History Repeats Itself:
The 60-Day Cyberspace Policy Review in Context

Eric A. Greenwald*

INTRODUCTION

On February 9, 2009, President Obama gave his National Security and Homeland Security Advisors 60 days to conduct a Cyberspace Policy Review.[1] The stated purpose of this "60-Day Review" was to provide a comprehensive assessment of U.S. policies for cybersecurity.[2] According to a White House press release, the review would "develop a strategic framework to ensure that U.S. Government cyber security initiatives are appropriately integrated, resourced and coordinated with Congress and the private sector."[3]

The 60-Day Review was an ambitious project and, in the end, took more than 60 days to complete.[4] When the final report was issued on May 29, 2009, it offered a careful assessment of the current situation and a broad vision of what the United States must accomplish to secure our digital future. This vision, however, was not fundamentally different from previous iterations of cybersecurity strategy that the U.S. government has issued over the past 12 years.

The 60-Day Review undoubtedly represents a critical step toward addressing the many challenges the United States faces in working to secure its public and private information systems. However, it is important to place this document in proper context and understand what it accomplishes and what business it leaves unfinished. Before much progress can be made in improving cybersecurity, there are some tough policy decisions that have to be made.

The 60-Day Review does not take on many of those decisions. Rather, it provides an accurate and troubling picture of what the country is up against. It offers a glimpse of the daunting but important tasks of trying to harmonize the cybersecurity programs within government, establishing an effective partnership with the private sector, and developing strong relationships with other nations to combat cyber crime. It recommends

---

* Chief Counsel for the House Permanent Select Committee on Intelligence. The views presented here are those of the author and do not necessarily reflect those of the Committee or any of its members.

1. *President Obama Directs the National Security and Homeland Security Advisors To Conduct Immediate Cyber Security Review*, (Feb. 9, 2009), *available at* http://www.whitehouse.gov/the_press_office/advisorstoconductimmediatecybersecurityreview.

2. *Id.*

3. *Id*.

4. The report was ultimately issued after 110 days.

promoting education, training, and technological innovation while also developing an effective institutional mechanism for responding to cybersecurity incidents.

But we have heard all of this before – more than once.

I. BACKGROUND

In the late 1990s and again in 2003, the U.S. government undertook comparable strategic reviews of the path toward securing cyberspace. Each of these assessments made findings and outlined proposals strikingly similar to the 60-Day Review. Most of the challenges described in the 60-Day Review are, therefore, very familiar to those who work in the cybersecurity field. Recognizing and cataloging these problems is an important step, but it is only a preliminary step and, unfortunately, one we are now taking for the third time.

The Review's conclusions do center around one concrete, foundational recommendation aimed at resolving many of these challenges – that the President should establish a single Cybersecurity Policy Official, or "Coordinator,"[5] operating from the White House, with clear presidential support, to coordinate policy and develop an action plan.[6]

This is an approach that President Obama has been advocating since well before taking office,[7] but it is not without controversy and is not universally embraced.[8] It is only one recommendation, but it may prove to be vital in achieving success on virtually all of the endeavors necessary to realizing the broader policy goals involved in securing U.S. information systems.

In essence, the 60-Day Review was not intended to provide a solution for the litany of cybersecurity problems facing the nation; rather, it was to

---

5. In the media, the Cybersecurity Coordinator is generally referred to as the "Cyber Czar." Although this is nothing more than a shorthand title, the label is a potent one. *See, e.g.*, Mark Leibovich, *The Tin-Star Title for the Too-Tough Job*, N.Y. TIMES, May 20, 2007, §4 (Week in Review), at 1:

> [Y]ou know it has gotten messy, the problem so immense – and the managers so desperate – that the only solution lies with something as fundamentally undemocratic as the appointment of a czar. . . . [C]zar jobs are often hailed as "newly created positions" and imbued with "unprecedented authority" to "cut through the bureaucracy" and "get things done." All of which usually ensures that their authority will be undercut at every turn, that they will be entangled in bureaucracy and get very few "things" done.

6. CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

7. Remarks of Senator Barack Obama, Summit on Confronting New Threats, Purdue University, July 16, 2008, *available at* http://www.cfr.org/publication/16807/barack_obamas_speech_at_the_university_of_purdue.html.

8. *See* CENTER FOR STRATEGIC AND INT'L STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY (2008), *available at* http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

provide the mechanism through which those problems might eventually be solved. It explains how the U.S. Government needs to begin its approach to this problem – with clear leadership from the White House.

This approach places a very heavy burden on the Cybersecurity Coordinator. Addressing the challenges outlined in the 60-Day Review will require reconciling serious turf battles over the distribution of statutory authorities, expertise, resources, and funding.[9] Previous iterations of cybersecurity strategies have failed to resolve these disputes, so the issuance of a strategy establishing a broad vision of what the U.S. government must accomplish, by itself, is insufficient to actually protect cybersecurity.[10]

II. THE HISTORICAL CONTEXT

Computer security has been the subject of congressional and executive branch action for decades, but these efforts took a significant turn on June 21, 1995, when President Clinton issued Presidential Decision Directive 39 (PDD 39)[11] in response to the bombing of the Murrah Federal Building in Oklahoma City two months earlier.[12] PDD 39 outlined national policy on counterterrorism and established infrastructure protection as a national priority.[13]

In that Directive, the President instructed the Attorney General to chair a cabinet-level committee – the Critical Infrastructure Working Group (CIWG) – to assess the vulnerabilities of America's critical infrastructures and make recommendations on how to protect them.[14] The CIWG recommended the creation of two entities: an interim task force to coordinate government responses to attacks on U.S. infrastructure and a

9. In recent years, the principal struggle in the policy debate over which federal agency should play the lead role in cybersecurity has been between the Department of Homeland Security (DHS), which is responsible for protecting critical infrastructure, and the National Security Agency (NSA), which is responsible for protecting classified computers and networks. However, several other agencies, including the Federal Bureau of Investigation, the Central Intelligence Agency, and the Department of Defense (of which NSA is a part), all play active roles in protecting U.S. information systems. Moreover, each federal agency is responsible for developing and implementing a strategy for protecting its own computer systems.

