Who Should Lead U.S. Cybersecurity Efforts?

BY KEVIN P. NEWMEYER

Threats to computer systems, government and commercial networks—and even private citizens' personal information—have exploded in recent years, but the U.S. Government has failed to address these threats adequately. One author has stated that "the cyber threat [is] the most pervasive and pernicious threat" facing the country today.[1] The danger is no longer random teenagers looking for thrills by hacking into the local university network, but sophisticated criminal enterprises looking to steal information or money. The same technologies used to attack financial systems can be unleashed on the Nation's critical infrastructure. In 2007, several Cabinet Departments including Defense, Homeland Security, and Commerce were hacked and terabytes of information were exfiltrated by unknown agents.[2]

The discovery of the Stuxnet virus in 2010 pointed to nation-state involvement in cyber attacks at an unprecedented level and followed the Ghostnet penetrations of the Dali Lama's networks in 2009. Cybersecurity changed from a nuisance problem in the early 1990s to a vital national security issue in the early 21st century. In one of his first acts, President Barack Obama called for a comprehensive review of U.S. policy on cybersecurity, but little has been done to implement the recommendations from the review.[3] While the White House published its *International Strategy for Cyberspace* in May 2011, the document does little to address the current domestic situation. Despite the need

Kevin P. Newmeyer is an Assistant Professor in the Center for Hemispheric Defense Studies at the National Defense University.

for effective national cybersecurity policy, the lack of consensus on which leadership model would best achieve the desired results continues to delay policy implementation.

Several authors have proposed strategies and models for U.S. cybersecurity policy leadership. One prominent school of thought, highlighted by the Center for Strategic and International Studies (CSIS) report *Securing Cyberspace for the 44th Presidency*, is that cybersecurity policy direction should fall under a powerful "czar" in the Executive Office of the President. The authors believe the centralization of power in the White House is the best course of action for providing the necessary policy direction. A second school of thought

> despite the need for effective national cybersecurity policy, the lack of consensus on which leadership model would best achieve the desired results continues to delay policy implementation

argues that policy direction would best be accomplished through a Cabinet-level department. One study from this school argues that responsibility should remain with the Department of Homeland Security due to its role as the lead agency for response to domestic incidents.[4] Others argue that moving the responsibility to the Executive Office of the President from Homeland Security would be insufficient and that a broader restructuring is needed to address the triad of cybersecurity (government at Federal, state, and local levels). Paul Rosenzweig presents an argument for the Department of Defense (DOD) assuming the leadership role based on the depth of talent and experience resident in the National Security Agency (NSA) as compared to the relative lack of human capital in the Department of Homeland Security.[5]

None of the present studies has provided a model that achieves the necessary political consensus on the approach to cybersecurity leadership to implement. Arguments for a strong White House role fail to address the limited success this model has had in other areas such as the war on drugs. Granting the leadership role to DOD ignores the lack of legal authorities for the military to act in domestic roles under the Posse Comitatus Act. The Department of Homeland Security, although having responsibility, has not been able to achieve necessary levels of performance for a variety of reasons. Indeed, the White House czar model offers the advantage of access to the inner circle of the President and the bully pulpit but no regulatory capability. The Cabinet department model offers regulatory power but lacks the authority of the White House in the interagency process.

Options for Cybersecurity Leadership

Policy leadership can remain in the White House with a powerful cyber czar able to set and implement policy decisions with the backing of the President. It could also be vested in one of the Cabinet departments. The Department of Homeland Security currently has a role in policy coordination among government agencies for nondefense networks and systems, but each department remains responsible for its own systems.[6] DOD is responsible for its own systems, both classified and unclassified, as well as some defense-related critical infrastructure necessary to defend the Nation. A third alternative is the creation of a new entity within the Federal Government as a hybrid.

