Public-Private Partnerships

for Critical Infrastructure Protection

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The last twenty years have been an experiment in how to adapt traditional governmental bureaucracies to a new environment that reflects the growing role of private actors as well as the transnational nature of the world today. One approach to this has centered on the public-private partnership approach as outlined in the Presidential Decision Directive 63 (PDD-63), signed by President Clinton in 1998.

Generally, project-oriented public-private partnerships have been more successful than process-oriented public-private partnerships. The former's missions tend to be more clearly defined, include a definite timeline, and usually enjoy a greater sense of urgency and support among senior leadership. On the other hand, institutionalizing process-oriented public-private partnerships has proved more challenging. The goals of such partnerships are often less clearly defined. Still, some process-oriented partnerships, namely in the financial and IT sectors, have developed sustainable models of success, which will be outlined in greater detail in this report.

Five common elements emerged from an analysis of the various forms of collaboration: senior leadership support, leadership in the partnership, institutional design, incentives and value, and proper timing. Senior leadership support was crucial for the Y2K project to effectively institutionalize collaboration in the financial sector. Senior leadership support facilitates the provision of resources to build up operational capacity, adds urgency, provides assistance in crucial moments, and helps break dependencies. Exercising effective leadership by those implementing the partnership is equally important to achieve early results and form the proper foundation for further growth. Such leadership is particularly important to ensure a smooth transition in the early stages of the partnership.

Still, institutions can only flourish if they have been designed intelligently. Such design includes a sustainable funding model, a clear division of labor, and the identification of appropriate counterparts. Their success is ultimately dependent on the underlying incentive structure, which can be partly influenced endogenously, creating value for the participants early on, and through specific and focused projects. Preferences and the cost-benefit perceptions of the participating actors will ultimately determine the success or failure of the partnership.. A sense of urgency helps to create a bond between the public and the private sectors, fostering a willingness to collaborate and achieve a common vision, ultimately allowing the partnership to mature and endure. The longevity of the partnership depends on the interplay between these factors and is a dynamic process with periods of both weak and strong performance.

The first part of this report outlines a short history of how public-private partnerships for critical infrastructure protection have evolved. The second part constitutes a mapping of the current system. It is followed by an analysis of three examples of collaborative governance, one project-oriented and two process-oriented partnerships. Part four summarizes the lessons learned outlining what makes public-private partnerships work. Methodologically, this research is based on a review of existing literature, complemented by 38 qualitative and semi-structured interviews with experts in government, the private sector, and academia.

Part 1: A Brief Historical Overview

Laying the Foundation: The Clinton Administration. The 1997 report of the President's Commission on Critical Infrastructure Protection put an emphasis on the growing cyber-threat. Many of the Commission's recommendations were implemented a year later through PDD-63. The strategy of PDD-63 focused on a public-private partnership. The President designated lead agencies in the federal government for specific critical infrastructure sectors. Each agency then appointed a Sector Liaison Official and identified Sector Coordinators in the private sector to act as their counterparts. PDD-63 also called for the creation of a single Information Sharing and Analysis Center (ISAC). The original idea was to create a single continuous incident and response information center, focused primarily on cybersecurity. Such an information center did not materialize, and ISACs were instead established by individual sectors.

Existing ISACs can be grouped into two categories. The first category includes those that were created based on existing private or public-private organizations and that were eventually designated as ISACs, such as the North American Electric Reliability Corporation (NERC) and the National Coordinating Center (NCC). The latter stands out as an originally joint public-private entity which designed its private sector meetings as the ISAC after PDD-63. The second category includes those ISACs that were established as new entities, for example in the banking, information, energy, and water sectors.

There also exist different funding models. Some ISACs received funding from the respective lead federal agency, e.g. the Water ISAC from the Environmental Protection Agency and the Electric Services ISACs from the Department of Energy. Some continue to receive federal funding today while others, such as the Department of Energy terminated their financial support. Several ISACs are fee-based service-providers. Ultimately, the ISACs created an umbrella organization, the ISAC Council, in 2003, now known as the National Council of ISACs. Its aim was "to develop trusted relationships among the sectors, and address common issues and concerns."[1]

Cybersecurity was a particular focus in PDD-63 and for the first ISACs. The first ISAC, the Financial Sector ISAC (FS-ISAC), was established in 1999. The Emergency Management and Response ISAC and designation of NCC as the Communications ISAC followed in 2000 as well as the Information Technology ISAC in 2001. The sector specific entities were complemented by a cross-sectoral public-private partnership. In 1999, several private-sector critical infrastructure owners and operators created the Partnership for Critical Infrastructure Security (PCIS) with more than 80 US companies and industry associations. It was incorporated as a nonprofit organization in 2001.[2] PCIS was considered "a joint effort between federal agencies and the private sector".[3] It organized joint public-private meetings and developed white papers to "address potential threats to and vulnerabilities of the computers and information networks upon which our nation's essential services depend", e.g. the 2001 Information Sharing White Paper.[4]

By 2001, four ISACs had been established. After 9/11, there was an important change in focus and eight additional ISACs were created within only two years. The transitional institutional changes after 9/11 were eventually consolidated in the 2002 Homeland Security Act, merging 22 governmental agencies to form the Department of Homeland Security (DHS). One year later, Homeland Security President Directive 7 (HDSP-7) superseded PDD-63 and has since remained the basis for critical infrastructure protection efforts.

HSDP-7 established 17 critical infrastructure sectors. In 2008, Critical Manufacturing was declared a critical infrastructure sector, thus bringing today's sector total to 18. For each sector, HSDP-7 designated a federal agency as the lead agency. This expanded the model under PDD-63, which was limited to a Sector Liaison Official and the Sector Coordinator, not entire organizations. In addition, in 2003 DHS created the US-CERT, based on the model developed by Carnegie Mellon University in 1988.

Consolidating the System: The 2006 National Infrastructure Protection Plan. Michael Chertoff became Secretary of Homeland Security in 2005 and quickly restructured the department. In March 2006, DHS implemented Sec. 214 (b) of the 2002 Homeland Security Act establishing CIPAC which is exempt from the Federal Advisory Committee Act of 1972 (FACA). FACA was created to make advisory bodies transparent and their meetings and written material available to the public. However, DHS "concluded that concerns regarding the Federal Advisory Committee Act (FACA) have frustrated vital communications between DHS and critical infrastructure sectors" and therefore decided to create the Critical Infrastructure Partnership Advisory Council (CIPAC).[5] Information-sharing is not the only activity covered by CIPAC. Its charter also includes planning, coordination, security and resilience program implementation, operational activities, and information sharing. CIPAC is not a new organization, but offers a model for public-private partnerships today. The implementation of CIPAC's charter is considered a milestone in the public-private partnership sector.

In 2006, DHS also published the National Infrastructure Protection Plan (NIPP) after an interim plan was released in 2005. NIPP highlights that a voluntary public-private partnership approach continues to be the primary means to protect the nation's critical infrastructures.[6] It expands coordination mechanisms by creating Government Coordinating Councils (GCC) for each sector with a designated lead agency. The GCC corresponds with the Sector Coordinating Councils (SCC) on the private side, which are self-organized and self-governed by private sector members. With the choice to establish new SCCs instead of relying on existing ISACs, HSDP-7 explicitly "declined to endorse the ISACs as the primary interface with the private sector. In fact, DHS conspicuously distanced itself from the ISAC model when it promoted the creation of Sector Coordinating Councils. As mandated by executive order (HSDP-7), the councils were set up to be more inclusive than ISACs and to allow any company or association operating within a sector to become a member for free."[7]

PCIS was recognized as the Private Sector Cross-Sector Coordinating Council in the NIPP for the cross-sector dimension. PCIS also provides input to the President's National Infrastructure Advisory Council when requested. Its counterparts on the government side are the Federal Senior Leadership Council (FSLC) and the State, Local, Tribal and Territorial Government Coordinating Council (SLTTGCC). CIPAC is the legal framework for both the sector-specific and the cross-sector public-private collaboration. The creation of the Cross-Sector Cyber Security Working Group in 2007 was a sign of the rebalancing of attention between the physical and virtual threats after the 9/11 attacks.

Part 2: Mapping the Current System

Today's critical infrastructure protection system consists of a myriad of entities. Some, such as the National Communications System, date back to the 1960's. Others, such as the National Cybersecurity and Communications Integration Center (NCCIC), were established as recently as

2009.

DHS is the lead agency when it comes to critical infrastructure protection. It oversees the NIPP, which outlines the status quo of the historically grown system. In 2009, DHS released an updated version of the 2006 NIPP but “t~~T~~he Obama administration has, to date, kept in place much of the policy and organization of the Bush Administration.”[8] According to DHS, “The NIPP uses the SCCs, GCCs, and the cross-sector councils as the primary forums for coordination of policy, planning, training, and other requirements needed to ensure efficient implementation and ongoing management and maintenance of the NIPP and the SSPs.”[9]

The changes in the 2009 NIPP focused on strengthening protection at the regional level through the Regional Consortium Coordinating Councils and an increased emphasis on resiliency, the focus upon which is now at par with protection.[10] The SCCs today have a larger membership than the respective ISACs. The structure of the SCCs’ relationships with the previously existing ISACs differs among sectors. The Homeland Security Information Network is also being expanded to cover all critical infrastructure sectors—therefore covering the physical threat dimension in addition to US-CERT’s cybersecurity mission.[11]

The most recent innovation is the establishment of the National Cybersecurity & Communications Integration Center (NCCIC), a 24x7 watch center and national response center focused on a common operating picture for cyber and communications networks. It brings together the previously fragmented operational capacities, including the US-CERT, ICS-CERT, the NCC, the FS-ISAC, IT-ISAC, MS-ISAC and representatives of various federal agencies.[12] While there are still some challenges the NCCIC needs to overcome in its infancy, Denise Anderson, Vice President of the FS-ISAC, points out that “A positive effect of the NCCIC and having people from government and the private sector side-by-side on the floor is that the government realized how often the financial sector, for example, is attacked and the level of expertise within financial institutions, which helped foster an understanding and appreciation for the sector’s capabilities”.

