on Executive action, and policy considerations.

2008 Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency
A key recommendation from the *CSIS Commission on Cybersecurity for the 44th Presidency* focused on redesigning and recasting the Government's relationship with the private sector to promote better cybersecurity.

2008 Internet Security Alliance *Cyber Security Social Contract*
A key recommendation of the Internet Security Alliance's report was the creation of *a social contract wherein government provides incentives for the private sector to make cyber security investments that are not justified by current business plans is a pragmatic alternative*. The report *identified what the government can best do, both long and short term to address these needs and specifies a series of steps the new Administration and Congress can take toward establishing a coherent, pragmatic, effective and sustainable system of cyber security*.

2003 President's National Strategy to Secure Cyberspace

The purpose of this document is to engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact. The *National Strategy to Secure Cyberspace* outlines an initial framework for both organizing and prioritizing efforts. It provides direction to the Federal Government departments and agencies that have roles in cyberspace security. It also identifies steps that State and local governments, private companies and organizations, and individual Americans can take to improve our collective cybersecurity. The *Strategy* highlights the role of public-private sector engagement. The document provides a framework of contributions to secure our parts of cyberspace.

APPENDIX D:

Presentations to the Cybersecurity Collaboration Task Force

APPENDIX D: PRESENTATIONS TO THE CYBERSECURITY COLLABORATION TASK FORCE

Government Presenters	
Presenter	Role
Dr. Peter Fonash	Acting Deputy Assistant Secretary Cybersecurity and Communications, Chief Technology Officer, and Acting Director National Cybersecurity Division (NCSD) Office of the Assistant Secretary for Cybersecurity and Communications Department of Homeland Security (DHS)
Mr. Jeffery Goldthorp	Chief of the Federal Communications Commission's Communications Systems Analysis Division in the Public Safety and Homeland Security Bureau
Ms. Mischel Kwon	Director, United States Computer Emergency Readiness Team (US-CERT)
Mr. Brett Lambo	Director, Cyber Exercise Program, NCSD
Ms. Jenny Menna	Acting Director, Critical Infrastructure Cyber Protection and Awareness, and Acting Director, Global Cyber Security, NCSD, DHS
Ms. Victoria Morgan	Director, Intelligence, Interagency and Networks, Defense Industrial Base (DIB) Cyber Security Task Force
Ms. Jordana Siegel	Director, Outreach and Awareness, NCSD, DHS

Industry Presenters	
Presenter	Role
Ms. Tiffany Jones	Director, Public Policy and North American Government Relations, Symantec
Mr. David Kessler	Senior Corporate Counsel, Symantec
Mr. Marcus Sachs	Executive Director, Government Affairs National Security Policy, Verizon
Mr. Jonathan Spear	Vice President and Deputy General Counsel, Verizon

Other Presenters	
Presenter	Role
Mr. Marcus Sachs	Director, SANS Internet Storm Center
Mr. Matt Ziemniak	Program Director, Cyber Operations Division, National Cyber-Forensics Training Alliance (NCFTA)

APPENDIX E:

Task Force Members, Government Personnel, and Other Participants

APPENDIX E: TASK FORCE MEMBERS, GOVERNMENT PERSONNEL, AND OTHER PARTICIPANTS

TASK FORCE MEMBERS

AT&T, Incorporated	Ms. Juliana Thomas
Bank of America	Mr. Larry Schaeffer
Boeing Company	Mr. Bob Steele
CSC	Mr. Guy Copeland
Harris Corporation	Mr. Richard White
Juniper Networks, Incorporated	Mr. Robert B. Dix, Jr.
Lockheed Martin Corporation	Gen. Charles Croom (Ret.)
Microsoft Corporation	Ms. Cheri McGuire
Nortel Networks Corporation	Dr. Jack Edwards
Qwest Communications International, Incorporated	Ms. Kathryn Condello
Raytheon Company	Gen. Bill Russ (Ret.)
Rockwell Collins, Incorporated	Mr. Ken Kato
Telecordia	Ms. Louise Tucker
VeriSign	Mr. William Gravell
Verizon Communications, Incorporated	Mr. Michael Hickey

OTHER PARTICIPANTS

AT&T, Incorporated	Ms. Rosemary Leffler
	Mr. John Markley
Boeing Company	William Reiner
CSC	Mr. Kenneth Thomas
Deloitte	Col. Gary McAlum (Ret.)
George Mason University Law School CIP	Ms. Maeve Dion
Harris Corporation	Ms. Tania Hanna
Mitre	Mr. Scott Tousley
Netmagic Associates LLC	Mr. Tony Rutkowski
Lockheed Martin Corporation	Dr. Eric Cole
	Mr. Arnie "AJ" Jackson
	Mr. James "Tom" Prunier
Qwest Communications International, Incorporated	Mr. Curtis Levinson
Raytheon Company	Mr. Charles McCaffrey
Science Applications International Corporation	Mr. Hank Kluepfel
	Mr. Steve Lines
Sprint Nextel Corporation	Ms. Allison Growney
Unisys	Ms. Patricia Titus
Valley View Corp.	Mr. Dan Bart
Verizon Communications, Incorporated	Mr. Jim Bean
	Mr. Marcus Sachs

GOVERNMENT PARTICIPANTS

Department of Homeland Security	Ms. Kathleen Blasco
	Mr. Kevin Dillon
	Mr. Ryan Higgins
	CAPT Alice Rand
	Mr. Matt Shabat
	Ms. Jordana Siegel
	Mr. Will Williams
	Ms. Chris Watson
Department of Defense	Lt. Col. Susan Camoroda
Federal Communications Commission	Mr. Gregory Cooke
	Mr. Richard Hovey