The History

The origins of U.S. cybersecurity policy rest in critical infrastructure protection efforts begun during the Clinton administration. President

Bill Clinton issued Executive Order 13010, "Critical Infrastructure Protection," in 1996, which created the President's Commission on Critical Infrastructure Protection and highlighted the threat to the Nation's economic and national security from cyber attacks. The recommendations of the commission resulted in President Clinton issuing Presidential Decision Directive (PDD) 63 in May 1998.

PDD 63 established several cybersecurity-related organizations within the government including the National Coordinator for Security, Infrastructure Protection, and Counterterrorism with an Office of Critical Infrastructure to support the Coordinator and the National Infrastructure Protection Center. It also was the first step in encouraging the formation of the sectoral Information Sharing and Analysis Centers (ISACs), which have continued to develop and form a key part of the public-private partnership necessary to secure cyberspace. With these centers, the Clinton administration focused on the public-private partnership as the means to secure cyberspace.

While the George W. Bush administration initially continued the Clinton approach, the attacks of 9/11 caused it to significantly refocus from cyber attacks on critical infrastructure to physical attacks by terrorist groups. *The National Strategy to Secure Cyberspace* was published in 2003 but was criticized as more a list of recommendations than a comprehensive strategy document that tied in ends, ways, and means.[7] In addition, the Bush administration published the *National Infrastructure Protection Plan* in 2006, which designated 17 (now 18) key infrastructure sectors that required individual protection plans. The Bush administration also published the *Comprehensive National Cybersecurity Initiative* in 2008, but critics found that its focus on the government Internet domain (.gov) was

too limited. During the Bush administration, cybersecurity responsibility was vague, with limited leadership and diluted responsibility in the White House, Homeland Security, and DOD. Homeland Security was given the overall coordination role, but responsibility still rested with individual agencies.

The Obama administration initiated its cybersecurity efforts with the "60-Day Cyberspace Policy Review." Published in late May 2009, the document was an ambitious effort that presented a solid review of where the government was in relation to cybersecurity, but it offered little in the way of vision on how to get to the destination. The key recommendation of the review is that the President should appoint a single cybersecurity policy official to serve as the central coordinator for government and national efforts. This essentially repeats the recommendation made by the Center for Strategic and International Studies commission report in 2008. Interestingly, the White House did not name a cyber czar until December 2009, when Howard Schmidt accepted the position. In May 2011, the White House issued the *International Strategy to Secure Cyberspace*, which provided an outline of U.S. intentions at the international level, but the document is largely silent on what needs to be done within the government and the Nation to address the challenges domestically.

This brings us to the present day. Although several bills were presented in the 110th Congress and even more in the 111th Congress, no comprehensive cybersecurity legalization has been voted into law, and more than 30 separate pieces of legislation are pending before the 112th Congress.[8] The Congressional Research Service pointed out that no single congressional committee or executive agency has primary responsibility for cybersecurity issues, and this has led to a hodgepodge

President Obama waits to be introduced at critical infrastructure CEOs meeting on cybersecurity at Eisenhower Executive Office Building

The White House (Pete Souza)

of initiatives and good ideas but no unifying focus.[9] Many similarities exist among the documents that form the progression of U.S. cybersecurity policy under three administrations, and the outlines of the policy are sound—but difficult interagency and legislative decisions necessary for effective action remain to be taken. The Government Accountability Office (GAO) commented that cybersecurity leadership was challenged by a lack of top-level leadership and the difficulty of coordinating across multiple agencies. It is a situation that cannot be allowed to continue; there is too much at risk.

Policy Options

There are several basic options for providing cybersecurity leadership within the U.S. Government: a powerful White House–based executive/coordinator; designation of a Cabinet-level agency with the requisite authority to be directive as opposed to consultative in dealing with other departments; and creation of some hybrid entity. If Cabinet-level leadership is chosen, the follow-up question is which department will take the lead, with Homeland Security and DOD as the most likely candidates.