10. KATHI ANN BROWN, CRITICAL PATH: A BRIEF HISTORY OF CRITICAL INFRASTRUCTURE PROTECTION IN THE UNITED STATES 156-158 (2006) *available at* http://cip.gmu.edu/archive/CIP_CriticalPath.pdf.

11. Presidential Decision Directive 39, June 21, 1995. A redacted version of the classified document is available at http://www.fas.org/irp/offdocs/pdd39.htm.

12. BROWN, *supra* note 10, at 72.

13. *Id.*

14. PDD 39, *supra* note 11.

more permanent commission to develop long-term strategy for protecting critical infrastructure.[15]

A. The President's Commission on Critical Infrastructure Protection and Presidential Decision Directive 63 (1996 to 2001)

Based on the CIWG's recommendations, on July 15, 1996, President Clinton issued Executive Order 13,010, establishing the President's Commission on Critical Infrastructure Protection (PCCIP).[16] The PCCIP was charged with developing a national policy and implementation strategies to protect U.S. critical infrastructures from both physical and cyber threats.

On October 13, 1997, the PCCIP issued a report titled *Critical Foundations: Protecting America's Infrastructures*.[17] PCCIP report outlined seven strategic policy objectives and established anticipated three-year outcomes for each.[18] According to the PCCIP report, these objectives were designed to provide a framework for longer term protection of the nation's critical infrastructures.[19]

To implement this broad agenda, the PCCIP recommended establishing a White House Office of National Infrastructure Assurance (ONIA) that would serve as the focal point for infrastructure assurance.[20] The

---

15. Office of the Attorney General, Memorandum on Critical Infrastructure Security (Mar. 14, 1996). *See also* Statement of Michael Vatis, Chief, National Infrastructure Protection Center, Before the Senate Judiciary Subcommittee on Terrorism, Technology and Government Information (June 10, 1998), *available at* http://www.fas.org/irp/congress/1998_hr/98061101_ppo.html.

16. Exec. Order No. 13,010, *Critical Infrastructure Protection*, Fed. Reg. 37,347 (July 15, 1996).

17. ROBERT T. MARSH, CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURES (1997), *available at* http://fas.org/sgp/library/pccip.pdf [hereinafter PCCIP REPORT].

18. *Id*. at 93-99. The PCCIP Report offered the following strategic objectives:

1. Promote a partnership between government and infrastructure owners and operators.
2. Ensure infrastructure owners and operators and state and local governments are sufficiently informed and supported to accomplish their infrastructure protection roles.
3. Establish national structures that will facilitate effective partnership between the federal government, state and local governments, and infrastructure owners.
4. Elevate national awareness of infrastructure threat, vulnerability, and interdependency assurance issues.
5. Initiate a series of information security management activities.
6. Sponsor legislation to increase the effectiveness of federal infrastructure assurance and protection efforts.
7. Increase investment in infrastructure assurance research.

19. *Id*. at 93.

20. *Id*. at 24, 50. The ONIA was never formed, but an NSC body was created pursuant to a subsequent presidential directive.

Commission was unambiguous concerning the importance of this recommendation and provided specific guidance on how the ONIA should be constituted:

> As a matter of urgency, an Office of National Infrastructure Assurance should be established under the National Security Council (NSC) and given overall program responsibility for infrastructure assurance matters, including policy implementation, strategy development, federal interagency coordination, and liaison with state and local governments and the private sector.[21]

Following an intensive interagency review of the PCCIP report, President Clinton issued Presidential Decision Directive 63 (PDD 63) on May 22, 1998.[22] The policy directives contained within PDD 63 represented an effort to implement the conclusions and recommendations of the PCCIP report[23] and to respond to the emerging threats to U.S. critical infrastructure.[24]

---

21. *Id.* at 24.

22. Presidential Decision Directive 63 [hereinafter PDD 63], Critical Infrastructure Protection, May 22, 1998, *available at* http://www.fas.org/irp/offdocs/pdd/pdd-63.htm. *See also* U.S. Department of Justice, Computer Crime and Intellectual Property Section, Critical Infrastructure Protection Fact Sheet, http://www.justice.gov/criminal/cybercrime/critinfr.html.

23. Michael A. Vatis, *Cyber Attacks: Protecting America's Security Against Digital Threats*, *in* COUNTERING TERRORISM: DIMENSIONS OF PREPAREDNESS 239 (Arnold M. Howitt & Robyn L. Pangi eds., 2003).

24. William Jefferson Clinton, Speech Before the U.S. Naval Academy (May 22, 1998), *available at* http://www.cnn.com/ALLPOLITICS/1998/05/22/clinton.academy/transcript.html. President Clinton was explicit in describing the nature of the threat and how PDD 63 would act to counter it:

> [W]e will launch a comprehensive plan to detect, deter and defend against attacks on our critical infrastructures – our power systems, water supplies, police, fire and medical services, air traffic control, financial services, telephone systems and computer networks.
>
> Just 15 years ago, these infrastructures – some within government, some in the private sector – were separate and distinct. Now they are linked together over vast computer electronic networks, greatly increasing our productivity but also making us much more vulnerable to disruption.
>
> . . .
>
> If we fail to take strong action, then terrorists, criminals and hostile regimes could invade and paralyze these vital systems, disrupting commerce, threatening health, weakening our capacity to function in a crisis.
>
> In response to these concerns, I established a commission chaired by retired General Tom [sic] Marsh to assess the vulnerability of our critical infrastructures.
>
> They returned with a pointed conclusion. Our vulnerability, particularly to cyber attacks, is real and growing. And I made important recommendations that we will now implement to put us ahead of the danger curve.