In addition to DHS and the NIPP partnership model, there are several Presidential advisory bodies. They constitute the most senior level public-private partnerships and focus on high level strategic advice. The requirements regarding transparency and information sharing differ from the NIPP system. For example, the National Infrastructure Advisory Council (NIAC) meets under FACA rules, whereas SCC and GCC meetings are exempt under CIPAC, which implements section 871 of the 2002 Homeland Security Act. The President’s advisory bodies usually produce reports as tangible outputs. The key advisory bodies for critical infrastructure protection are the NIAC and the National Security Telecommunications Advisory Committee (NSTAC).

NIAC was established by PDD-63 and was originally named the National Infrastructure Assurance Council.[13] It never met under its original name and was replaced in 2001 by the NIAC after President Bush assumed office. It focuses on “enhancing public-private partnerships, monitoring the development of ISACs, and encouraging the private sector to perform periodic vulnerability assessments of critical information and telecommunications systems.”[14] The NIAC meets four times a year under FACA rules and has reported to the President through the Secretary of Homeland Security since 2003.[15]

The National Security Telecommunications Advisory Committee (NSTAC) was created in 1982 and advises the President on telecommunications matters that are relevant to national security. The Committee provides information and advice on national security communication capabilities and their effect on national security. The FACA provisions are performed by the Secretary of Defense on behalf of the President, as applicable except reporting annually to Congress.[16] The CSIS Commission on Cybersecurity for the 44th Presidency recommended merging NIAC and NSTAC, but they have remained separated bodies.

There are three other potentially relevant presidential advisory bodies. The first is the President's Council of Advisors on Science and Technology which dates back to 1933 and advises the President on general issues pertaining to science and technology.[17] The council's meetings are publicly broadcasted and fall under FACA rules. The second relevant body is the President's Intelligence Advisory Board, set up in 1956 as "a nonpartisan body, independent of the Intelligence Community" assessing the work of the intelligence organizations.[18] The third relevant advisory body is the President's Working Group on Financial Markets, which was established after Black Monday in 1987.[19] The Financial and Banking Information Infrastructure Committee serving as the Government Coordinating Council in the banking and financial sector was chartered under this group.[20] A similar body exists at the departmental level in the form of the Homeland Security Advisory Council, which advises the Secretary of Homeland Security. It includes a subcommittee named the Private Sector Senior Advisory Committee.

Part 3: Analysis of Select Public-Private Partnerships

The following three case studies examine successful partnerships. The first examines the Y2K efforts, a public-private project to fix the millennium bug before the old century ended. It identifies key drivers of project-oriented partnerships. The second and third case studies focus on process-oriented partnerships designed open-endedly. They face specific challenges because some of the key factors driving the success of project-oriented partnerships, such as a sense of urgency and the resulting sustained support from senior leadership, are harder to replicate. As Manuel Suter from the ETH Zuerich points out, "information sharing is too abstract. Projects like common exercises are easier to sell as deliverables." Yet, there are also useful lessons how process-oriented partnerships can be successful over time.

Y2K: A Successful Public-Private Project

In July 1996, President Clinton received a letter from Senator Daniel Patrick Moynihan warning of a "Year 2000 Time Bomb."[21] The time bomb, also known as the Y2K threat, was a problem in the software code of early computers. Due to the need to squeeze data and minimize storage, programmers often only used the last two digits of a year omitting the "19". With the advent of the new century, many computers had no instruction how to distinguish 1900 from 2000. This created a major headache for the government and multiple private sector industries (including financial services) in the run-up to January 1, 2000. The project to fix the software bug concluded successfully after an extraordinary joint effort by the government and the private sector during the late 1990s. Y2K became a non-event, due in part to these collaborative efforts. According to John Carlson, Executive Vice President of BITS/Financial Services Roundtable "Y2K was an important test case for both the private and public sectors in learning how to collaborate ...the effort included assessing the risk, remediating software code, testing, overseeing vendors, coordination with other inter-dependent sectors, and communication with customers." Mr. Carlson worked closely with the financial services industry to address the challenge as part of the regulation team in the late 1990s.

President Clinton created the "Year 2000 Conversion Council" chaired by John Koskinen, assistant to the President, in February 1998. Later that year, Congress passed the "Year 2000 Information and Readiness Disclosure Act" (the Act). What followed has been described as "interagency and government/private sector cooperation not seen since World War II." More than $100 billion was spent in the US alone.[22] According to the White House Information Coordination Center, "after the stunning success of the millennium rollover, some have referred to Y2K as a non-event."[23] Whether the non-event was the causal effect of successful Y2K efforts or rather a sign that they were a gargantuan waste of resources,[24] the level of public-private cooperation remains outstanding. The question is how?

The efforts to prepare for January 1, 2000 had a clear goal: fix the millennium bug. The emphasis was on solving a one-time problem rather than institutionalizing the partnership for other purposes thereafter. The project's success is due to several factors. First, leadership is crucial to create legitimacy and support.[25] The National Y2K Information Coordination Center identified leadership as the most important among its 39 best practices.[26] "The leadership must have a vision; communicate that vision to all parties involved, and support people in its development and implementation."[27] In the Y2K example, the attention and support from senior leaders existed across the board. The President signed an Executive Order and created a new office at the highest level of government to coordinate the efforts among agencies. Moreover, White House efforts were supported by a bipartisan legislative act which took Congress only three months to pass after being introduced in July.[28]

Second, there was a clear vision and sense of urgency. The vision was primarily set exogenously by the technological situation: the problem was clear and the technical solution fairly straightforward. According to the Act, the goal was "Reprogramming or replacing affected systems before the problem incapacitates essential systems [which] is a matter of national and global interest." That is why the key challenge was not an information technology issue but a management issue of how to fix the problem using a large, international solution. Regarding the means to achieve this end, the Act read "The national interest will be served by uniform legal standards in connection with the disclosure and exchange of year 2000 readiness information that will promote disclosures and exchanges of such information in a timely fashion."

The Act included anti-trust exemptions, special liability provisions and protection of information submitted as so-called "Year 2000 Statements", caps on punitive damages, as well as a sunset clause for the national year 2000 website that the Administrator of General Services was required to maintain until July 14, 2002, under section 9.[29] The Global 2000 Coordinating Group created a country ranking that they shared with regulators and government leaders around the world (and inadvertently on C-SPAN, which broadcasted a hearing in the Senate on the topic) as part of a naming and shaming mechanism. A similar ranking was compiled for individual sectors in the United States.

Operational capacity was also a major concern. The Information Coordination Center at the White House, for example, "was created from essentially zero in March (three people, no budget) into a trained and exercised operational facility in December complete with communications and software staffed by 36 core personnel, 400 detailees from government and private infrastructure and 160 contract support personnel in two 12-hour shifts gathering information from well over 2000 sources on a phenomenon no one had ever seen before."[30] IT departments in the private sector spent a majority of their time and resources in 1999 on Y2K while the industry set up National Information Centers for critical infrastructure. Moreover, two dozen CEOs of Fortune 500 companies formed the Senior Advisors Group meeting with the President's Council on a bi-monthly basis to address cross-sector issues. Importantly, financial resources in the billions of dollars enabled the fast built up of operational capacity. These efforts even extended beyond national borders. The International Y2K Cooperation Center established in Washington in March 1999, and led by Bruce McConnell and the Global 2000 Co-ordinating Group in the private sector, addressed the international dimension of the problem.

In short, the Y2K efforts are an example for a successful project-based public-private partnership with many practices and lessons learned that can be adopted for similar enterprises. The attention by senior leadership created a clear vision and authority for the officials tasked to solve the problem in a limited amount of time and provided the resources to build an operational capacity for that purpose. Eventually, the institutions and processes established to address the Y2K problem were disbanded. The exemptions in the Act expired, the International Y2K Cooperation Center closed as well as the National Y2K Information Coordination Center. According to Jim Devlin, now an independent risk management consultant serving as FSSCC Secretary, "Organizations like the Global 2000 Coordinating Committee were always planned to phase-out, which was also part of the reason large institutions could be convinced to dedicate substantial human and financial resources to them". There are limits to replicate this particular success for process-oriented collaborations. The antitrust exemption, for example, lasted only temporarily from October 19, 1998 to July 14, 2001.[31] Making such anti-trust exemptions permanent is a much more difficult political objective to implement.