Option A: National Coordinator in the Executive Office of the President. A leading option for cybersecurity leadership is to establish a National Coordinator for Cybersecurity within the White House structure. This option is favored by the CSIS report and the Obama administration's 60-day review. The CSIS plan recommended:

❖ appointing an assistant for cyberspace and establishing a cybersecurity directorate within the National Security Council to assume current Homeland Security Council responsibilities

❖ establishing a National Office for Cyberspace that would assume the responsibilities for the current National Cybersecurity Center and Joint Interagency Cyber Task Force.

The office/official would also assume oversight and control over the multiple cybersecurity functions within the Federal Government and provide a single point of authority on related policy decisions.

The CSIS report placed the blame for the current weakness in cybersecurity policy at the Federal level on "lack of strategic focus, overlapping missions, poor coordination and collaboration, and diffuse responsibility."[10] This lack of focus continued even though the Clinton administration adopted PDD 63 and established Richard Clarke as the National Coordinator for Security, Infrastructure Protection, and Counterterrorism.

Sharp concurred with the CSIS recommendation and pointed out the current lack of an authoritative decisionmaker in a position to compel action to respond to a serious threat to national security.[11] He offered two models—one based on U.S. Strategic Command and its ability to order military components within the Global Information Grid to take action, and the other based on the role played by the Director of National Intelligence (DNI). The DNI cannot direct subordinate agencies to take action, but it has the power to reallocate resources, make budgetary changes, and issue formal taskings that would enable a National Coordinator for Cybersecurity to be effective. The CSIS report also offered the DNI as a potential model

for the coordinator, highlighting the role the DNI plays as a strategist and network-builder. Senator Joseph Lieberman stated that there needs to be a strong cybersecurity coordinator within the White House to oversee both the civilian and military efforts in cybersecurity when he introduced legislation in 2009 to implement the CSIS recommendations.[12]

The White House cyber czar option has not met with universal approval. There are several weaknesses in the PDD 63 version, including the lack of budget authority and difficulties in getting the different departments to agree. Resources are the key in Washington, and without budget authority, the National Cyber Coordinator will have a difficult job. Fundamental to the importance of the cyber czar is the authority delegated to him by the President. To be effective, a leader requires authority commensurate with his responsibility. Empowerment of the cyber czar by the President is fundamental.

Others have questioned the effectiveness of czars in general and argue that yet another rearrangement of the deck chairs is not necessary. They believe that merely placing responsibility in the White House would be insufficient to effect change and that much more drastic reorganization would be required.

Another weakness of the White House cyber czar is the lack of accountability to Congress. The current advisor, Howard Schmidt, was not subjected to a Senate confirmation. Several administrations have rejected calls for Presidential advisors to testify before Congress. The legislation proposed by Senator Lieberman required the President to nominate a cyber coordinator for Senate approval similar to the process used for the DNI. This would instill some measure of congressional oversight and allow Congress to demand testimony from the cyber czar. Senator Robert Byrd noted that

the increased use of Presidential czars presented a potential threat to the Constitution's system of checks and balances. Senator Susan Collins resisted placing cybersecurity leadership in the White House because of the difficulty for congressional oversight of budgets and spending.[13]

Filling the job of a cybersecurity coordinator proved difficult. It took more than 7 months from the completion of the Obama administration's cybersecurity review to name the coordinator. The GAO saw the slow adoption of the policy review's recommendations as a result of the lack of authoritative guidance from the White House.[14]

> the interagency process is far from smooth, and each department secretary values his or her direct line to the President

Option B: Place a Cabinet Department in Charge. Two primary options exist for placing a Cabinet department in charge of cybersecurity: Defense and Homeland Security. Before looking at the details involved with each one, some general observations are in order. Cabinet-level management of the problem is more in line with the traditional response to threats for the U.S. Government. It provides for congressional oversight via the confirmation and budget processes. Cabinet-level officials may be summoned to testify before Congress. Agencies operate under authorities designated in law and are normally empowered to publish regulations that are binding on individuals and companies.