The Directive established several new federal entities – some of which were modified forms of groups that were already in existence.[25] The centerpiece of the new administrative bodies was the National Infrastructure Advisory Council (NIAC).[26] The NIAC was located within the White House and was chaired by a National Coordinator for Security, Infrastructure Protection, and Counterterrorism.[27]

The National Coordinator was appointed by the President and housed in the NSC.[28] As an institutional matter, the creation of the National Coordinator bears a striking resemblance to the recommendation to establish a Cybersecurity Coordinator that was presented in the 60-Day Review. In fact, the two proposals share a number of fundamental elements:

- Establish policy coordinator within the White House:

  PDD 63: "The National Coordinator will be appointed by the President and report to the President through the Assistant to the President for National Security Affairs, who shall assure appropriate coordination with the Assistant to the President for Economic Affairs."[29]

  60-Day Review: "The President should consider appointing a cybersecurity policy official at the White House, reporting to the NSC and dual-hatted with the [National Economic Council], to coordinate the Nation's cybersecurity-related policies and activities."[30]

- Develop a strong public-private relationship to improve coordination and reduce vulnerabilities:

---

25. Among other entities, PDD 63 established the Critical Infrastructure Coordination Group, the National Infrastructure Assurance Council, the National Infrastructure Protection Center, and the Information Sharing and Analysis Centers. *See* U.S. Department of Justice, Computer Crime and Intellectual Property Section, Critical Infrastructure Protection, White Paper – The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, Sections VI, Annex A, *available at* http://www.justice.gov/criminal/cybercrime/white_pr.htm [hereinafter PDD 63 White Paper].

26. *Id.* at Annex A.

27. *Id*. The position of National Coordinator was established pursuant to PDD 62, which was also issued on May 22, 1998. *See* White House Fact Sheet, Combating Terrorism: Presidential Decision Directive 62 (May 22, 1998), *available at* http://www.fas.org/irp/offdocs/pdd-62.htm.

28. *Id*.

29. *Id.* at §VI.

30. CYBERSPACE POLICY REVIEW, *supra* note 6, at 17. When the Cybersecurity Coordinator, Howard Schmidt, was finally appointed on December 22, 2009, the White House directed that he report only to the National Security Council and not to the National Economic Council, as contemplated under the 60-Day Review. *See* Ellen Nakashima & Debbi Wilgoren, *Obama To Name Former Bush, Microsoft Official as Cyber-Czar*, WASH. POST, Dec. 22, 2009, at A04.

PDD 63: "Since the targets of attacks on our critical infrastructure would likely include both facilities in the economy and those in the government, the elimination of our potential vulnerability requires a closely coordinated effort of both the government and the private sector. To succeed, this partnership must be genuine, mutual and cooperative."[31]

60-Day Review: "The public and private sectors' interests are intertwined with a shared responsibility for ensuring a secure, reliable infrastructure upon which businesses and government services depend. Government and industry leaders – both nationally and internationally – need to delineate roles and responsibilities, integrate capabilities, and take ownership of the problem to develop holistic solutions."[32]

- Promote public awareness on the importance of computer security:

PDD 63: "There shall be Vulnerability Awareness and Education Program within both the government and the private sector to sensitize people regarding the importance of security and to train them in security standards, particularly regarding cyber systems."[33]

60-Day Review: "The Federal government, in partnership with educators and industry, should conduct a national cybersecurity public awareness and education. The President's cybersecurity policy official should lead the development and direct the implementation of this public awareness strategy. . . ."[34]

- Develop long-term research and development investment strategies:

PDD 63: "Federally-sponsored research and development in support of infrastructure protection shall be coordinated, be subject to multi-year planning, take into account private sector research, and be adequately funded to minimize our vulnerabilities on a rapid but achievable timetable."[35]

60-Day Review: "Under the leadership of the President's cybersecurity policy official, . . . the Federal government should provide a framework for research and development strategies that

31. PDD 63 White Paper, *supra* note 25, at §IV.
32. CYBERSPACE POLICY REVIEW, *supra* note 6, at 17.
33. PDD 63 White Paper, *supra* note 25, at §VIII.
34. CYBERSPACE POLICY REVIEW, *supra* note 6, at 13.
35. PDD 63 White Paper, *supra* note 25, at §VIII.

> focus on game-changing technologies that will help meet infrastructure objectives. . . ."[36]

- Promote international cooperation on cybersecurity:

> *PDD 63*: "There shall be a plan to expand cooperation on critical infrastructure protection with like-minded and friendly nations, international organizations and multinational corporations."[37]
>
> *60-Day Review*: "The Federal government should work with international partners to develop policies that encourage the development of a global, trusted eco-system that protects privacy rights and civil liberties and governs appropriate use of law enforcement activities to protect citizens and infrastructures."[38]

- Establish a centralized incident response center:

> *PDD 63*: "[The National Infrastructure Protection Center] will be linked electronically to the rest of the Federal Government, including other warning and operations centers, as well as any private sector sharing and analysis centers. Its mission will include providing timely warnings of international threats, comprehensive analyses and law enforcement investigation and response."[39]
>
> 60-Day Review: "The United States needs a comprehensive framework to ensure a coordinated response by the Federal, State, local, and tribal governments, the private sector, and international allies to significant incidents."[40]