<u>Lessons Learned:</u>

- Create a sense of urgency and use triggering moments as windows of opportunity
  Looming deadline of January 1, 2000, and Y2K bug

- Lobby for and secure senior leadership support from the start
  Senator Moynihan's letter to the President, President's support, CEO support

- Include senior leaders for crucial situations throughout the collaboration
  Vice President Gore's participation in meeting with failing agencies

- Use senior leadership support to gain access to necessary financial resources
  Support from CEOs freed private sector capital to support efforts

- Create legal environment that allows necessary actions to be taken
  Temporary exemptions of the Year 2000 Information and Readiness Disclosure Act

- Focus on interdependencies and international dimension
  International Y2K Cooperation Center and Global 2000 Co-ordinating Group

The Financial Sector: A Successful Collaboration over Time

The efforts by the financial sector to institutionalize critical infrastructure protection as an ongoing process have been a model for other sectors. The crisis playbook with a standard set of operating processes and guidelines is considered exemplary and the sector is currently working on a white paper on risk mitigation of Advanced Persistent Threat.[32] Moreover, the FS-ISAC is widely considered to be a success. Officials from the Treasury do not outright recommend but quietly suggests to financial institutions who are not yet members of the FS-ISAC to explore its work. In 2012, the commercial facilities sector was planning to tap into the FS-ISAC for its own needs which includes a round the clock Security Operations Center.

A sense of urgency drove the creation of the FS-ISAC, which was the first ISAC to be established after PDD-63. Y2K was the triggering moment that added this sense of urgency, and the leadership exercised as part of the Y2K efforts produced crucial positive spill-over effects for simultaneous efforts to strengthen critical infrastructure protection. The FS-ISAC continued to exist after Y2K; unlike the Information Coordination Center at the White House, which disbanded after Y2K. After January 1, 2000, the sense of urgency subsided. Then the 9/11 attacks happened. Most officials still knew whom to call, even though more than a year had passed since the Y2K institutions had been disbanded, and they applied the lessons and practices learned from the Y2K effort to the challenge presented by 9/11.

The financial sector also realized the importance of creating regionally-based partnerships, establishing Chicago FIRST in 2003. This contributed to the integration of the element of regional partnerships in the NIPP later on as Christopher Terzich, Chair of the Regional Consortium Coordinating Council points out.

Recognizing the important of leadership, the search for exceptional leaders continues to be a primary objective for the FSSCC. When the FSSCC seeks new leadership, it engages not only with its members, but reaches out to the top leadership of their member's institutions to secure their help in keeping the FSSCC going. As one of the experts interviewed for this study states that "this is critical because it is necessary to invest resources... it is almost like a self-imposed tax for the sector, but we made it work."

The institutional design also proved crucial. The FS-ISAC's proportional fee structure has been particularly effective at creating a sustainable funding flow for the ISAC. There are seven different types of members, ranging from Critical Information Only Participants that do not pay a fee and receive only urgent and crisis alerts, to Platinum Members who enjoy the full range of services and the right to participate in board meetings.[33] It allows a smaller institution to get access to information produced by the ISAC, increasing its reach throughout the sector, while larger institutions are also eligible to serve on its governance bodies. Further, while the ISAC is a separate entity, it is part of the FSSCC's membership. The institutional design has therefore created an incentive structure diversified enough to create value for small and large entities alike while being tailored to a diversity of needs. The maturity of the FS-ISAC becomes clear when considering Anderson's comment that "a few years ago, we'd celebrate when information sharing occurred at all. Today we are inundated with information shared by our members, who realize the value of information sharing."

How information is shared among sector members is another important component of institutional design. Scott Algeier, Executive Director of the IT-ISAC, for example, describes the IT-ISAC's culture as one where threat information shared with one member will be shared with all members. The FS-ISAC has a different philosophy expressed in its membership categories. These different approaches have direct implications. For example, the IT-ISAC wanted to join the Defense Industrial Base information sharing pilot project.[34] However, the IT-ISAC could ultimately not do so because information through the project would have been shared only with specific members which would have been inconsistent with the IT-ISAC's Member Agreement. Some FS-ISAC members, on the other hand, could participate individually and the government determines which banks are the most critical and work only with those select members of the financial sector for this specific program. The FS-ISAC includes an anonymous online submission tool and uses a traffic light system to classify information along the spectrum from specific to broad group. The system is similar to the Network Security Information Exchange (NSIE) information sharing levels in the telecommunications sector which has been adopted by US-CERT.[35]

Classification	**Target Audience**
Red	Restricted to a defined group (e.g. only those present in a meeting), should not be shared with anyone outside of the group
Amber	May be shared with FS-ISAC members.
Green	May be shared with FS-ISAC members and partners (e.g. DHS, the Treasury and other government agencies and ISACs), is not to be shared in public forums
White	May be shared freely and is subject to standard copyright rules
Source: FS-ISAC Operating Rules 5.6 (c)	

The two different approaches are not necessarily exclusive, and both are challenges faced by government. The U.S. Department of State's 'no double standard policy' is an example on how to decide if information should be shared to either a specific group or a broad group. It is based on the 1990 Aviation Security Improvement Act (49 U.S.C. 44905).

There continues to be a concern regarding information sharing between the private and the public sector, though. Paul Smocer, President of BITS/Financial Services Roundtable, pointed out in his testimony on June 1, 2012 "some are concerned that information exchanged will not be protected and will subsequently be revealed... while true even with private-to-private sharing, this is especially true with private companies sharing information with public entities ... private organizations are concerned that revelation of the information will impact their reputation and the confidence of their customers – regardless of their industry."[36]

The architecture of the FSSCC also exhibits a thorough thought-process. Its formal structure as a LLC was set up to formalize roles and to create repeatable processes. The leadership was initially set up for Vice-Chairs to be the Chairs in waiting to ensure continuity in leadership. As one interviewee points out, "other councils change their entire leadership and sometimes have to start from scratch." The processes are reinforced by the culture and interdependencies in the sector. The interviewee adds that "there is an amazing interdependence that is not competitive in the sector. The big banks, for example, all clear trades for each other." The FSSCC does not charge fees and is based on its member's contribution of time and expertise. It counts 52 members consisting of financial institutions and associations including clearinghouses, commercial banks, credit rating agencies, exchanges, insurance companies, investment banks, retail banks, and electronic payment firms.

The financial sector's relationship to the government has been described as very good by people interviewed for this study, both from the financial sector and other sectors. As one private sector representative points out "We always seek input from the Treasury. They have a seat, not necessarily a voting seat, but they have a seat at the table." The Treasury also honored the private sector leadership of the FSSCC by awarding the title of Sector Coordinator to its elected chair. According to Greg Garcia, former DHS Assistant Secretary for Cyber-security and Communications, this was done as a special recognition of the importance of the position. However, about three years ago the interpretation of its authority under HSPD-7 changed, and the Treasury no longer appoints a coordinator.

These initial decisions created a path dependence that has put the partnership in the financial sector on a sound footing and allowed it to build and enhance its operational capacity over time. The sense of urgency that existed during Y2K and the 9/11 attacks fostered the early initiatives. These became institutionalized and sustainable as a result of a continuous funding flow and quality leadership. These institutions have been maturing for more than a decade, reaching an operational capacity valued by government and other sectors.

The expertise built in the financial sector is sought by other sectors, who hope to emulate its success. The FS-ISAC has been working with the aviation sector to establish an Aviation-ISAC, and has been advising the oil and gas sector. The latter originally had an ISAC coordinated by the American Petroleum Institute, the Energy ISAC, but this no longer exists.[37] The organization was dissolved when "due to the loss of funding from the Department of Energy, SAIC is no longer provid[ed] services to the Energy ISAC organization."[38] It seems that the industry had no incentive to provide the resources on its own at the time, in spite of the monetary and human capital available in the energy sector. The threat landscape, or the perception thereof, seems to have changed recently, however. The reporting on cyber-attacks against oil and gas infrastructure earlier this year has helped recent efforts to revive ISAC.[39]

Lessons Learned:

- Create a sense of urgency by bundling similar challenges
  FS-ISAC created in response to PDD-63 but mission to "prepare for Y2K"
- Use senior leadership support in one sector to secure senior leadership support in another
  The Treasury Department reaching out to CEO of Citibank
- Select good managers/leaders for implementation
  John Reed's selection of Rhonda MacLean
- Create value from the start
  Rhonda MacLean's efforts to demonstrate how each sector can add value
- Focus on leadership transition
  The smooth leadership transition from Rhonda MacLean to Don Donahue
- Develop sustainable short-term and long-term funding model
  The proportional fee structure designed as a long-term sustainable funding model
- Create flexible information-sharing system directing information to where it is needed
  Creation of the traffic light protocol

The UK Experience: Focusing on the Basics

The United Kingdom is one of only two countries among the 27 members of the European Union with a national agency dedicated solely for critical infrastructure protection.[40] Its Centre for the

Protection of National Infrastructure (CPNI) is an interagency center that merged two governmental bodies in 2007 and builds on the UK's counter-terrorism efforts. The UK's Parliamentary Office of Science and Technology highlights that "there is a consensus that CPNI has good relations with private sector operators within the critical national infrastructure." The UK case study therefore offers some best practices which have already been emulated elsewhere in Europe.[41]