There are challenges to placing a Cabinet-level department in charge. The interagency process is far from smooth, and each department secretary values his

or her direct line to the President. Placing one department in a position to mandate to another how it is to defend and operate its internal computer systems could be problematic. The Trusted Internet Connection (TIC) program that was designed to reduce the number of governmental connections to the Internet is indicative of some of the problems. TIC was launched in 2007 by the Office of Management and Budget to improve the reliability and security of U.S. Government networks, with all departments except DOD required to participate. As of September 2009, none of the 23 agencies involved was fully compliant.[15]

Option B (1): Placing the Department of Homeland Security in Charge. The Department of Homeland Security legal authorities allow it to protect information shared with the private sector, lead a civilian response to a cyber attack, request law enforcement and intelligence assistance from other government agencies, and offer liability protection to companies that sell and use technology to defend against cyber terrorism. Given that more than 85 percent of the government's information traffic flows over private sector networks, it is necessary that the lead agency for cybersecurity has strong relations with the private sector. Homeland Security has already established relationships with the private sector via the ISACs and has included private sector representatives on the watch floor at the National Cybersecurity and Communications Integration Center (NCCIC). Homeland Security also has existing regulatory capacity.

Additionally, Homeland Security has experience with cybersecurity. Since the creation of the department, it has had significant responsibilities for critical infrastructure protection and cybersecurity. The department currently directs

the U.S. Computer Emergency Readiness Team, NCCIC, and has implemented lessons learned and modified its internal structure to address its shortcomings. With its appointment to a focal point role, it has advanced cybersecurity readiness within government, but it is far from perfect.

Among the challenges facing Homeland Security is attracting and retaining sufficient personnel to meet its current, let alone expanded cybersecurity responsibilities. In 2011, the department announced that it plans to increase its cybersecurity staff by 50 percent to 400 by October 2012. This will be particularly challenging in an age when governmental salaries are frozen and the demand from the private sector is continuing to grow.

The CSIS report recommends that the departments retain their existing operational responsibilities. Citing the concept that cybersecurity has now become an essential national security issue, the report argues that a departmental-level agency could not perform the overarching policy coordination needed and thus rejects an enhanced Department of Homeland Security oversight role. With the threat including foreign intelligence agencies and militaries, the report argues that cybersecurity is well beyond the scope of Homeland Security and critical infrastructure protection. Cybersecurity has become an international problem that significantly exceeds the capabilities and management capacity of Homeland Security.

Option B (2): Placing the Department of Defense in Charge. Others suggested that DOD be given the leadership role for cybersecurity across the government. Defense already has responsibility for defending its own systems and has been forward leaning in establishing policy and making organizational changes for cybersecurity. Among the initiatives was the establishment of U.S. Cyber Command to

have overall responsibility within the military for cyber defense and attack issues. The department has also established relationships with the private sector through its defense industrial base cybersecurity pilot initiatives, which fall under its responsibility for defense-related critical infrastructure protection.

Much of the argument for giving cybersecurity leadership responsibility to DOD is based on its combination of experience and manpower.[16] NSA has extensive experience and capability for monitoring and protecting networks. In October 2010, Homeland Security and DOD signed a memorandum of understanding that allowed NSA to support Homeland Security cybersecurity efforts and established a personnel exchange between the agencies.[17]

The drawbacks of placing DOD in charge of cybersecurity are numerous. The legal restrictions of the Posse Comitatus Act on domestic activity by military forces represent only the most basic of issues. The department for the most part lacks regulatory authority and law enforcement powers. It is also a drastic departure from the department's primary mission. Defense also would suffer many of the same challenges in interagency coordination that affect Homeland Security. Additionally, DOD relationships with the private sector are not nearly as extensive as Homeland Security's. Challenges would also be likely from civil liberties groups and Congress to a greater militarization of cyberspace.