In implementing PDD 63, President Clinton selected Richard A. Clarke in 1998 to become the first National Coordinator for Security, Infrastructure Protection, and Counterterrorism. Clarke was authorized to provide advice in the established budget process, but his position carried no actual budget authority.[41] And it is unclear whether his efforts at coordinating cybersecurity policy had the desired effect on unifying the federal government. As Irv Pikus, who served on the PCCIP, notes:

> [The] White House, at least implicitly, had the responsibility for coordinating this whole activity. . . . [But] this was the most discombobulated activity you could imagine. We had every agency going off on its own direction, nobody putting it together. We had

36. CYBERSPACE POLICY REVIEW, *supra* note 6 at 32.
37. PDD 63 White Paper, *supra* note 25, at §VIII.
38. CYBERSPACE POLICY REVIEW, *supra* note 6, at 34.
39. PDD 63 White Paper, *supra* note 25, at Annex A.
40. CYBERSPACE POLICY REVIEW, *supra* note 6, at iv-v.
41. *Id.*; *see* Judith Miller & William J. Broad, *Exercise Finds U.S. Unable To Handle Germ War Threat*, N.Y. TIMES, Apr. 26, 1998, §1, at 1.

> no coordination meetings to speak off. Clarke only wanted to meet with people at the assistant secretary level or above, but those guys were not interested in this stuff. . . . He didn't want to meet with us and so we were off on our own and when it came time to go to Congress to get budgets, the White House was nowhere to be seen. . . .[42]

Perhaps the single most important contribution of the PCCIP and PDD 63 was to establish critical infrastructure protection as a national security issue.[43] Even though the efforts to create a single coordinating authority may have fallen short, the concept and goal of centralizing the policy process across government has persisted and gained momentum as a result of President Obama's approach to this issue.

On the operational side, PDD 63 established the National Infrastructure Protection Center (NIPC).[44] NIPC was housed in the Federal Bureau of Investigation but was comprised of elements from various federal agencies, including the Central Intelligence Agency, the National Security Agency, and the Departments of Energy and Defense.[45] The organization was responsible for handling information related to cybersecurity threats, vulnerabilities, and attacks. PDD 63 established the NIPC as the focal point for collecting and disseminating information and coordinating responses to computer-related incidents.[46]

Separately, PDD 63 established the Critical Infrastructure Assurance Office (CIAO) in the Department of Commerce to coordinate the development of a public-private partnership to assess and address vulnerabilities of critical infrastructures in various sectors of government and the economy.[47]

After only a handful of years, however, the fate of NIPC and CIAO would become emblematic of the overall shift in the locus of authority for cybersecurity in the U.S. government, when, following September 11, the Secretary of Homeland Security became the nation's cyber coordinator.

---

42. BROWN, *supra* note 10, at 156.

43. *Id.* at 166-167.

44. PDD 63 White Paper, *supra* note 25. NIPC was originally created on February 26, 1998, at the direction of Attorney General Janet Reno and FBI Director Louis Freeh. PDD 63 formally recognized the Center's role three months later. For a more detailed description of NIPC's history, *see* Vatis, *supra* note 15.

45. Vatis, *supra* note 15.

46. PDD 63 White Paper, *supra* note 25.

47. *See* PDD 63 White Paper, *supra* note 25; *see also* U.S. Department of Commerce, Bureau of Industry and Security, Bureau of Export Administration Fiscal Year 1999 Annual Report, chap. 10, http://www.bis.doc.gov/news/publications/99annreport/ann99chap10.html. Under PDD 63, the proposed name for this entity was the National Plan Coordination (NPC).

B. The National Strategy To Secure Cyberspace and Homeland Security Presidential Directive 7 (2002 to 2007)

The terrorist attacks of September 11, 2001, fundamentally altered the U.S. government's approach to critical infrastructure protection. But while the profile of the entities responsible for U.S. cybersecurity changed dramatically, the basic policies remained more or less intact.

In direct response to the September 11 attacks, Congress established the Department of Homeland Security (DHS) on November 25, 2002, pursuant to the Homeland Security Act (HSA).[48] One of the central principles behind the creation of DHS was the establishment of a single focal point for protecting the homeland, including critical infrastructures.[49] Accordingly, the responsibility for coordinating national policy on infrastructure protection shifted from the National Coordinator to the Secretary of Homeland Security.[50] Under the HSA, both NIPC and CIAO were transferred to DHS.[51]

Shortly thereafter, in February 2003, the White House issued a National Strategy to Secure Cyberspace.[52] The stated purpose of this policy document was to "engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact."[53] In the end, however, it largely reiterated much of what was conveyed in the PCCIP Report and re-issued many of the same policy recommendations.[54]

Just ten months later, in December 2003, the White House issued Homeland Security Presidential Directive 7 (HSPD-7) to direct the

---

48. Homeland Security Act, Pub. L. No. 107-296, 116 Stat. 2135 (2002).

49. *See* Department of Homeland Security, Brief Documentary History of the Department of Homeland Security, 2001-2008 (2008), *available at* http://www.dhs.gov/xlibrary/assets/brief_documentary_history_of_dhs_2001_2008.pdf.

50. National Strategy for Homeland Security, 31 (July 16, 2002), *available at* http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf.

51. 6 U.S.C.A. §121 (West 2007 & Supp. 2010).

52. NATIONAL STRATEGY TO SECURE CYBERSPACE (2003), *available at* http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf.

53. *Id.* at vii.