The CPNI mission statement reads "CPNI's protective security advice is aimed at reducing the vulnerability of the critical national infrastructure to national security threats such as terrorism and espionage. The context in which these threats are addressed at national level is outlined below. Advice covers physical, personnel and information security, and includes cyber security."[42] It receives resources from the government, the private sector, and academia. It posts its publications on its website and also organizes closed information sharing sessions with the private sector and conducts risk assessment reports.[43]

According to a European Commission report, "although there are many information sharing programs underway across the EU, the most commonly cited program was the Information Exchange model developed and implemented by CPNI in the UK".[44] In the United States, NIAC also took note of these efforts giving a statement "that the United Kingdom has successfully accomplished the exchange of risk information, even among competitors. The system uses Chatham House Rule, which requires that participants refrain from discussing who shared the risk information and instead focus on how to mitigate the risk."[45]

So how have the information exchanges been able to build a trusted community? First, the exchanges have had time to mature. The first exchanges date back to 2003.[46] Second, their role is different from and, arguably, created lower expectations compared to those for ISACs. While the latter focus on analysis "IEs operate on a basis where the free flow of information in the meeting is prized as the output. ISACs, by comparison, include more explicit provisions for the capture of data for reports, analysis and product as an output" according to the European Network and Information Security Agency.[47] Finally, they are built on a set of basic and specific rules, namely,

- No cost to members
- 2 members per organization
- Designated members cannot delegate participation (the same members must be present at every meeting)
- Membership determined by existing members
- CPNI provides co-chair and co-ordinator and hosts meetings
- Meetings are held every 6-8 weeks
- Meetings are face to face
- Meetings are held under Chatham House Rule
- Information sharing protocol agreed by all members

- Trusted group of industry and government representatives[48]

The information exchanges in the UK were modeled after the National Security Information Exchanges in the U.S, but lessons learned from their implementation are now flowing back to the US.[49] Interestingly, the NSIEs have similar rules. According to Garcia, these rules are "are all about trust. The same person must attend meetings, the meetings are in person, information must be actionable, no note taking is allowed, and the meetings generally follow the Las Vegas rule – what happens in the room, stays in the room."

Moreover, membership in the NSIEs was limited from the beginning because of a concern that if the membership was too large, trust could not be built and there would be a negative effect on operations.[50] At a theoretical level this concern corresponds with the argument put forth by Professor Robin Dunbar, an anthropologist at Oxford University. Professor Dunbar advances the idea that there are natural limits and rules governing social relationships and trust among humans. This also explains the recommendation by the Intelligence and National Security Alliance that "an effective partnership has a representative group of members, large enough to be sufficiently inclusive, but small enough to retain the ability to act quickly."[51]

At the same time, some of the concerns in the UK resemble those found in the literature and interviews pertaining to the US experience. How can smaller operators be reached? How can access to relevant information be provided to those who need it? How can assistance be given to operators that lack expertise to implement guidance?[52] How can senior management be convinced to invest in security? Chatham House, for example, writes in a report that "in one case senior management had little sense of the company's unmitigated cyber dependencies, and when ICT staff raised concerns they were told that no further funding was available."[53] Differences in the level of maturity also exist in the UK. The Institution of Civil Engineers highlights that "while some sectors, notably water and parts of the power network have well developed resilience policies and procedures to address risks, the development in other areas is not as mature."[54]

Lessons Learned:

- Focus on agreeing basic rules to build trust
  Rules to keep group relatively small requiring regular attendance and face-to-face interaction in order to build a relationship of trust over time (and potentially rules governing expulsions in case of repeated absence similar to the bylaws of the ITSCC)

- Provide possibility to submit information anonymously
  Chatham House rule applying to Information Exchange; FS-ISAC also provides possibility to submit information anonymously

- Manage expectations
  Information Exchanges set up to increase flow of information rather than analyze data compared to ISACs lowering expectations at the beginning of the partnership

- Learn from experience in other countries
  The UK information exchanges were modeled after the NSIE in the US and some of the UK lessons learned are now spilling over back informing improvements to the system in the US

Part 4: What Makes Public-Private Partnerships Work

The five key elements of success are: (1) senior leadership support, (2) leadership in the partnership, (3) institutional design, (4) incentives and value, (5) timing - urgency and maturity.

1. Senior leadership support for the partnership

Support from senior leadership was crucial in the cases that were viewed as successes, ranging from the Y2K efforts to more recent efforts, such as the initiative developing "Principles for Voluntary Efforts to Reduce the Impact of Botnets in Cyberspace."[55] Importantly, leadership support must go beyond the initial development phase. "Leadership is very important. You need someone who is a champion of the effort and who is willing to dedicate the time and resources to start, and perhaps more importantly, to institutionalize it so it lives beyond the leaders who created it," Brian Tishuk remarked, looking back on nearly twenty years of government experience and on his current role at ChicagoFIRST. The successful and smooth transition from the first to the next generation is a particularly fragile moment that requires particular attention and leadership.

Senior leadership support was also crucial for the larger exercise to establish the FSSCC to secure the industry's infrastructure. Representatives from the private sector pointed out that the Treasury's leadership was important to kickstart the efforts and that Bank of America CEO Ken Lewis not only committed to take the lead on the private side but followed the mantra "If we do this, let's do it right". As a result, Bank of America lead the effort to set up the council and dedicated two full-time staff members for a period of two years to support this effort. In addition Bank of America employee, Rhonda MacLean, became the Sector Coordinator in 2002.

In the private sector, such leadership support is particularly important. This is because suggestions by the CSO or CSIO on how to improve security may not always have the ear of the senior management leadership. Sometimes corporate security officials face the challenge of how to effectively leverage their authority internally. That is also why NIAC's recommendations have focused on creating more senior executive level involvement for years. In its 2012 report, it highlights that "there is currently not an effective process to engage – in a systematic and *sustained* manner – senior executives in the private sector with their counterparts in government".[56] Reiterating the point Greg Wilshusen, Director of Information Security Issues at the GAO, makes about "evidence that many senior executives do not fully appreciate the risks their companies face from sophisticated, emerging cyber threats," Garcia suggests that companies should have staff members devoted to the issue of critical infrastructure protection full-time in addition to providing them with authority.

2. Exercising leadership in the partnership

In addition to support from senior leadership, officials implementing the partnership must also lead. A lack of leadership at this level and the lack of institutionalizing collaborative efforts can have significant adverse effects, as experiences in the chemical sector shows. In 2002, the chemical sector designated the American Chemical Council's CHEMTREC as its official ISAC.[57] A few years later, this arrangement ceased to exist. Today the chemical sector no longer has an ISAC.

A key tool for any leader is to create a sense of urgency. "You need a deadline of some sort. If everyone works on the same objective with a deadline looming ahead, it channels energy, speed and direction" Devlin answered when asked about what makes public-private partnerships work. Such urgency can emerge exogenously through a triggering event, such as the 9/11 attacks, Hurricane Katrina, the Times Square bombing attempt, etc. But it can also be shaped by leaders themselves, for example by highlighting a change in the threat landscape or framing the urgency of a particular problem. Thomas Farmer, Assistant Vice President for Security at the Association of American Railroads, highlights the importance of defining a concise, readily understandable strategy and formulating clear goals to attain its fundamental priorities. Translating the urgency into specific objectives is the next important step to maximize the heightened attention and activity.

Effective leadership is important to improve management. There appears to be a lack of basic processes institutionalizing follow-up, feedback loops, the creation of institutional memory, and fostering bureaucratic learning. These processes do not take place automatically but require the active involvement and support from senior officials to integrate the time and resource investment into regular work streams. Kathryn Condello, Director for National Security and Emergency Preparedness at CenturyLink, points out that "the government's institutional memory is very weak" as a result of the staff turn-over. Some of the weaknesses identified in the first Cyber Storm exercise, a cyber-security exercise organized by DHS, continued to appear during Cyber Storm III, such as the role of standard operating procedures and the understanding of alert levels.[58] This arguably occurred because by the time one planning cycle concludes the next has already begun, without the implementation of the lessons learned from the previous one. These are not problems inherent to critical infrastructure protection or public-private collaboration; rather they are general management and organizational issues that need to be addressed by both sides.

One explanation for this finding is a fragmented accountability mechanism in the partnership model. GAO, for example, has no authority over the private sector. Its study depended on voluntary cooperation by the private sector. The private sector, on the other hand, cannot measure the government's performance. "Where is the accountability for monitoring that lessons learned are implemented and processes improved?" Symantec's Cheri McGuire asks. Yet neither side has an incentive to call for an accountability system. Independent third parties, such as think tanks and universities, can only fulfill this role in a limited capability, facing either classified or proprietary information. This ultimately leaves the public on the losing side. Mainstreaming independent oversight and accountability mechanisms is urgent and important.