Option B (3): Create a New Cabinet-level Agency for Cybersecurity. Creating a new agency that combines all cybersecurity functions offers a chance to address the deficiencies of the current models. Precedents exist with the National Security Act of 1947, which created DOD in response to the new threats emerging from the Cold War and the aftermath of World

War II, and with the creation of the Department of Homeland Security in 2002 in response to the attacks of 9/11. Several experts and politicians have claimed that the threat of cyber attack and other cyber risks have exceeded the capabilities of current arrangements and that cybersecurity

> **a Cabinet-level agency allows for congressional oversight of budgets and leadership consistent with normal constitutional process**

is now an issue of national security. Creation of a new agency allows for the combining of cyber offensive and defensive operations. With proper legislative action, the new agency could be given the necessary regulatory and law enforcement authorities to execute its missions. A Cabinet-level agency allows for congressional oversight of budgets and leadership consistent with normal constitutional process.

Consolidation within one department clarifies the lines of authority and centralizing control over budgets and policy. It counters the lack of unity of effort that is often cited as one of the significant failures of the current system.

The creation of a new agency is not a panacea. As the experience with Homeland Security demonstrated, it is not easy to combine agencies from different departments with different organizational cultures into an effective organization. The delays in properly organizing for cybersecurity and taking effective action are already a national security issue. Turf wars are already an issue with cybersecurity policy. A new agency would also face the same issues as other departments with interagency coordination and compliance among equals.

Option C: Create a Director of Cybersecurity. A variation of the White

House cyber czar would be the creation of a powerful coordinator for cybersecurity along the lines of the DNI. Created in the aftermath of the 9/11 attacks to unify the efforts of domestic, international, and military intelligence programs, the DNI serves as the head of the Intelligence Community. The office establishes objectives and priorities across the intelligence agencies to meet the needs of the executive and legislative branches as well as the Armed Forces. Of critical importance, the DNI develops and executes the budget for the National Intelligence Program based on inputs and priorities from the Service and agency components.

A similar position could be created for cyber security, a Director of Cybersecurity (DCYBER). Implementing legislation could allow for budget oversight across the Federal Government, Senate confirmation of the director, and establishment of clear lines of authority and responsibility with the government as well as for relationships with the private sector.

Analysis of Options

None of the options available is perfect. While several bills have been introduced to Congress over the past several years, progress has been slow. Cybersecurity must compete on the legislative and executive agenda with other significant issues. Health care, financial reform, public debt, and ongoing wars continue to dominate the news and the legislative agenda. It is clear, however, that current structures are insufficient to achieve cybersecurity. Repeated studies and reviews have yielded remarkably similar recommendations.

The centralization of cybersecurity policy initiatives in the Executive Office of the President remains a leading contender; it offers the power of the Presidency to achieve

USAF Brigadier General Gregory Brundidge discusses need to aid collaboration and improve empowerment of cyber defense personnel, technology, and processes

U.S. Army (Martin Greeson)

cross-organizational agreement within the executive branch. Strong leadership is clearly essential for achieving sufficient cybersecurity.

The most significant limitations on a White House cyber czar center on his authority to compel compliance from the disparate executive branch agencies. Without a clear establishment of authorities in legislation, the individual would only have the referent power and authority granted by his standing with the President. Lack of strong backing from the President would constrain his effectiveness in executing his mission. To be effective, the position needs a legal structure solidified in legislation similar to the DNI, which would imply greater congressional oversight.

In examining the various Cabinet-level department options, it is difficult to argue that any of them could overcome the problems of the current structure. The present system has obviously failed as repeated penetration of DOD and other governmental systems has entailed the loss of terabytes of data.

Placing the responsibilities in DOD presents numerous challenges. While defending systems from foreign attack could become a defense mission, the department has little experience with regulatory matters and procedures. The civil liberty implications of using the military in domestic intelligence activities are enormous. The Posse Comitatus Act would have to be significantly revised to allow for military activity beyond training inside the United States. This would cause civil liberties debates greater than those over the USA PATRIOT Act. Placing the military in charge of cybersecurity for civilian systems would not be politically viable.