54. *Id.* at ix-x. For example, the *National Strategy To Secure Cyberspace* outlined the key responsibilities of the Secretary of Homeland Security, echoing the functions of the National Coordinator under PDD 63:

1. Developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States.
2. Providing crisis management in response to attacks on critical information systems.
3. Providing technical assistance to the private sector and other government entities with respect to emergency recovery plans for failures of critical information systems.
4. Coordinating with other agencies of the federal government.
5. Performing and funding research and development along with other agencies that will lead to new scientific understanding and technologies in support of homeland security.

implementation of the recommendations contained within the National Strategy to Secure Cyberspace.[55] HSPD-7 superseded PDD 63[56] and established the Secretary of Homeland Security as the lead coordinator for protecting U.S. critical infrastructure, including information systems and telecommunications networks.[57] Although the new directive shifted this authority away from the White House, the responsibilities of the Secretary as a coordinator of cybersecurity policy remained consistent with those of the National Coordinator under PDD 63.

In particular, HSPD-7 established that:

> The Secretary shall be responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States. The Secretary shall serve as the principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources.[58]

HSPD-7 also preserved many of the critical implementation elements of PDD 63:[59]

- Public-private partnership:

> "In accordance with applicable laws or regulations, the Department and the Sector-Specific Agencies will collaborate with appropriate private sector entities and continue to encourage the development of information sharing and analysis mechanisms."[60]

- Research and development strategy:

> "In coordination with the Director of the Office of Science and Technology Policy, the Secretary [of Homeland Security] shall prepare on an annual basis a Federal Research and Development

---

55. Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection* (Dec. 17, 2003), *available at* http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1 [hereinafter HSPD-7].

56. CYBERSPACE POLICY REVIEW, *supra* note 6, at C-11.

57. HSPD-7, *supra* note 55, at §15.

58. HSPD-7, *supra* note 55, at §12.

59. Strangely, HSPD-7 does not include any specific prescriptive measures for raising public awareness of the cybersecurity threat; *contrast* National Strategy to Secure Cyberspace, *supra* note 52, at 37-42, drafted only 10 months earlier, which includes a "National Cyberspace Security Awareness and Training Program" as one of its five National Cyberspace Security Priorities and outlines a detailed plan for implementing this program among large and small businesses, educational institutions, and state and local governments. *See also id.* at 37-42, x-xii, 2-4, 32-33, 55, 57-58.

60. HSPD-7, *supra* note 55, at §25. *See also id.* at §§12, 16, 19(a), 27(c).

Plan in support of this directive."[61]

- International cooperation:

"[The Secretary shall produce] a strategy to identify, prioritize, and coordinate the protection of critical infrastructure and key resources, including how the Department intends to work with Federal departments and agencies, State and local governments, the private sector, and foreign countries and international organizations."[62]

- Cybersecurity incident response center:

"The Director of [the Office of Management and Budget] will ensure the operation of a central Federal information security incident center consistent with the requirements of the Federal Information Security Management Act of 2002."[63]

The directives under HSPD-7 still remain in effect today, but the recent focus on cybersecurity at the federal level suggests that the locus of authority for cybersecurity policy may, once again, shift back to the White House.[64] There is logic to the notion of having the White House coordinate cybersecurity policy, as the various agencies continue to wage turf battles for control.[65] Although there are advocates who argue that DHS was created precisely for the purpose of building a structure that would merge critical infrastructure protection under one agency,[66] the Department has not

61. HSPD-7, *supra* note 55, at §30. *See also id.* at §22(e).

62. HSPD-7, *supra* note 55, at §27(a). *See also* §§16, 22(a).

63. HSPD-7, *supra* note 55, at §22(f). The Federal Information Security Management Act requires the Director of OMB to ensure that a "central Federal information security incident center" (1) provide timely technical assistance regarding information security incidents, (2) compile and analyze information about information security, (3) inform agencies about information security threats, and (4) consult with other agencies about information security incidents. 44 U.S.C. §3546 (2006).

64. In addition to the 60-Day Review's recommendation that cybersecurity policy be coordinated out of the National Security Council, legislation pending at the time of this writing would require by statute that cybersecurity policy be coordinated at the White House. *See* S. 778, 111th Cong. (2009). By contrast, at the time of this writing, Senator Susan Collins of Maine was preparing to sponsor a bill that would give the Department of Homeland Security, rather than the White House, primary responsibility for protecting public and private information systems. *See* Chris Strohm, *Collins Says DHS Should Lead Cyber Security, not White House*, CONGRESS DAILY, Sept. 25, 2009, *available at* http://www.nextgov.com/nextgov/ng_20090925_9014.php?oref=rss.

65. James Risen & Eric Lichtblau, *Control of Cybersecurity Becomes Divisive Issue*, N.Y. TIMES, Apr. 16, 2009, at A18; s*ee* Siobhan Gorman, *Cybersecurity Review Sets Turf Battle*, WALL ST. J., May 1, 2009, *available at* http://online.wsj.com/article/SB124113159891774733.html.

66. *See* opening statement of Sen. Susan Collins in *Cybersecurity: Developing a National Strategy, Hearing of the Senate Comm. on Homeland Security and Governmental Affairs*; *see also* Andy Greenberg, *Top Cyber Official Sounds Off*, FORBES, Mar. 9, 2009,

made a great deal of headway in unifying or harmonizing cybersecurity policy since its creation in 2002. Though, ultimately, the previous attempt to center authority for formulating cybersecurity policy in the White House was also less than a complete success.[67]

C. The Comprehensive National Cybersecurity Initiative and the 60-Day Review (2008 to Present)

On January 2, 2008, President Bush established the Comprehensive National Cybersecurity Initiative (CNCI).[68] The creation of the initiative did not come with any fanfare or public statement. Several weeks later, White House spokesman Scott Stanzel explained that the new directive "represents a continuation of our efforts to secure government networks, protect against constant intrusion attempts, address vulnerabilities and anticipate future threats."[69]

The details of the CNCI remain classified, but the U.S. government has released the basic outlines of the Initiative, which it has broken down into a dozen discrete initiatives and divided them into three focus areas:[70]

- Focus Area I: Establishing Front Lines of Defense
  1. *Deploy Trusted Internet Connections*: Reduce the number of Internet access points to federal agencies from 4,300 to fewer than 100.
  2. *Deploy Passive Sensors Across Federal Systems*: Use Einstein 1 and 2 intrusion detection systems are designed to scan Internet packets for known signatures of malicious code.
  3. *Deploy Intrusion Prevention Systems in Federal Systems*: Use Einstein 3 system to assess patterns of malicious code in Internet traffic and block packets that are deemed harmful.