According to Todd M. Keil, former DHS Assistant Secretary for Infrastructure Protection from 2009-2012,

> "A partnership must offer something unique, so both sides benefit. The Overseas Security Advisory Council (OSAC) has been very successful because its agents are around the world and can provide real time information and unique value no one else can replicate. For each sector there is something unique, but the challenge is to identify what this issue is for each sector and for both sides. That is why, when I assumed my new position, I started looking at intelligence information sharing. I knew based on the example of OSAC that there must be a unique value. So when I looked at OIP's clearance program, I realized that the office was supporting 1,200 clearances without actually using them. It was more of a resource if need be rather than using them on a regular basis. That is when we created the Engagement Working Group.
>
> The goal of the Engagement Working Group is to determine if information needs to get shared

> more broadly with private sector representatives. The first meeting included 15 government officials and 8 private sector representatives to discuss the threat and whether and whom to share the information with in the private sector. Importantly, the Engagement Working Group is not a set group of people but a mechanism. People still tend to misunderstand though and complain why they were not part of a specific meeting. But it is a structure set up to come together to discuss threats specific to specific sectors. At the same time, we always have someone from PCIS present to ensure that there is someone participating representing all sectors.
>
> With regard to the legal dimension, there is no blanket authorization. Each meeting requires individual authorization. Moreover each member participates to inform the decision-making process representing the sector and not the company or association. Every meeting opens with a briefing outlining the informal rules of the road and stressing that each member represents the sector and not a company and that, in case of a follow-up meeting, the same person is required to attend and not a surrogate. This holds even if the proposed surrogate also holds a clearance. You need the same person who has the same knowledge as a group. There were three instances when threats emerged where the group decided that the information needed to be shared in a classified setting and a team was sent around the country to brief people. The 'Seven Cities Briefing' was one of them. Sometimes these briefings would take place in the SCIF of the Secret Service, a fusion Center, or in one case a military facility. But there were also instances when private sector officials advised not to share information because there was not really anything the sector could do with it and that it will only create confusion. I was surprised about that because I anticipated they would say to share everything. It was a sign that this was working."

3. Institutional design

Smart institutional design is key to early efforts, and for providing a framework able to survive periods of weak leadership. Models in the financial sector have been particularly influential for other sectors, but its representatives were among the first to highlight that these models might not work for other sectors. In some sectors, foodstuffs among them, ISACs were created and eventually discontinued. Other sectors, like commercial real estate, are reorganizing their sectors. But even mature models such as those in the financial sector continue to be under scrutiny. So while it is tempting to apply a template across the board, the current system has created a pushback against a one-size-fits-all approach. As Condello highlights, "I am on call 24/7. But do all 16 sectors need a 24/7/365 ISAC? Unclear. Do all sectors need a presidential advisory body? Also unclear."

A key challenge is aligning the policy and operational aspects between the private and public sector. Roger Callahan, one of the architects of the system in the financial sector, now Managing Director at Information Assurance Advisory LLC, points out, "Looking back, I think, we made a mistake. We created the ISAC and SCC as two independent entities instead of putting the ISAC under the SCC. The SCC would do the strategic thinking about big problems, and the ISAC would focus on operational aspects. But if you create two separate institutions with independent authority to go their own way, they will go their own way. Greater synergetic benefits could have been achieved with a single executive board and a common governance structure."

This seems to be reinforced by the view expressed by Anderson that "an ISAC is in no way subordinate to a SCC, but should be seen as a partner in helping to shape operational strategy and policy. For example, the FS-ISAC was founded long before the FSSCC and in fact has a more robust legal and financial framework." These path dependences can also create tension though. McGuire explains that "the IT-ISAC is the designated operational arm of the IT-SCC, but there are also frictions since the SCC has 80 members but the ISAC has only 20 dues paying members. This puts a financial constraint on the ISAC which shares some of its data with all

SCC members." Her comment also showcases how the IT-ISAC's relationship with the IT-SCC is an interesting example of a positive externality and beneficiary spill-over effect of information from the ISAC to the larger SCC. Angela McKay, Senior Security Strategist at Microsoft, highlights the importance of grouping expertise among experts to focus on the policy, operational, and legal aspects to maximize everyone's contribution and minimize such conflicts.

Choosing the optimal institutional design from the start pays off before path dependencies can develop, creating additional barriers to reform down the road. The Food and Agriculture Sector faced these challenges when "conflict among the sub-councils kept the FASCC from electing leadership for a very long time and only recently did the FASCC decide that this was a necessary evil".[59] As Keil points out "an important feature when the SCCs were established was that government did not dictate the structure and membership of the SCCs. It was up to the private sector representatives in each sector to determine that based on their specific sector needs. So if a SCC is not working well today, then the sector members have the ability to improve the SCC themselves by changing its governance structure."

A second dimension is the selection of counterparts, namely the relationship between the private sector and regulatory agencies. This can be designed to be mutually beneficial if the right firewalls are in place. Identifying the adequate counterparts within a government agency and a corporation is crucial, particularly as critical infrastructure protection is a concern shared among the participants. Several experts also highlighted that career bureaucrats are better suited for such positions when compared with political appointees who, on average, leave after two years. The former are able to provide the continuity across administrations considered crucial by the experts interviewed for this study. NIAC also points out that political appointees' "lack of critical infrastructure subject-matter expertise can seriously hamper the process of analyzing intelligence."[60]

There does not seem to be a standard recipe as to whether the relationship between a sector and its governmental counterpart is working. Experts interviewed for this study said it boils down to two factors: either the private sector was already regulated and had an established relationship with its regulator by the time critical infrastructure protection became a priority (for example the financial or telecommunications sector) or this did not exist and both, the private sector and the governmental counterpart, had to collaborate from the beginning (for example the IT sector). The 2008 Critical Infrastructure Partnership Strategic Assessment of NIAC draws a similar conclusion, "the healthiest partnerships exist in sectors where longstanding relationships between industry and government built trust over time".[61]

Financial resources are crucial to sustain these partnerships. The financial sector considers the issue a high enough priority to invest its own resources to create a sustainable institution. Its ISAC is fee-based. Others' funding models vary. Some entities are fully funded by the government, such as the National Coordinating Center of the National Communications System. According to Condello, "The NCC is the only capability that is public-private, and fully funded by the government. The private sector contributes the time of its staff members." Others, such as the FS-ISAC, are fully funded by the private sector through a fee-based system. Both were often mentioned as successful examples. The appropriate funding model therefore depends on the sector. As Devlin point out, "No matter what industry we talk about, if major firms see a significant common interest, then they are willing to dedicate the resources. It is a question of prioritization," a view also expressed by Wilshusen. The government needs to decide on a case by case basis in which sector there might exist a negative externality that could affect national security. In the absence of such externalities, one sector needs to fund them. As the 2012 NIAC study highlights, “Sector security specialists note a shift in the targets of sophisticated cyber attacks, which often now focus on smaller companies that cannot afford the same level of protection or access to intelligence sources that larger companies can. Because the sector is highly interconnected, criminals can often get the information or access they want by targeting smaller companies and in turn accessing the electronic networks that tie them to larger institutions.”[62]

At the cross-sectoral level, the PCIS plays an important role to prevent duplicative efforts and an indirect inter-agency coordinating role for the government. Several private sector representatives pointed out how there are currently several supply-chain efforts underway by different government agencies submitting requests to private sector corporations without coordinating them with other agencies. A similar criticism was noted in a NIAC 2006 report reporting frustrations of “repeated solicitations for identical information from multiple government agencies”.[63] And while the private sector PCIS helps the government indirectly to coordinate itself for playing the role of *deus ex machina*, the government can play the same role to bring the private sector together. But Bob Dix, chair of the PCIS, also points out that “The public and the private sector need to improve aligning timing, resources, and priorities between both sectors. There is a gap between priority and mission alignment and we need to replace this flawed process with a common planning process.”

Andrew Kennedy at BITS/Financial Services Roundtable reflects on the relationship between private and public sectors pointing out “we have been making slow but steady progress collaborating with ISP and telecommunication sectors on a wide range of issues. When the Department of Commerce convened a multi-industry meeting on botnet mitigation we were able to accelerate work on this important issue. The government can play an important role in focusing our attention on difficult cross-sectoral challenges, even when solutions must largely be driven by the private sector.”

The Y2K experience and the global nature of financial institutions highlight the important link between national and international efforts. Calls for stronger international engagement are also expressed by groups such as the Internet Security Alliance, Tech America, and the Business Software Alliance.[64] And GAO already made this point in 2009 recommending to “focus greater attention on addressing the global aspects of cyberspace.”[65] There is a range of international organizations that are relevant for critical infrastructure protection such as the International Organization for Standardization, the International Society of Automation, or the International Telecommunications Union.[66] While the Cyber Storm II exercise included participants from the ‘Five Eyes’ countries, Australia, Canada, New Zealand, and the United Kingdom, the group was expanded for Cyber Storm III including 12 countries.[67] An unresolved challenge is how to share information with the private sector when companies are multinational and their employees include executives who are non-US citizens as highlighted by the NIAC.[68]

Generally, the system today exhibits a lack of nimbleness. It is driven by the initial institutional design rather than need. At the same time, there are outstanding fundamental issues that the protection of critical infrastructure and its ownership and operation by private sector entities raise. For example, even when the government issues clearances and hosts classified briefings for private sector representatives, their value is limited because participants cannot share the information they learned with others in their institutions and can therefore only be a starting point.