Creation of a new department to focus on cybersecurity would achieve many of the objectives listed in the CSIS report. It would allow for collection of the many siloed activities currently under

DOD, Homeland Security, Commerce, and State. The establishing legislation would have to clarify authorities, regulatory powers, and relationships with the existing departments. The budget and nomination process provides for the needed congressional oversight.

The challenges to a new department are daunting. Starting something in Washington at the Cabinet level normally requires a dramatic trigger event along the lines of 9/11 or an indefatigable champion willing to expend the political capital necessary to carry the battle. To date, this has not occurred on the cyber front. Other issues have occupied the political space and pushed cybersecurity to the rear. A new department would also face significant growing pains. In the current budget and political climate, it is unlikely to garner the support needed in Congress. While it may provide the best operational and constitutional solution, it is the least likely in the near to mid term.

Retaining cybersecurity leadership within the Department of Homeland Security is the most likely alternative among the Cabinet-level organizations. As previously discussed, the department has the basic regulatory functions necessary and significant experience in cyber-security issues. The relationship with DOD has improved significantly in cybersecurity and a cooperative strategy is in place.

What Homeland Security lacks in the cyber-security leadership role is consistent Presidential and congressional focus. It has a coordination role given to it by the President in a series of decision documents, but coordination is not control. Homeland Security cannot truly compel other departments to adhere to its policies and decisions. The department itself is still growing and developing. Less than 10 years old, it does not have the longstanding policies and cultures of the Department of State or DOD. Congress has not helped the problems at the department and must clarify its committee jurisdiction issues regarding not only cybersecurity but also all of the missions assigned to Homeland Security. At present, more than 80 committees have a role in the department's oversight.[18]

The other significant hurdle for Homeland Security is building the human capital necessary to establish and implement policy and operations in support of cybersecurity. The department has announced ambitious plans for growing its cyber forces, but it will not be easy. Recruiting and retaining these specialists will be a constant challenge.

Recommendations

Cybersecurity is a daunting policy problem, and a simple solution is not apparent. The choice will be a compromise among various options that must occur within a political environment with a limited attention span and several competing priorities. The President and Congress should do the following:

❖ Establish a Director of National Cybersecurity. The director role would be modeled on the DNI with some significant enhancements. With proper legislative action, the DCYBER would have clear budget and operational authority over cyber-security programs across the Federal Government. Individual departments would not be able to reprogram funds without DCYBER approval. The position would be subject to the advice and consent of the Senate as other political appointees. DCYBER would have a fixed 5-year term with the possibility of reappointment for 1 additional term. Fixed terms allow for a

measure of independence from political concerns and are used in other Federal agencies such as the Federal Bureau of Investigation and Equal Opportunity Commission.

❖ Enact legislation to provide Homeland Security clear directive authority for cybersecurity across nondefense agencies. Simple coordination has not been effective in improving cybersecurity across Federal agencies. A definitive authority is required for Homeland Security to mandate action and adjust the priorities of other agencies for this critical national security issue.

❖ Enact legislation to establish a U.S. Government Cybercorps. To attract and retain qualified personnel, the standard General Schedule has proven insufficient. A better alignment of incentives and streamlined recruiting with flexible personnel policies is necessary. Positions within agencies would be allocated for Cybercorps-designated personnel in much the same manner as Intelligence Community and acquisition specialists are currently designated. Funds would be established for continued professional education and training for Cybercorps personnel to remain current.

❖ Formalize personnel exchanges between Homeland Security and DOD for cybersecurity personnel. The existing memorandum of understanding between the two departments should be codified in legislation. Congress needs to outline the limitations on intelligence exchange between military and law enforcement for cyber related issues.