---

available at http://www.forbes.com/2009/03/09/rod-beckstrom-security-technology-security-beckstrom.html; Gregg Carlstrom, *NSA Dominating Cybersecurity; DHS Official Quits, Warning of Bad Strategy* FEDERAL TIMES, Mar. 16, 2009, *available at* http://www.federaltimes.com/index.php?S=3988926; Strohm, *supra* note 64.

67. For an instructive debate on how cybersecurity policy should be organized within the federal government, see CSIS, *supra* note 8.

68. The CNCI was established pursuant to National Security Presidential Directive 54/Homeland Security Presidential Directive 23, which remains classified. *See* DHS "Protecting Our Federal Networks Against Cyber Attacks," *available at* http://www.dhs.gov/xnews/ releases/pr_1207684277498.shtm.

69. Ellen Nakashima, *Bush Order Expands Network Monitoring*; *Intelligence Agencies To Track Intrusions*, WASH. POST, Jan. 26, 2008, at A3.

70. U.S. HOUSE OF REPRESENTATIVES, HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE, HPSCI WHITE PAPER ON CYBER SECURITY 2-4 (2008).

4. *Coordinate and Redirect Research and Development (R&D) Efforts*: Improve progress in developing new technologies by coordinating disparate government R&D efforts.

- Focus Area II: Defend Against Full Spectrum of Threats

5. *Connect Government Cyber Warning Centers*: Establish connectivity between and among the various federal warning centers to promote awareness of threats.
6. *Develop Government-Wide Cyber Counterintelligence Plan*: Advance a single, integrated plan to address physical and electronic threats to U.S. government information systems.
7. *Increase Security of Classified Networks*: Protect the sensitive information that resides on secure government networks against unauthorized disclosure.
8. Expand Cyber Education: Promote training and professional education for cybersecurity experts.

- Focus Area III: Shape the Future Environment

9. *Develop Leap-Ahead Technologies*: Encourage work on developing transformational technologies.
10. *Define Deterrence Programs and Strategies*: Reduce vulnerabilities and deter cyber attacks.
11. *Develop a Global Supply Chain Risk Management Plan*: Reduce the potential threat from counterfeit or compromised technology acquired on the increasingly global and vulnerable market.
12. *Define the Role of Cyber Security in Private Sector Domains*: Establish new mechanisms to allow government and the private sector to work together in protecting information systems.[71]

The various components to the CNCI resemble the broad policy goals and critical elements contained within earlier strategies and policy directives, though the objectives outlined in four of these initiatives – the first, second, third, and fifth – are much more specific and concrete than much of what we have seen in previous iterations.[72] These four initiatives suggest that the government is moving beyond the previous model of offering sweeping policy recommendations with little guidance on specific action steps and few decisions on the specifics of implementation.

---

71. THE COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE (declassified summary), *available at* http:// www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

72. Arguably, the initial design of NIPC resembles the proposal outlined in Initiative #5, but the CNCI proposal is more advanced.

Unfortunately, this new approach is limited to a few significant steps in improving security that the various agencies have managed to agree are necessary to protect government information systems. The particulars of these initiatives, along with substantive information concerning progress to date in implementation, remain classified and not subject to public discussion.[73]

The remaining CNCI initiatives offer several policy pronouncements, many of which are similar to previous strategies and directives. The classified document provides significant details, including milestones and timelines, but even those often contain generalities such as "identify linkages" and "complete plan" with very little guidance on the substance of the challenges that need to be resolved.

As a result, serious questions remain as to how the government will drive consensus on these initiatives and take action. Much of the heavy lifting has yet to be done, and resolution will inevitably involve significant bureaucratic battles. The CNCI leaves open the question as to how the federal government will approach these battles.

Prior to his election, President Obama issued a very clear statement of policy suggesting that he had an answer. In a campaign speech at Purdue University on July 16, 2008, then-candidate Obama offered a vision of how the federal government would lead the effort to protect cyberspace.

> As President, I'll make cyber security the top priority that it should be in the 21st century. I'll declare our cyber-infrastructure a strategic asset, and appoint a National Cyber Advisor who will report directly to me. We'll coordinate efforts across the federal government, implement a truly national cyber-security policy, and tighten standards to secure information – from the networks that power the federal government, to the networks that you use in your personal lives.[74]

It was this speech that signaled President Obama's intent to reconsider and revise the government's approach to coordinating cybersecurity policy decisions. Only three weeks after his inauguration, President Obama directed his National Security and Homeland Security Advisors "to conduct an immediate review of the plan, programs, and activities underway throughout the government dedicated to cyber security."[75]

The 60-Day Review itself did not delve deeply into the particulars of

---

73. This has become a point of contention, in particular, because the private sector owns and operates the vast majority of the telecommunications and information technology infrastructure but are largely unable to scrutinize the government's approach to cybersecurity.

74. Senator Barack Obama, Remarks at the Summit on Confronting New Threats at Purdue University (July 16, 2008), *available at* http://www.cfr.org/publication/16807/barack_obamas_speech_at_the_university_of_purdue.html.

75. Cyber Security Press Release, *supra* note 1.

the initiatives in the CNCI. Rather, it offered a more general discussion on many of the same broad policy goals that have been outlined in the previous iterations of cybersecurity strategy and leaves the hard work and difficult decisions to the recently named Cybersecurity Coordinator.

To be sure, the particulars of each policy statement and each directive are markedly different. There are significant distinctions and subtle nuances to be drawn between and among these proposals. But, at their essence, these documents share many critical elements.

Each points to the serious nature of the threat of impending cyber attack. Each is a call to action. Each offers policy prescriptions that mirror those of their predecessors:

- Establishing a single office for coordinating cybersecurity policy across the federal government.[76]
- Developing the partnership between public and private entities.[77]
- Promoting public awareness of the threat.[78]
- Establishing a long-term R&D strategy.[79]
- Promoting international cooperation on prevention of cyber crime.[80]
- Creating a centralized organization to respond to cybersecurity incidents.[81]

---

76. PCCIP REPORT, *supra* note 17, at xi, 22, 24, 47-65; PDD 63 White Paper, *supra* note 25, at §VI, Annex A; NATIONAL STRATEGY TO SECURE CYBERSPACE, *supra* note 52, at vii, ix, 1-2, 20, 28, 38-40, 56; HSPD-7, *supra* note 55, at §§12-17, 28; CYBERSPACE POLICY REVIEW, *supra* note 6, at iii-iv, vi, 4-5, 7-12, 20, 37.

77. PCCIP REPORT, *supra* note 17, at xi, 19, 23, 24, 35-45, 47-65, 93-99; PDD 63 White Paper, *supra* note 25, at Sections IV, V; NATIONAL STRATEGY TO SECURE CYBERSPACE, *supra* note 52, at ix, x, xiii, 13, 17, 20-25, 32, 34, 39, 56-58; HSPD-7, *supra* note 55, at §§12, 16, 19(a), 25, 27(c); CYBERSPACE POLICY REVIEW, *supra* note 6, at iv, vi, 18, 28, 37.

78. PCCIP REPORT, *supra* note 17, at xi, 49, 61, 67-71, 96-97, A-9, A-31, A-42, A-52; PDD 63 White Paper, *supra* note 25, at §VI, §VIII, Annex A, Annex B; NATIONAL STRATEGY TO SECURE CYBERSPACE, *supra* note 52, at x-xii, 2-4, 32-33, 37-42, 55, 57-58; CYBERSPACE POLICY REVIEW, *supra* note 6, at I, iv, vi, 8, 13-15, 37.

79. PCCIP REPORT, *supra* note 17, at xi, 23, 89-91, 98-99, A-30-32; PDD 63 White Paper, *supra* note 25, at §VII and Annex A; NATIONAL STRATEGY TO SECURE CYBERSPACE, *supra* note 52, at 2, 34-35, 57; HSPD-7, *supra* note 55, at §§22(e), 30; CYBERSPACE POLICY REVIEW, *supra* note 6, at vi, 8, 14-15, 31-35, 37, 38.

80. PCCIP REPORT, *supra* note 17, at 63-64, 85, 87, 98, A-9; PDD 63 White Paper, *supra* note 26, at §§V, VIII; NATIONAL STRATEGY TO SECURE CYBERSPACE, *supra* note 52, at x, xii-xiii, 4, 17, 49-5254, 59-60; HSPD-7, *supra* note 55, at §§16, 22(a), 27(a); CYBERSPACE POLICY REVIEW, *supra* note 6, at iv-v, vi, 8, 20-21, 28, 33-35, 37, 38.

81. PCCIP REPORT, *supra* note 17, at 22, 51, 62-62, 79-80, 91, 95, 99, A-19; PDD 63 White Paper, *supra* note 25, at §VIII, Annex A; NATIONAL STRATEGY TO SECURE CYBERSPACE, *supra* note 52, at x, 3, 8-9, 19-26, 54, 55; HSPD-7, *supra* note 55, at §27(d); CYBERSPACE POLICY REVIEW, *supra* note 6, at i, iii-v, vi, 8, 23-29, 35, 37, 38.

The 60-Day Review does not ignore these previous documents; in fact, it references them in an effort to draw a distinction with these earlier iterations, but some of this discussion is a little difficult to decipher:

> Both [PDD 63 and HSPD-7] focused purely on defensive strategies, and HSPD-7 did not encompass protection of Federal government information systems. In 2007, the Comprehensive National Cybersecurity Initiative (CNCI) took a different approach. Core to this strategy is the "bridging" of historically separate cyber defensive missions with law enforcement, intelligence, counterintelligence, and military capabilities to address the full spectrum of cyber threats from remote network intrusions and insider operations to supply chain vulnerabilities.[82]

The reference to "defensive strategies" may be meant to imply that PDD 63 and HSPD-7 fail to focus attention on capacity building, information sharing, incident response, and research and development (which represent four of the five key topics discussed in the 60-Day Review).[83] But these two directives, along with the strategy documents preceding them, focus considerable attention on each one of these elements.[84]

It is a reasonable allegation that PDD 63 and HSPD-7 do not explicitly address questions concerning supply chain vulnerabilities,[85] but as awareness of that particular threat increased, the policy directives they established could easily have been modified to incorporate measures to address such concerns.

Separately, the notion that HSPD-7 does not address issues related to federal government information systems appears at odds with that directive's requirement that all federal departments and agencies formulate

---

82. CYBERSPACE POLICY REVIEW, *supra* note 6, at 4.

83. CYBERSPACE POLICY REVIEW, *supra* note 6, at 5.

84. *See* text accompanying notes 76-81.

85. The Internet Security Alliance offers the following description of supply chain vulnerabilities:

> There is a serious danger that the supply chain for electronic components, including microchips, could be infiltrated at some stage by hostile agents. These hostile agents could alter the circuitry of the electronic components or substitute counterfeit components with altered circuitry. The altered circuitry could contain "malicious firmware" that would function in much the same way as malicious software. If the electronic components were connected to any network that enemy attackers could access, the malicious firmware could give them control of the information systems.

Scott Borg, Internet Security Alliance, *Securing the Supply Chain for Electronic Equipment: A Strategy and Framework* (n.d.), *available at* http://www.whitehouse.gov/filesdocuments/cyber/ISA%20%20Securing%20the%20Supply%20Chain%20for%20Electronic%20Equipment.pdf.

plans for protecting the physical and cyber critical infrastructure and key resources that they own or operate.[86]

While, as noted above, the CNCI does take a different approach with respect to four of the dozen initiatives, the 60-Day Review seems to cast, as its central distinguishing feature, the "bridging" approach that the CNCI purportedly brings afresh to the discussion on cybersecurity. But this too seems difficult to understand. PDD 63 and HSPD-7, along with their supporting strategy documents, hold as a central theme the importance of coordinating the disparate roles of law enforcement, the Intelligence Community, and the military. The idea behind each was to establish a single, unified cybersecurity strategy led by the White House and DHS, respectively.[87]

It is an arguable point that PDD 63 and HSPD-7 do not invoke the same language of "bridging" in outlining their directives, but it is abundantly clear from the supporting policy documents that coordination and integration formed the backbone of the previous iterations of U.S. cyber strategy as well. It therefore seems spurious to contend that the concepts are not implicit in the associated directives.[88] Though these three strategies

---

86. HSPD-7, *supra* note 55, at §34.

87. The following are the more salient references to the integration of the various cyber missions in the previous strategy documents:

> The Commission believes that the federal government's job in infrastructure protection includes the traditional defense, law enforcement, intelligence, and other responsibilities as well as the additional effort, resources and processes to respond to the cyber dimension. The structures detailed in our recommendations are designed to expand the reach of existing capabilities, provide a means to coordinate them, and integrate them with the resources of the owners and operators.

PCCIP REPORT, *supra* note 17, at 22.

> The primary functions of the National Office would be government-wide policy formulation, oversight of government activities in infrastructure assurance and cyber security issues, and coordination of cyber support to existing and planned decision-making processes in the law enforcement, national security, counterterrorism, and intelligence areas.

PCCIP REPORT, *supra* note 17, at 51.

> The United States must improve interagency coordination between law enforcement, national security, and defense agencies involving cyber-based attacks and espionage, ensuring that criminal matters are referred, as appropriate, among those agencies.

NATIONAL STRATEGY TO SECURE CYBERSPACE, *supra* note 52, at 59.

88. The responsibility of the National Coordinator and the Secretary of DHS to integrate the various cyber missions across government is evident in the following sections of the relevant presidential directives:

> Although the National Coordinator will not direct Departments and Agencies, he or she will ensure interagency coordination for policy development and implementation, and will review crisis activities concerning infrastructure events with significant foreign involvement. The National Coordinator will provide advice, in the context of the established annual budget process, regarding agency budgets for critical infrastructure protection.

are not identical, they all share the same basic approach to securing cyberspace.

CONCLUSION

The 60-Day Review represents an important step forward in securing U.S. information systems. It once again addresses the importance of improving cybersecurity and the extraordinary difficulties involved in achieving that goal.

It would have been unrealistic for the White House team to provide, within their 60-day time limit, resolution for the thorny cybersecurity problems that the United States is facing. As it turns out, it took the President nearly seven months to appoint a Cybersecurity Coordinator, the first order of business in the Review's action plan.

But as the United States moves forward in securing its information systems, the country must shift away from reflection and study and toward decision and action. The time has passed for the pronouncement of strategic goals without strategic direction. We have been through that process enough times over the past several years.

When Howard Schmidt, the newly appointed Cybersecurity Coordinator, carries out the second order of business outlined in the 60-Day Review (preparing a national cybersecurity strategy), he must do more than just repeat the exercise of cataloging the problems and identifying broad policy objectives. There must be specific direction on how those objectives should be achieved.

The country has reached a point where some tough choices need to be made. Parochial interests will have to be challenged, and risks will have to be taken. As we move forward, there will be no magic bullets, and it will be impossible to please everyone. No matter how these challenges are resolved, there will be influential players in both the public and private sectors who will oppose any solution that the White House ultimately proposes.

The principal reason that the country needs leadership from the White House (as the 60-Day Review recommends) is that there are many

---

PDD 63 White Paper, *supra* note 25, at Annex A.

> The Secretary will continue to maintain an organization to serve as a focal point for the security of cyberspace. The organization will facilitate interactions and collaborations between and among Federal departments and agencies, State and local governments, the private sector, academia and international organizations. To the extent permitted by law, Federal departments and agencies with cyber expertise, including but not limited to the Departments of Justice, Commerce, the Treasury, Defense, Energy, and State, and the Central Intelligence Agency, will collaborate with and support the organization in accomplishing its mission.

HSPD-7, *supra* note 55, at §16.

bureaucratic and proprietary conflicts that need to be addressed and settled decisively.

This idea is hardly new to the people who have been waging those fights for years. Every few years, a proposal has come along in the form of a cybersecurity strategy and a promise of leadership from the White House or DHS, but the implementation has always fallen short. The time has come for that leadership to manifest itself in decisive policy decisions and specific steps that will address these seemingly intractable political, practical, and bureaucratic problems.

For the benefit of national security and economic viability, it is now incumbent upon the President to lend his full authority and commitment to that process and to start taking action.