4. Incentives and creating value

For a collaboration to last as a process beyond the project there must be a return on the investment of the participants' time and resources. Tishuk says "there must be reason for its existence for it to stand the test of time." Others call it "incentives" or "value." This return on investment does not need to occur every time, but must happen at least occasionally in order to earn a pay-off. Self-interest was the most frequent answer by experts when asked why financial institutions were so engaged in the collaboration with government. Condello is broader in her analysis, "What makes sectors successful? Sectors that live by flow. Financial data flows. Oil flows. Electricity flows. These sectors are concerned if the flow of their products is interrupted and are highly incented to ensure the reliability and integrity of that flow, and are process-driven to achieve that." Others have called these sectors the "millisecond sectors."[69]

One of the experts interviewed for this study explains that companies are primarily motivated to strengthen security in order to mitigate reputational risk rather than avoiding government fines. Guy Copeland, Senior Principal at CSC and co-chair of the joint, government and private sectors, Cross Sector Cyber Security Working Group of the PCIS, points out that companies generally are driven by their fiduciary responsibility vis-à-vis their shareholders and investors. He adds that as part of meeting those responsibilities, they must build and maintain a positive brand reputation because they realize that inadequate security may lead to brand damage and loss of clients and suppliers who fear their shared information and access may not be adequately protected. And McKay suggests that the partnership should focus on specific projects in order to achieve concrete results addressing one of the key challenges between the project and process-focused partnerships.

But even if there is interest to participate, value does not appear out of thin air. Creating value is often a policy and not a technical challenge; information sharing is an obvious example. Keil's initiative also shows that this challenge requires research, analysis, and a strategy. At the same time, the link between self-interest and positive externalities is crucial. The Intelligence and National Security Alliance points out that partners must have "a sufficiently high stake in and motivation or incentive to improve the security of the internet" and "able to demonstrate that in advancing their interest they are also advancing the wider public interest."[70] The example of the financial sector which has created a pull effect for other sectors to benefit or emulate its services is one example of this mechanism.

In spite of these examples showing that much can be done to create incentives and values, there are also fundamental differences of preferences among sectors that exist independently of managerial issues. "The interests of private business and of the state are often not convergent when it comes to CIP and that PPP are therefore hardly suitable as solutions."[71] Some sectors can be nudged while the convergence of interests in others might require additional subsidies or regulation to shift the preference curve. Again, this depends on the individual sector and there might be different perceptions of the incentive structures and values between sectors and even within a sector.

As Carlson points out, "After leaders in the financial services sector raised concerns about software security, Microsoft and other major software companies responded and started building better relationships and fostering greater collaboration in order to tackle the problem. Microsoft viewed it as important to its franchise in serving large corporate customers. Leaders in the financial services industry viewed it as critical to protecting sensitive customer information, managing information technology risks, and containing costs associated with alerting customers and patching or upgrading systems. To Microsoft's credit, it initiated a major company-wide project to enhance software assurance through it Trustworthy Computing Initiative. Similar challenges concerning software assurance exist today given the rapid adoption of smart phones and tablets and the integration of these mobile technologies. Now is the time to collaborate among mobile device manufacturers, wireless providers and others that are experimenting in this space in order to protect consumers and enterprises."

And Dix makes the important point, "We need to focus on the economic aspect more. The market is delivering technical solutions at an unprecedented rate but there is a gap in adoption across all stakeholder groups ranging from small and medium-sized companies, to home users, academic institutions, and government agencies. We need to look more into that."

5. Timing - urgency and maturity

Path dependence has already been highlighted as an obstacle to an efficient institutional design. That is why exogenous events must be carefully monitored as they can open opportunities to overcome established patterns and change perceptions among stakeholders. Triggering moments can be used to create urgency and to drive change. Major events, such as the September 11th attack, had such an effect. The result was major changes and a lasting impact on the system. "There was a big boost after 9/11," Carlson recalls and "after 9/11 there was a real transition with more efforts to coordinate and collaborate." However, smaller events unknown to outsiders can also have a lasting impact on individual leaders. GAO's Michael Gilmore, assistant director for information security issues, recalled an incident where "a CEO received a letter from an unknown woman who sent him internal financial reports from his company that she had found used as stuffing for a purse bought from a street vendor. After some investigating, the CEO found out that the shredding company hired to shred the company's paper simply had not shred it. This security incident created greater emphasis on security at the company and changed the atmosphere in the company so that security was now considered as an enabler for the business in general." While such exogenous events cannot be controlled, their occurrence creates a window of opportunity for the collaboration between government and the private sector which can be seized by the participants if they recognize the opportunity and use it to enhance the partnership.

It is also important to conceptualize maturity and an evolutionary model of partnership as a dynamic rather than linear process. A partnership will not become more effective automatically over time. There is a selection bias to focus on successes where this is the case while failures, e.g. ISAC's that have been discontinued, are underreported. Maturity and models such as the capability maturity model used in the 2012 NIAC study[72] are therefore a dynamic process and a partnership can be more mature now but less mature tomorrow. This can be the result of a period of weak leadership, a lack of resources, etc. It is therefore important to prepare and plan for such periods of weak leadership, to take action to change it, or to have the ability to bridge such periods. The more mature a partnership, the less likely it is that such periods will have a lasting or deeply negative impact.

Building a lasting collaboration and trust requires time to produce results, often longer than one individual remains in a professional position. This can stand at odds with the professional goals of individuals in government and corporations, who must not only worry about producing results, but also advancing in his or her career. This logic reinforces the argument against political appointees in government who rotate frequently. It also requires incentives in the private sector to allow a person to work on these issues for a long term. As Condello points out "It takes four to six years for a project idea to wind its way from a company through the SCC through the government budgetary process until it becomes an operational program. This is a long process for the private sector, which generally operates on a quarter-by-quarter basis. Compounded by gaps in continuity from high government turnover, these projects might be scrapped half-way through the process. This does not mean the government process is inappropriately slow, it just means that it takes time and continuity to implement ideas." A good example of this is the creation of the NCCIC. Recommendations to establish such an operational capability date back to at least 2003 if not even back to PDD-63 and the idea of a singular ISAC.[73]

On both sides, personal turnover poses a challenge. According to the NIAC, "people don't stay in one position, and when they leave, their clearance goes with them, leaving a gap in cleared personnel within a department or company."[74] Copeland notes that key position turnovers in DHS and elsewhere in the executive branch and private sector, combined with the inevitable stresses and turmoil of a major reorganization and startup of a new department under intense, competing pressures, has, despite the best intentions and efforts of DHS leadership, led to proliferation of new initiatives, sometimes without appreciation or awareness for initiatives launched previously. This is why NIAC recommends that "because of the personnel turnover throughout the public and private sectors, the Federal Government must institutionalize mechanisms that foster trust, thereby minimizing the dependence on personal relationships," a call reiterated by GAO,[75] and one which must be complemented by similar efforts in the private sector.[76]

Conclusion

PDD-63 envisioned that after five years in effect, the nation's critical infrastructures would be secure. However, nearly a decade later the goal has not yet been achieved. Some sectors such as the oil and gas sector do not even have an ISAC, though their vulnerabilities have been exploited and calls for a common operational center did not materialize in form of the NCCIC until 2009. Some sectors are ahead of the curve but much work remains to be done.

The Y2K experience demonstrated that the public and private sectors are capable of working together to solve a problem that is not only national but global in scale. Together, they provided enormous resources to implement changes in systems throughout the nation and also abroad. Congress passed legislation that enabled private companies to focus on fixing the bug rather than worrying about potential legal ramifications. Dedicated officials in government and corporate IT departments implemented the immense project and resorted to senior leadership support in crucial moments to collaborate nationally and internationally.

The financial sector showed how the lessons learned and best practices of the Y2K project could be mainstreamed into a long-term collaboration. They became institutionalized and replicated in the FSSCC while the FS-ISAC continued to build a reputation for which it is admired throughout the sectors today. Leadership was particularly crucial for the transition from one early leadership generation to the next. Resources were available to create an operational capacity capable of producing value for its participants. The institutional design focused on including technical experts, a scalable membership, and importantly, a sustainable funding model.

The United Kingdom took note of the United States' success and decided to emulate them. Building on the lessons learned, the UK information exchanges soon became a model for other countries in Europe that faced the challenge of building trust between sectors. The process in the UK highlights the importance of getting the basics right. It emphasis the significance of simple rules of the road, such as keeping membership small to build trust through social ties, regular face-to-face meetings, and clear principles for attendance, while also ensuring enough representatives from the different sectors.

The private sector owners and operators of critical infrastructure are the first and last line of defense. Self-interest does drive protection efforts, but there remains the danger of a negative security externality, especially if an actor is not capable or willing to invest the resources required to reach the level of protection necessary for national security purposes. The government can play an important role by leading from behind the scenes and coordinating activities in its role as a convener, facilitating efforts by providing seed money, and providing legitimacy and the legal authorizing environment.

Issues such as legal concerns over Cooperative Research and Development Agreements, the effect of stricter lobbying rules on CIPAC meetings, or the clearance process continue to be subjects of criticism.[77] Yet, those are operational issues that can be solved if there is political will. As Cheri McGuire at Symantec points out, "Let's focus on solving problems and creating something meaningful".

End notes

[1] National Council of ISACs, "Information Sharing and Analysis Centers (ISAC)." Last modified September 2012. http://www.isaccouncil.org/index.php?option=com_content&view=article&id=87&Itemid=194.