❖ Establish a permanent position for private sector participation in DCYBER. With the vast majority of computer networks and other critical infrastructure under private sector control, it is imperative that they have a continuous voice in the policymaking process. Confidentiality and liability issues are manageable.

Conclusion

Cybersecurity concerns have only grown with the expansion of digital technology into all aspects of daily life and daily government operations. President Obama in the *International Strategy to Secure Cyberspace* stated that cybersecurity is part and parcel of everyday life for all Americans and much of the world. Maintaining the status quo of scattered responsibilities and patchwork policy solutions is not only poor governance but also potentially places the Nation's critical assets at risk.

Establishing a strong DCYBER at a Cabinet-equivalent level would provide the necessary leadership within the Federal Government. The Department of Homeland Security would continue to play an important role in protecting civilian governmental systems and coordinating with the private sector. DOD has already taken several steps to improve its capabilities for action, and senior leaders are addressing cybersecurity in a responsible manner.

Congress and the President need to demonstrate the political leadership and expend the political capital to make the needed changes in legislation and structure on the domestic front. Waiting for a perfect solution to appear is not an option. Decisive action is required now. **PRISM**

Notes

[1] Walter Gary Sharp, Sr., "The Past, Present and Future of Cybersecurity," *Journal of National Security Law & Policy* 4, no. 13 (2010), 13–16, available at <http://insct.org/jnslp/wp-content/uploads/2010/08/03_Sharp.pdf>.

[2] This problem continues unabated. During the presentation of the Department of Defense Cyber Security Strategy in July 2011, Deputy Secretary of Defense William J. Lynn III commented that another major loss of sensitive data occurred in early 2011.

[3] See the *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, DC: The White House, 2009), available at <www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf> and the follow-on critique *Cybersecurity Two Years Later*, A Report of the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency (Washington, DC: CSIS, January 2011), available at <http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf>.

[4] Gus P. Coldebella and Brian M. White, "Foundation Questions Regarding the Federal Role in Cybersecurity," *Journal of National Security Law & Policy* 4, no. 233 (2010), 233–245.

[5] Paul Rosenzweig, "10 Conservative Principles for Cybersecurity Policy," Backgrounder No. 2513 (Washington, DC: The Heritage Foundation, 2011), available at <www.heritage.org/research/reports/2011/01/10-conservative-principles-for-cybersecurity-policy>.

[6] Sharp.

[7] The CSIS Commission on Cybersecurity for the 44th President was a strong critic. See also Catherine A. Theohary and John Rollins, *Cybersecurity, Current Legislation, Executive Branch Initiatives, and Options for Congress* (Washington, DC: Congressional Research Service, 2009).

[8] Amber Corrin, "Will Congressional Infighting Stall Cybersecurity Laws?" *Federal Computer Week*, October 11, 2011, available at <http://fcw.com/articles/2011/10/11/congress-cybersecurity-legislation-umuc-panel.aspx>.

[9] Theohary and Rollins.

[10] *Cybersecurity Two Years Later*, 34.

[11] Sharp, 15–16.

[12] Patrick Marshall, "Cybersecurity," *CQ Researcher* 20, no. 8, February 26, 2010.

[13] Ibid.

[14] David A. Powner, *Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed*, GAO-11-24 (Washington, DC: Government Accountability Office, October 2010), available at <www.gao.gov/products/GAO-11-24>.

[15] Gregory C. Wilshusen, *Concerted Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies*, GAO-10-237 (Washington, DC: Government Accountability Office, March 2010), available at <www.gao.gov/new.items/d10237.pdf>.

[16] Rosenzweig.

[17] "Memorandum of Agreement Between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity," September 2010, available at <www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf>.

[18] See Timothy Balunis, Jr., and William Hemphill, "Escaping the Entanglement: Reversing Jurisdictional Fragmentation over the Department of Homeland Security," *Journal of Homeland Security & Emergency Management* 6, no. 1 (2009).