[2] Microsoft, "Protecting our Critical Infrastructure ." Last modified December 13, 1999. http://www.microsoft.com/issues/essays/1999/12-13preserve.mspx;

[2] Personick, Steward, and Cynthia A. Patterson , Critical Information Infrastructure Protection and the Law: An Overview of Key Issues (Committee on Critical Information Infrastructure Protection and the Law, National Research Council, 2003): p. 11

[3] Verton, Dan and Matt Hamblen, "Cyberattack Report: Some Progress Made," Computerworld, Vol. 34, issue 49 (December 4, 2000): 1.

Microsoft, "Protecting our Critical Infrastructure ." Last modified December 13, 1999. http://www.microsoft.com/issues/essays/1999/12-13preserve.mspx.

[4] Personick, Steward, and Cynthia A. Patterson , Critical Information Infrastructure Protection and the Law: An Overview of Key Issues (Committee on Critical Information Infrastructure Protection and the Law, National Research Council, 2003): p. 23-23

[5] U.S. Department of Homeland Security, "Critical Infrastructure Partnership Advisory Council." Last modified March 24, 2006. http://www.fas.org/sgp/news/2006/03/dhsci032406.html.

[6] U.S. Government Accountability Office, "Critical Infrastructure Protection: Cybersecurity Guidance is Available, but More Can Be Done to Promote Its Use." (Washington, DC: Government Accountability Office, December 2011), p. 6. Last modified 2011. http://www.gao.gov/assets/590/587529.pdf.

[7] Prieto III, Daniel. "Information Sharing with the Private Sector – History, Challenges, Innovation, and Prospects," in *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, edited by Philip Auerswald, Lewis Branscomb, Erwann Michel-Kerjan, and Todd La Porte (Cambridge, U.K.: Cambridge University Press, 2006), p. 411-412.

[8] Moteff, Jack, *Critical Infrastructures: Background, Policy, and Implementation*, (Washington, DC: Congressional Research Service, July 2011), p. 12.

[9] U.S. Department of Homeland Security, "National Infrastructure Protection Plan 2006", p. 94. Last modified 2006. http://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf

[10] U.S. Government Accountability Office, "Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience." (Washington, DC: Government Accountability Office, March 2010). Last modified 2010. http://www.gao.gov/assets/310/301494.pdf.

[11] Moteff, Jack, *Critical Infrastructures: Background, Policy, and Implementation*, (Washington, DC: Congressional Research Service, July 2011), p. 23.

[12] U.S. Department of Homeland Security, "DHS Highlights Two Cybersecurity Initiatives to Enhance Coordination with State and Local Governments and Private Sector Partners." Last modified November 18, 2010. http://www.dhs.gov/news/2010/11/18/dhs-highlights-two-cybersecurity-initiatives-enhance-coordination-state-and-local.

Anderson, Denise. National Institute of Standards and Technology, "Kick-Starting NCCIC Information Sharing." Last modified 2012. http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-02/feb2_ispa-nccic-information-sharing_danderson.pdf.

[13] Moteff, Jack, *Critical Infrastructures: Background, Policy, and Implementation*, (Washington, DC: Congressional Research Service, July 2011), p. 5.

[14] Moteff, Jack, *Critical Infrastructures: Background, Policy, and Implementation*, (Washington, DC: Congressional Research Service, July 2011), p. 10.

[15] The White House, "Executive Order 13286", (February 28,2003). http://www.fas.org/irp/offdocs/eo/eo-13286.htm.

[16] National Archives, "Executive Order 12382--President's National Security Telecommunications Advisory Committee." http://www.archives.gov/federal-register/codification/executive-order/12382.html

[17] The White House, "Office of Science and Technology Policy About PCAST." http://www.whitehouse.gov/administration/eop/ostp/pcast/about.

[18] The White House, "President's Intelligence Advisory Board and Intelligence Oversight Board About the PIAB." http://www.whitehouse.gov/administration/eop/piab/about

[19] Dumenco, Simon. New York Magazine, "Saved by the Cabal! Paging the president's shadowy Plunge Protection Team." Last modified January 27, 2008. http://nymag.com/news/intelligencer/43342/.

[20] Smocer, Paul. BITS, "Statement of BITS President Paul Smocer on Behalf of the Financial Services Roundtable." Last modified June 1, 2012. http://www.bits.org/publications/regulation/BITSTestimonyHouseFS060112.pdf.

[21] Moynihan, Senator Daniel Patrick. John Lindquist, "Senator Daniel Patrick Moynihan's Letter to the President Concerning the Year 2000 Problem." Last modified January 6, 2001. http://www.jlindquist.com/dpmy2k.html.

[22] Mitchell, Dr. Robert L. Computer World, "Y2K: The good, the bad and the crazy." Last modified December 28, 2009. http://www.computerworld.com/s/article/9142555/Y2K_The_good_the_bad_and_the_crazy?taxonomyId=14&pageNumber=2.

[23] National Y2K Information Coordination Center, *Best Practices and Lessons Learned,* June 19, 2000. Last modified 2000. http://web.archive.org/web/20040821065933/http://www.y2k.gov/docs/ICClesslearn.html

[24] Alfred, Randy. Wired, "Sept. 9, 1999: 9/9/99 No Big Deal for Computers." Last modified September 9, 2011. http://www.wired.com/thisdayintech/tag/y2k/.

[25] Moore, Mark, Creating Public Value: Strategic Management in Government (Cambridge, MA: Harvard University Press, 1997).

[26] Web Archive Y2K.gov, "National Y2K Information Coordination Center." Last modified June 19, 2000. http://web.archive.org/web/20040821065933/http://www.y2k.gov/docs/ICClesslearn.html

[27] National Y2K Information Coordination Center, *Best Practices and Lessons Learned,* June 19, 2000. Last modified 2000. http://web.archive.org/web/20040821065933/http://www.y2k.gov/docs/ICClesslearn.html

Federal Deposit Insurance Corporation, "Lessons Learned from the Year 2000 Project." Last modified April 10, 2000. http://www.fdic.gov/news/news/inactivefinancial/2000/fil0026a.html

[28] Govtracks.us, "S. 2392 (105th): Year 2000 Information and Readiness Disclosure Act." http://www.govtrack.us/congress/bills/105/s2392.

[29] U.S. Government Printing Office, "Year 2000 Information and Readiness Disclosure Act." Last modified October 19, 1998. http://www.gpo.gov/fdsys/pkg/PLAW-105publ271/pdf/PLAW-105publ271.pdf .

National Communications System, "The President's National Security Telecommunications Advisory Committee Cyber security Collaboration Report." Last modified May 21, 2009. http://www.ncs.gov/nstac/reports/2009/NSTAC CCTF Report.pdf.

[30] National Y2K Information Coordination Center, *Best Practices and Lessons Learned,* June 19, 2000. Last modified 2000. http://web.archive.org/web/20040821065933/http://www.y2k.gov/docs/ICClesslearn.html

[31] U.S. Government, "Public Law 105-271- OCT. 19, 1998." Last modified 1998. http://www.gpo.gov/fdsys/pkg/PLAW-105publ271/pdf/PLAW-105publ271.pdf.

[32] Berkeley III, Alfred R., Wesley Bush, Philip G. Heasley, James B. Nicholson, James A. Reid, and Michael J. Wallace. National Infrastructure Advisory Council, "Intelligence Information Sharing: Final Report and Recommendations." Last modified 2012. http://www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf

[33] Financial Services-Information Sharing and Analysis Center, "Operating Rules." Last modified 2011. http://www.fsisac.com/files/FS-ISAC_OperatingRules_2012.pdf.

[34] National Infrastructure Advisory Council, "Intelligence Information Sharing Final Report and Recommendations.", p. B-12. Last modified January 10, 2012. http://www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf.

[35] National Communications System, “Guide to Understanding the National Coordinating Center for Telecommunications and the Network Security Information Exchanges.” Last Modified 2001.

[36] Smocer, Paul. The United States House of Representatives Committee on Financial Services, "Cyber Threats to Capital Markets and Corporate Accounts." Last modified 2012. http://www.bits.org/publications/regulation/BITSTestimonyHouseFS060112.pdf.

[37] Libutti, Frank. U.S. Department of Homeland Security, "Oil and Natural Gas Sector Homeland Security Coordination Council." Last modified 2004. http://www.npga.org/files/public/Oil_NG_Sector_Homeland_Security_Letter_6-04.pdf.

ISAC Council, "Reach of the Major ISACs." Last modified 2004. http://www.isaccouncil.org/index.php?option=com_docman&task=doc_view&gid=14&Itemid=208

[38] Energy ISAC, “Due to the loss of funding” (March 8, 2005). Last modified 2005. http://web.archive.org/web/20050308150458/http://www.energyisac.com/

[39] Clayton, Mark. The Christian Science Monitor, "Exclusive: potential China link to cyberattacks on gas pipeline companies." Last modified 2012. http://www.csmonitor.com/USA/2012/0510/Exclusive-potential-China-link-to-cyberattacks-on-gas-pipeline-companies.

[40] European Commission/Booz & Company, *Study: Stock-Taking of Existing Critical Infrastructure Protection Activities* (2007), p. 14. Last modified 2007. http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/2009_CIP%20stock_taking.pdf

[41] European Commission/Booz & Company, *Study: Stock-Taking of Existing Critical Infrastructure Protection Activities* (2007), p. 297. Last modified 2007. http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/2009_CIP%20stock_taking.pdf

[42] Centre for the Protection of National Infrastructure, "CPNI- the policy context." http://www.cpni.gov.uk/about/context/.

[43] European Commission/Booz & Company, *Study: Stock-Taking of Existing Critical Infrastructure Protection Activities* (2007), p. 427. Last modified 2007. http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/2009_CIP%20stock_taking.pdf

[44] European Commission/Booz & Company, *Study: Stock-Taking of Existing Critical Infrastructure Protection Activities* (2007), p. 19. Last modified 2007. http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/2009_CIP%20stock_taking.pdf

[45] National Infrastructure Advisory Council, Critical Infrastructure Resilience – Final Report and Recommendations (September 8, 2009), p. 23. Last modified 2009. http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf

[46] Centre for the Protection of National Infrastructure, "CPNI- the policy context." http://www.cpni.gov.uk/about/context/.

[47] European Network and Information Security Agency, Incentives and Challenges for Information Sharing in the Context of Network and Information Security (2010), p. 11. Last modified 2010.

[48] European Commission/Booz & Company, *Study: Stock-Taking of Existing Critical Infrastructure Protection Activities* (2007), p. 19-20, 442. Last modified 2007. http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/2009_CIP%20stock_taking.pdf

[49] National Security Telecommunications Advisory Committee, "Network Security Information Exchanges." http://www.ncs.gov/nstac/reports/fact_sheet/NSTAC_08.pdf.

[50] National Communications System (March 2001) "Guide to Understanding the National Coordinating Center for Telecommunications and the Network Security Information Exchanges", p. 17.

[51] Mazzafro, Joseph. Intelligence and National Security Alliance, "Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models." Last modified 2009. http://www.insaonline.org/assets/files/CyberPaperNov09R3.pdf.

[52] United Kingdom Houses of Parliament, Parliamentary Office of Science & Technology, *Postnote - Cyber Security in the UK*, no. 389 (September 2011). Last modified 2011. www.parliament.uk/briefing-papers/POST-PN-389.pdf

[53] Cornish, Paul, David Livingstone, et al. *Cyber Security and the UK's Critical National Infrastructure - A Chatham House Report*, (London: Chatham House, September 2011), p. 11. Last modified 2011. http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r0911cyber.pdf

[54] Institution of Civil Engineers, The State of the Nation – Defending Critical Infrastructure (London: Institution of Civil Engineers, June 2009), p. 12. Last modified 2009.http://www.ice.org.uk/getattachment/5e93aedd-3b4c-44db-acfa-d176e0ccbb0e/State-of-the-Nation--Defending-Critical-Infrastruc.aspx

[55] Smocer, Paul. The United States House of Representatives Committee on Financial Services, "Cyber Threats to Capital Markets and Corporate Accounts." Last modified 2012. http://www.bits.org/publications/regulation/BITSTestimonyHouseFS060112.pdf

[56] Berkeley III, Alfred R., Gilbert G. Gallegos, and Margaret E. Grayson. National Infrastructure Advisory Council, "Critical Infrastructure Partnership Strategic Assessment: Final Report and Recommendations." Last modified 2008. http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_protection_assessment_final_report.pdf

Berkeley III, Alfred R., Wesley Bush, Philip G. Heasley, James B. Nicholson, James A. Reid, and Michael J. Wallace. National Infrastructure Advisory Council, "Intelligence Information Sharing: Final Report and Recommendations." Last modified 2012. http://www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf.

Chambers, John T., and Gilbert G. Gallegos. National Infrastructure Advisory Council, "Public-Private Sector Intelligence Coordination: Final Report and Recommendations by the Council." Last modified 2006. http://www.dhs.gov/xlibrary/assets/niac/niac_icwgreport_july06.pdf.

[57] ISAC Council, "Reach of the Major ISACs." Last modified 2004.

http://www.isaccouncil.org/index.php?option=com_docman&task=doc_view&gid=14&Itemid=208.

[58] U.S. Department of Homeland Security, "Cyber Storm Exercise Report: Department of Homeland Security Office of Cybersecurity and Communications National Cyber Security Division." September 12, 2006. p. 6.

U.S. Department of Homeland Security, "Cyber Storm II Final Report: Department of Homeland Security Office of Cybersecurity and Communications National Cyber Security Division." Last modified 2009. http://www.dhs.gov/xlibrary/assets/csc_ncsd_cyber_stormII_final09.pdf.

U.S. Department of Homeland Security, "Cyber Storm III Final Report: Department of Homeland Security Office of Cybersecurity and Communications National Cyber Security Division." Last modified 2011.

[59] McGuinn, Martin G., and Marilyn Ware. National Infrastructure Advisory Council, "Sector Partnership Model Implementation: Final Report and Recommendations by the Council." Last modified 2005. http://www.dhs.gov/xlibrary/assets/niac/NIAC_SPMWGReport_Feb06.pdf.

[60] Chambers, John T., and Gilbert G. Gallegos. National Infrastructure Advisory Council, "Public-Private Sector Intelligence Coordination: Final Report and Recommendations by the Council." Last modified 2006. http://www.dhs.gov/xlibrary/assets/niac/niac_icwgreport_july06.pdf.

[61] Berkeley III, Alfred R., Gilbert G. Gallegos, and Margaret E. Grayson. National Infrastructure Advisory Council, "Critical Infrastructure Partnership Strategic Assessment: Final Report and Recommendations." Last modified 2008. http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_protection_assessment_final_report.pdf.

[62] Berkeley III, Alfred R., Wesley Bush, Philip G. Heasley, James B. Nicholson, James A. Reid, and Michael J. Wallace. National Infrastructure Advisory Council, "Intelligence Information Sharing: Final Report and Recommendations." Last modified 2012. http://www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf

[63] Chambers, John T., and Gilbert G. Gallegos. National Infrastructure Advisory Council, "Public-Private Sector Intelligence Coordination: Final Report and Recommendations by the Council." Last modified 2006. http://www.dhs.gov/xlibrary/assets/niac/niac_icwgreport_july06.pdf.

[64] National Security Telecommunications Advisory Committee, "Network Security Information Exchanges." http://www.ncs.gov/nstac/reports/fact_sheet/NSTAC_08.pdf.

[65] Powner, David. U.S. Government Accountability Office, "Statement - National Cybersecurity Strategy: Key Improvements are Needed to Strengthen the Nation's Posture." Last modified 2009. http://www.gao.gov/new.items/d09432t.pdf.

[66] U.S. Government Accountability Office, "Critical Infrastructure Protection: Cybersecurity Guidance is Available, but More Can Be Done to Promote Its Use." (Washington, DC: Government Accountability Office, December 2011). Last modified 2011. http://www.gao.gov/assets/590/587529.pdf.

[67] U.S. Department of Homeland Security, "Cyber Storm: Securing Cyber Space." Last modified 2012. http://www.dhs.gov/cyber-storm-securing-cyber-space.

[68] Berkeley III, Alfred R., Wesley Bush, Philip G. Heasley, James B. Nicholson, James A. Reid, and Michael J. Wallace. National Infrastructure Advisory Council, "Intelligence Information Sharing: Final Report and Recommendations." Last modified 2012. http://www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf

[69] Berkeley III, Alfred R., Wesley Bush, Philip G. Heasley, James B. Nicholson, James A. Reid, and Michael J. Wallace. National Infrastructure Advisory Council, "Intelligence Information Sharing: Final Report and Recommendations." Last modified 2012. http://www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf

[70] Mazzafro, Joseph. Intelligence and National Security Alliance, "Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models." Last modified 2009. http://www.insaonline.org/assets/files/CyberPaperNov09R3.pdf.

[71] Dunn-Cavelty, Myriam, and Manuel Suter, “Public-Private Partnerships are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection,” International Journal of Critical Infrastructure Protection, Vol. 4, no. 2 (March 1, 2009): p. 179-187.

[72] Berkeley III, Alfred R., Wesley Bush, Philip G. Heasley, James B. Nicholson, James A. Reid, and Michael J. Wallace. National Infrastructure Advisory Council, "Intelligence Information Sharing: Final Report and Recommendations." Last modified 2012. http://www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf.

[73] 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." Last modified 2009.

http://www.ncs.gov/nstac/reports/2009/NSTAC CCTF Report.pdf

[74] Berkeley III, Alfred R., Wesley Bush, Philip G. Heasley, James B. Nicholson, James A. Reid, and Michael J. Wallace. National Infrastructure Advisory Council, "Intelligence Information Sharing: Final Report and Recommendations." Last modified 2012. http://www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf.

[75] Powner, David. U.S. Government Accountability Office, "Statement - National Cybersecurity Strategy: Key Improvements are Needed to Strengthen the Nation's Posture." Last modified 2009. http://www.gao.gov/new.items/d09432t.pdf.

[76] Chambers, John T., and Gilbert G. Gallegos. National Infrastructure Advisory Council, "Public-Private Sector Intelligence Coordination: Final Report and Recommendations by the Council." Last modified 2006. http://www.dhs.gov/xlibrary/assets/niac/niac_icwgreport_july06.pdf.

[77] Berkeley III, Alfred R., and Mike Wallace. National Infrastructure Advisory Council, "A Framework for Establishing Critical Infrastructure Resilience Goals." Last modified 2010. http://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf.