Will There Be Cybersecurity Legislation?

John Grant*

> Independent efforts will not be sufficient to address this challenge without a central coordination mechanism, an updated national strategy, an action plan developed and coordinated across the Executive Branch, and *the support of Congress.*[1]

INTRODUCTION

In the course of just a few decades, information technology has become an essential component of American life, playing a critical role in nearly every sector of the economy. Consequently, government policy affecting information technology currently emanates from multiple agencies under multiple authorities – often with little or no coordination. The White House's Cyberspace Policy Review (the Review) wisely recognized that the first priority in improving cybersecurity is to establish a single point of leadership within the federal government and called for the support of Congress in pursuit of this agenda.

Congressional involvement in some form is inevitable, but there is considerable uncertainty as to what Congress needs to do and whether it is capable of taking action once it decides to do so. With an agenda already strained to near the breaking point by legislation to address health care reform, climate change, energy, and financial regulatory reform – as well as the annual appropriations bills – the capacity of Congress to act will depend, in some part, on the necessity of action. For the last eight years, homeland security has dominated the congressional agenda. With the memory of the terrorist attacks of September 11 becoming ever more distant, there may be little appetite for taking on yet another major piece of complex and costly homeland security legislation.

Part I of this article considers the question of necessity. The Homeland Security Act,[2] the Federal Information Security Management Act,[3] the Communications Act,[4] and any number of other statutes provide substantial authorities over federal and nonfederal information infrastructure.[5] Do

---

* Minority Counsel for the Senate Committee on Homeland Security and Governmental Affairs. The views expressed in this article are those of the author and do not necessarily reflect those of the Members and Staff of the Committee.

1. CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE 7 (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (emphasis added).

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

3. Federal Information Security Management Act, 44 U.S.C. §§3541-3549 (2006).

4. Communications Act of 1934, 47 U.S.C. §§151-161 (2006).

5. "The term 'information infrastructure' means the underlying framework that

these statutes provide the federal government with all of the tools that it needs to effectively manage cybersecurity? Are they compatible, or do they create a series of conflicting authorities that will paralyze the agencies that seek to execute them?

Part II considers whether, if Congress needs to act, it can effectively do so. Information technology has become an engine of the economy, and the businesses that provide it wield enormous influence. Any substantial reorganization will draw opposition. Without the impetus of an attack on U.S. cyberspace comparable to the September 11 attacks, we may legitimately ask whether any reform legislation can overcome the opposition of powerful stakeholders. Beyond the political realities, there is also the question of whether, given its inherent institutional limitations, Congress can effectively legislate in this area. Does the slow pace of congressional action coupled with a general lack of technical expertise inhibit Congress's ability to craft and enact legislation responsive to the cybersecurity vulnerabilities of today and the future?

This article concludes by identifying the likely endpoints in a spectrum of options for organizing the federal government's cybersecurity regime.

I. THE QUESTION OF NECESSITY

There are a number of potential sources of executive branch authority over the security of both federally controlled and privately owned information infrastructure. While volumes could be written appraising the strengths and weaknesses of each source, this article has a different focus. It briefly discusses the major authorities and then proposes that congressional action focus less on granting new authority and more on defining how the existing authorities interact.

A. The Federal Information Security Management Act

The Federal Information Security Management Act (FISMA) was enacted to "provide for development and maintenance of minimum controls required to protect federal information and information systems" and "provide a mechanism for improved oversight of federal agency information security programs."[6] FISMA attempts to accomplish this in two ways – by delineating a set of agency responsibilities and giving the Office of Management and Budget (OMB) oversight authority.[7]

---

information systems and assets rely on in processing, transmitting, receiving, or storing information electronically." Information and Communications Enhancement Act (ICE), S. 921, 111th Cong. §3551(b)(4) (2009).

6. 44 U.S.C. §§3541(3)-3541(4) (2006).

7. *Id.* §§3543–3544.

Specifically, agencies are required to implement agency-wide programs:

> . . . providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of
>
> (i) information collected or maintained by or on behalf of the agency; and
>
> (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.[8]

In short, agencies are given broad authority to make their own security arrangements under the purportedly watchful eye of OMB.

As implemented, FISMA has received reviews that are far from glowing. The Government Accountability Office (GAO) continues to designate federal information security as a government-wide, high-risk area in biennial GAO reports to Congress.[9] FISMA has been criticized as a "paperwork exercise" that does little to actually improve security.[10] The Center for Strategic and International Studies (CSIS), in its *Securing Cyberspace for the 44th Presidency*, outlined a concise litany of failures:

> FISMA lacks effective guidance and standards for determining appropriate levels of risk; it lacks requirements for testing or measuring an agency's vulnerabilities or its plans for mitigating such vulnerabilities; it fails to define agency responsibilities for effective controls over contractors or vendors; and it does not recognize the emergence of new technologies and network architectures.[11]

Nonetheless, it is important to note that these criticisms do not necessarily suggest that federal agencies lack the statutory authority to protect their information infrastructure. Rather, it is FISMA's usefulness as a measure of security and an oversight tool that is questionable. While in the end it may be considered *desirable* for Congress to act to address these perceived weaknesses in FISMA, it does not follow that it is *necessary* for

---

8. *Id.* §3544(a)(1)(A).

9. *See* GOVERMENT ACCOUNTABILITY OFFICE, HIGH-RISK SERIES: AN UPDATE 47 (2009) (GAO-09-271), *available at* http://www.gao.gov/new.items/d09271.pdf.

10. Dan Verton, *Survey Finds Digital Divide Among Federal CISOs*, COMPUTERWORLD, Nov. 23, 2004, *available at* http://www.computerworld.com/s/article/ print/97763/Survey_finds _digital_divide_among_federal_CISOs.

11. CENTER FOR STRATEGIC AND INT'L STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY 1, 69 (2008), *available at* http://csis.org/files/media/csis/pubs/081208_securing cyberspace_44.pdf [hereinafter CSIS Report].

Congress to act in order for agencies to have the means to secure their information infrastructure.

B. The Homeland Security Act

Under the Homeland Security Act of 2002,[12] various successor statutes[13] and executive orders such as Executive Order 13,286,[14] the Department of Homeland Security (DHS) has responsibilities for protecting information infrastructure. Thirteen key cybersecurity responsibilities have been vested in the DHS, including:

> (1) developing a comprehensive national plan for [Critical Infrastructure Protection], including cybersecurity; (2) developing partnerships and coordinating with other federal agencies, state and local governments, and the private sector; (3) developing and enhancing national cyber analysis and warning capabilities; (4) providing and coordinating incident response and recovery planning, including conducting incident response exercises; and (5) identifying, assessing, and supporting efforts to reduce cyber threats and vulnerabilities, including those associated with infrastructure control systems.[15]

Many of these responsibilities derive from authorities that are not specifically related to information technology, but rather extrapolated from general authorities relating to critical infrastructure protection.

The DHS has come under considerable criticism for its discharge of these responsibilities. GAO has reported that the "DHS has yet to comprehensively satisfy its key responsibilities for protecting computer-reliant critical infrastructures."[16] This could be due in part to ongoing uncertainty as to just what the Department's role should be in terms of privately owned critical infrastructure. As noted in the Review:

> The question remains unresolved as to what extent protection of these same infrastructures from the same harms by the same actors [referring to physical attacks on critical infrastructure by criminals or terrorists] should be a government responsibility if the attacks

---

12. *See, e.g.*, Homeland Security Act, 6 U.S.C. §143 (2006).

13. *See, e.g.*, Implementing Recommendations of the 9/11 Commission Act of 2007, 6 U.S.C. §121 (2006 & Supp. I 2007).

14. Exec. Order No. 13,286, *Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security*, 68 Fed. Reg. 10,619 (Feb. 23, 2003).

15. GOVERMENT ACCOUNTABILITY OFFICE, CYBERSECURITY: CONTINUED FEDERAL EFFORTS ARE NEEDED TO PROTECT CRITICAL SYSTEMS AND INFORMATION 3 (GAO-09-835T 2009), *available* at http://www.gao.gov/new.items/d09835t.pdf.

16. *See id.* at 6.

> were carried out remotely via computer networks rather than by direct physical action.[17]

The CSIS report concluded that the supposed public-private partnership touted by the DHS to address these questions "is marked by serious shortcomings," including "lack of agreement on roles and responsibilities, an obsession with information sharing for its own sake, and the creation of new public-private groups each time a problem arises without any effort to eliminate redundancy."[18]

C. Miscellaneous Regulatory Authorities

Authority to provide for the security of information infrastructure is not always found in statutory provisions labeled "cybersecurity." Information technology is a supporting component of nearly every major piece of critical infrastructure, much of which is itself regulated by specific federal agencies. Thus, cybersecurity often falls under the purview of other regulatory bodies through provisions of their individual authorizing statutes.

For example, the Electric Reliability provision of the Federal Power Act gives the Federal Energy Regulatory Commission (FERC) the authority to enforce compliance with reliability standards.[19] A "reliability standard" is defined as "a requirement. . . . to provide for reliable operation of the bulk-power system" and includes "requirements for the operation of existing bulk-power system facilities, including cybersecurity protection. . . ."[20] As with other authorities, some question this provision's effectiveness. The Electric Reliability provision of the Federal Power Act has been criticized as ineffective because of the long lead time before standards can be established, lack of authority to compel power companies to protect security-sensitive information, and the excessive degree of discretion given to utilities in deciding how to implement the standards.[21] When a potential cyber vulnerability in the electrical grid was identified in 2008, Congress even considered passing legislation to provide the FERC with additional authority to respond to imminent cybersecurity threats.[22]

---

17. CYBERSPACE POLICY REVIEW, *supra* note 1, at 28.

18. CSIS Report, *supra* note 11, at 43.

19. 16 U.S.C. §824o(b) (2006).

20. *Id.* §824o(a)-(3).

21. *See Cyber Security: Hearing Before the S. Comm. on Energy & Nat. Resources*, 111th Cong. 1 (2009) (testimony of Joseph McClelland, Off. of Electric Reliability).

22. *See* Stephanie Condon, *Cybersecurity Worries Spur Congress To Rethink Electrical Grid*, CNET NEWS, Sept. 12, 2008, http://news.cnet.com/8301-13578_3-10040101-38.html.

D. Inherent Authority

In addition to the statutory authorities held by agencies, there is an argument that the President has certain inherent powers flowing from constitutionally granted war powers. If the concept of "war powers" is extended to encompass the broader notion of national security, then the President could have significant cybersecurity authorities that require no congressional authorization.[23] However, broad invocation of such powers remains controversial, and recent attempts based on a broad interpretation of these powers, such as to justify warrantless wiretapping, may make their use in the cybersecurity context politically unpalatable.

E. Organization

Given these authorities, there is a strong case to be made that the executive branch already possesses significant authority to address security vulnerabilities in both the federal and nonfederal information infrastructure. However, while the executive branch may possess adequate authority, the questions – in some cases, ambiguity – surrounding the execution of that authority suggest that the executive branch is not currently organized in a manner that allows it to wield that authority effectively.

The Review particularly focused on how conflicting authorities may result in a lack of clear leadership, a significant concern:

> Answering the question of "who is in charge" must address the distribution of statutory authorities and missions across departments and agencies. This is particularly the case as telecommunications and Internet-type networks converge and other infrastructure sectors adopt the Internet as a primary means of interconnectivity. Unifying mission responsibilities that evolved over more than a century will require the Federal government to clarify policies for cybersecurity and the cybersecurity-related roles and responsibilities of various departments and agencies.[24]

The CSIS report reached a similar conclusion, comparing the legion of cyber experts scattered throughout the federal government to a "large fleet of well-meaning bumper cars."[25]

This problem is not necessarily unique to cybersecurity. A recent report from the Project on National Security Reform suggested that the national security apparatus in general is structurally incapable of handling

---

23. *See* John Rollins & Anna C. Henning, *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations* (Cong. Res. Serv. R40427), Mar. 10, 2009, at 10.

24. CYBERSPACE POLICY REVIEW, *supra* note 1, at 4.

25. CSIS Report, *supra* note 11, at 34.

threats that require the simultaneous integration of the assets of American power.[26] Cybersecurity is a prime example of an issue that presents new challenges that cut across multiple agency jurisdictions and consequently requires government-wide coordination. Yet, as the Project on National Security Reform concluded, "departments and agencies, when faced with challenges that fall outside traditional departmental competencies, almost invariably produce ad hoc arrangements that prove suboptimal by almost every measure."[27] While a discussion of reforming the entire national security system is beyond the scope of this article, the issues confronting the government in organizing its response to cyber threats are quite comparable.

Both the CSIS report and the Review concluded that the leadership question can be resolved by establishing White House dominance. The Review concluded that "anchoring and elevating leadership for cybersecurity-related policies at the White House signals to the United States and the international community that we are serious about cybersecurity."[28] The CSIS report concluded that "only the White House has the necessary authority and oversight for cybersecurity."[29] Although the Obama administration has yet to fully implement the recommendations of either the CSIS report or the Review, its penchant for centralized White House authority – in the form of the increasingly ubiquitous "czar" – is well established.[30]

Thus, the necessity of congressional action may arise not from the need to adopt these centralization recommendations, but rather from a desire to prevent their implementation. The reliance on issue czars in the Administration has drawn fire from several camps, including prominent voices in Congress. Senator Robert C. Byrd, the Senate's senior member, has suggested that such positions "can threaten the Constitutional system of checks and balances."[31] Other members have noted that czars operating out of the Executive Office of the President are subject to less oversight than

---

26. *See* PROJECT ON NAT'L SECURITY REFORM, FORGING A NEW SHIELD, at ii (2008), *available at* http://www.pnsr.org/data/files/pnsr_forging_a_new_shield_report.pdf. *See also* Gordon Lederman, *National Security Reform for the Twenty-first Century: A New National Security Act and Reflections on Legislation's Role in Organizational Change*, 3 J. NAT'L SECURITY L. & POL'Y 363 (2009).

27. PROJECT ON NAT'L SECURITY REFORM, *supra* note 26, at viii.

28. CYBERSPACE POLICY REVIEW, *supra* note 1, at 7.

29. CSIS Report, *supra* note 11, at 36.

30. *See* Laura Meckler, "*Czars" Ascend at White House*, WALL ST. J., Dec. 15, 2008, at A6. On December 22, 2009, the White House appointed a Cybersecurity Coordinator, Howard Schmidt. *See* Ellen Nakashima & Debbi Wilgoren, *Obama To Name Former Bush, Microsoft Official as Cyber-Czar*, WASH. POST, Dec. 22, 2009, at A04.

31. Press Release, Off. of Sen. Robert C. Byrd, Byrd Questions Obama Administration on Role of White House "Czar" Positions (Feb. 25, 2009), *available at* http://byrd.senate.gov/mediacenter/view_article.cfm?ID=331.

Senate-confirmed Cabinet secretaries and are consequently less accountable to the American public for their actions.[32] Furthermore, as noted by the Project on National Security Reform, "White House centralization of interagency missions also risks creating an untenable span of control over policy implementation," impeding "timely, disciplined, and integrated decision formulation and option assessment over time."[33] If Congress takes these criticisms to heart, then it should feel compelled to initiate cybersecurity reform, lest the White House act to fill a perceived leadership vacuum.

F. Summary

Although the way in which cybersecurity authority has been implemented leaves much to be desired, it appears that the Constitution and Congress have imbued the executive branch with sufficient authority to provide for the security of both public and private information infrastructures. Furthermore, the President's prerogative to organize and direct the activities of the executive branch would allow him an attempt to overcome the obstacles that have prevented effective interagency coordination. However, Congress may still find it necessary to act in order to ensure that the management of the cybersecurity mission is sufficiently transparent and accountable to Congress and the American public.

II. CONGRESSIONAL CAPACITY

Deciding to act is only one part of the challenge, however. The next question to consider is whether Congress has the capacity to enact legislation in this area. Information technology is a powerful component of the U.S. economy. Sizeable corporate interests wield considerable influence on elected officials. At the same time, inherent institutional weaknesses in the legislative branch may hamper its ability to legislate effectively in response to cyber threats and vulnerabilities. This part discusses the factors influencing Congress's ability to pass legislation on information technology and what that legislation would need to look like.

A. Burden

Climate change legislation, regulation of financial institutions, and myriad other issues compete with cybersecurity for congressional attention.[34] If historical precedent is followed, the second session of the

---

32. *See, e.g.*, Letter from Sen. Susan Collins to President Barack Obama (Sept. 15, 2009), *available at* http://www.ireport.com/docs/DOC-329196.

33. *See* PROJECT ON NAT'L SEC. REFORM, *supra* note 26, at viii.

34. *See*, *e.g.*, Anna Mulrine, *Democrats in Congress Push Ambitious Agenda*, U.S. NEWS, July 8, 2009, *available at* http://www.usnews.com/articles/news/politics/2009/07

111th Congress will be abbreviated in order to allow members to return to their districts to campaign for the midterm elections. There may be little time on the crowded agenda to take up contentious and complex legislation relating to cybersecurity. Consequently, if cybersecurity legislation is going to pass, congressional leadership will be looking for a relatively non-controversial bill that will attract few amendments and consume little precious floor time.

B. Motivation

Congressional action is often most expeditious when motivated by outside forces – one need only look at the spate of legislation passed in the wake of the terrorist attacks of September 11, 2001. There is a question as to whether any event has occurred or set of new circumstances exists that will spur public pressure for congressional action.

Certainly, cyber threats have made newspaper headlines in the course of the last several years. For example:

- Newspapers reported that both the McCain and Obama campaign computer systems were penetrated, as well as those of a number of government agencies.[35]
- Several vulnerabilities to the electrical grid were reported.[36]
- The United States was the victim of a prolonged "denial of service" attack directed at both government and privately owned systems.[37]
- Identity theft as a consequence of cyber crime is on the rise and companies lose millions of dollars per year as a consequence.[38]

Nonetheless, none of these incidents has had a significant or prolonged effect on the general public's use of the information infrastructure. There has been no spectacular disruption of service or long-term damage to critical infrastructure. Consequently, there has been no sizeable public clamor for action on cybersecurity – particularly when other issues, such as

---

/08/democrats-in-congress-push-ambitious-agenda.html.

35. *See* Dan Goodin, *Obama, McCain Campaigns Hit with 'Sophisticated' Cyberattack*, REGISTER, Nov. 5, 2008, *available at* http://www.theregister.co.uk/2008/11/05/obama_mccain_cyberattack/.

36. *See* Condon, *supra* note 22.

37. *See* Julian E. Barnes & Josh Meyer, *Cyber Attack Is Met with Speculation and Shrugs; Some Think North Korea Launched the Virus Whose Targets Included the White House and NYSE. Others Scoff.*, L.A. TIMES, July 9, 2009, at A10.

38. *See Cybercrime Rising, Report Warns*, BBC NEWS, Mar. 31, 2009, *available at* http://news. bbc.co.uk/2/hi/americas/7973886.stm.

health care reform[39] or the confirmation of a new Supreme Court justice,[40] dominate the news cycle.

C. Complexity

Cybersecurity involves complex technical issues that are constantly evolving thanks to the rapid pace of technical innovation. Members of Congress are regularly briefed on both the threats and the measures used to combat them. Such briefings can be highly technical. Even when they are not, they can still be beyond the understanding of members with less familiarity with the Internet and information technology. As a consequence, the development of comprehensive cybersecurity legislation will often be driven by staff, lobbyists, and industry stakeholders with the expertise to understand the technical issues under discussion. While this allows bills to be drafted and introduced, there is a point in the life of any piece of legislation in which direct action from Senators or Members of Congress is necessary to secure space on a busy committee mark-up agenda or the packed floor schedule in each chamber. However, once such personal action is taken members become obligated to make floor speeches, attend press conferences, and field questions related to cybersecurity – something they may be hesitant to do if they are uncomfortable with the subject matter.

D. Opposition

As with any piece of legislation, a key factor in determining the likelihood of passage is the level of opposition. In general terms, the most significant lightning rod in any cybersecurity legislation is likely to be the imposition of mandatory standards on privately owned information technology infrastructure.[41] It has frequently been claimed that the Internet is free from regulation and that any attempt to impose a mandatory regime could stifle the innovation that has turned information technology into an economic engine.[42] Any bill that is perceived – rightly or wrongly – as imposing regulation on the Internet will draw substantial opposition.

---

39. *See, e.g.*, David M. Herszenhorn & Robert Pear, *Final Votes in Congress Cap Battle over Health*, N.Y. TIMES, Mar. 26, 2010, at A17.

40. *See, e.g.*, Sheryl Gay Stolberg, *A Knock-Down, Drag-Out – Yawn*, N.Y. TIMES, June 3, 2010, at A19 (Senate confirmation hearing for Elena Kagan scheduled to begin on June 28, 2010); Charlie Savage, *Senate Approves Sotomayor for the Supreme Court*, N.Y. TIMES, Aug. 7, 2009, at A1.

41. *See* Joby Warrick & Walter Pincus, *Senate Legislation Would Federalize Cybersecurity; Rules for Private Networks also Proposed*, WASH. POST, Apr. 1, 2009, at A4.

42. For an excellent discussion of how cybersecurity measures currently under discussion affect innovation, see Gregory T. Nojeim, *Cybersecurity and Freedom on the Internet*, 4 J. NAT'L SECURITY L. & POL'Y 119 (2010).

An example of potential opposition can be seen by the reaction to Senators Jay Rockefeller and Olympia Snowe introduction of the Cybersecurity Act of 2009. The bill includes provisions establishing cybersecurity standards for both government and private sector information infrastructure, requiring the licensing and certification of cybersecurity professionals, and designating the Department of Commerce as the clearinghouse for cybersecurity threat and vulnerability information.[43] Reaction to the bill was initially muted but gives an indication of potential future opposition. TechAmerica, a leading industry trade association, warned that "some provisions of the Rockefeller-Snowe bill may impose prescriptive regulations on the private-sector that could inhibit the very technology innovation needed for greater prosperity and security."[44] Phil Bond, President of TechAmerica, added that "the last thing we need is cybersecurity innovation that moves at the speed of government."[45] Larry Clinton, President of the Internet Security Alliance, criticized the bill's vagueness and stated that without clarification his organization – which has close ties to Verizon, Nortel, and other key industry stakeholders – could not support the bill.[46]

In addition to industry opposition, the Rockefeller-Snowe bill drew concern from the privacy and civil liberties community as well. The Center for Democracy and Technology expressed concern that the bill would give "the federal government extraordinary power over private sector Internet services, applications and software."[47] The Electronic Frontier Foundation argued that provisions of the bill "could eviscerate statutory protections for private information."[48]

E. Jurisdiction

Information technology has become part of nearly every major industry and service in the United States. Consequently, most – if not all – of the congressional committees could seek jurisdiction over cybersecurity.

---

43. Cybersecurity Act of 2009, S. 773, 111th Cong. (2009).

44. Press Release, TechAmerica, TechAmerica Welcomes Congressional Focus on Cybersecurity, Expresses Reservations About Rockefeller Bill (Apr. 3, 2009), *available at* http://www.techamerica.org/techamerica-welcomes-congressional-focus-on-cybersecurity-expresses-reservations-about-rockefeller-bill.

45. *Id.*

46. *See* Declan McCullagh, *Bill Would Give President Emergency Control of Internet*, SODAHEAD.COM, Aug. 28, 2009, http://www.sodahead.com/united-states/bill-would-give-president-emergency-control-of-internet/blog-147327/.

47. Kenneth Corbin, *Groups Warn New Cybersecurity Bill Oversteps*, INTERNET NEWS, Apr. 7, 2009, http://www.internetnews.com/government/print.php/3814171.

48. Jenifer Granick, *Federal Authority over the Internet? The Cybersecurity Act of 2009*, Electronic Frontier Found., Apr. 10, 2009, http://www.eff.org/deeplinks/2009/04/cybersecurity-act.

Already in the Senate, the Chairman and Ranking Member of the Commerce Committee have introduced two bills,[49] several prominent members of the Judiciary Committee have introduced data breach bills[50] with significant cybersecurity implications, and the Chairman and Ranking Member of the Homeland Security and Governmental Affairs Committee have announced their intention to develop comprehensive cybersecurity legislation.[51] Given the prominence of the issue and the economic power of the information technology industry, it is unlikely that the aforementioned committees – among the most powerful in the Senate – will cede jurisdiction without considerable reluctance. Similar jurisdictional tensions can be found in the House of Representatives as well.[52]

III. A RANGE OF OPTIONS

As this article has argued, the federal government may already possess sufficient authority to manage cybersecurity, and if congressional action is needed, it is in the area of reorganizing those authorities to ensure that the federal government strategy is effectively coordinated. Congress has a range of approaches to address this reorganization. At one end of the spectrum is a more draconian regime that would involve vesting a single entity with the necessary authority over both the federal government and the private sector to direct measures to ensure the security of information infrastructure. At the other end of the spectrum is a regime that would leave each agency or component with its existing authority but establish decisionmaking mechanisms by which it could be ensured that these individual authorities were coordinated and working consistently.

A. Direct Authority

The most dramatic and arguably the cleanest approach to establishing a new cybersecurity regime would be the creation of a single new entity to oversee the security of the information infrastructure. This new cybersecurity "agency" would be responsible for coordinating the federal government's entire approach to information infrastructure security. Such authority would go beyond mere strategy development, and include the authority to direct action both at the agency level and to some extent within

---

49. Cybersecurity Act of 2009, *supra* note 43.

50. Data Breach Notification Act, S. 139, 111th Cong. (2009); Personal Data Privacy and Security Act, S. 1490, 111th Cong. (2009).

51. *See, e.g.*, Gautham Nagesh, *Lawmakers Join Forces on Cybersecurity Legislation*, NEXTGOV, Sept. 4, 2009, http://www.nextgov.com/nextgov/ng_20090914_5789.php.

52. *See e.g.*, Cybersecurity Education Enhancement Act, H.R. 266, 111th Cong. (2009) (dealing primarily with grants to support cybersecurity education and professional development, which was referred to the House Committees on Science and Technology, on Education and Labor, and on Homeland Security).

the private sector. The agency would have the authority to set security standards that would be binding on agencies and on the information infrastructure controlled by the private sector. The agency would be both seizing authorities from other Cabinet-level departments and directing those departments in securing their own networks, as well as regulating information technology systems in private sector industries that are otherwise subject to the regulatory authorities of the departments. The agency would, therefore, need ways to compel action. Such mechanisms would likely include the authority to write and rewrite agency information security budgets, access to agency enterprise architecture, access to the intelligence and law enforcement information necessary to identify threat signatures, the authority to isolate compromised systems from the network or take them offline completely, and the authority to conduct operational evaluations of federal and private sector information infrastructure.

An agency given these strategic responsibilities and broad operational authorities over cybersecurity would necessarily be of considerable size. If it were assembled in the same way as the DHS – by, in most cases, joining disparate components of existing departments under a single umbrella – large chunks of the Department of Commerce, OMB, and the DHS would be uprooted and placed under the new agency. Assuming that national security systems remained within the purview of the intelligence community and the Department of Defense, it would still be necessary to develop mechanisms by which they could coordinate with the new agency. Such an agency would require a substantial budget.

Action on this scale in the current political environment is highly unlikely. Any attempt to create such an agency would be compared to the creation of the DHS, which seven years after the enactment of the Homeland Security Act is still struggling to operate effectively. As a consequence, there is a concern that the U.S. cybersecurity regime would remain rudderless and disorganized for years to come in the face of growing threats. As suggested by the response to the Snowe-Rockefeller bill, industry would be strongly opposed to any agency that would be empowered to regulate the private sector. Congress would also almost certainly balk at the high start-up costs involved in creating a new agency, especially in light of a ballooning federal deficit and difficult economic times. Those start-up costs might be lessened if, instead of creating a new agency, Congress gave an existing agency these authorities. However, any attempt to empower one agency would likely meet with fierce resistance because it would be seen as a power grab by other congressional authorizing committees with an interest in cybersecurity.

B. Coordinating Authority

At the other end of the scale is the creation of a smaller entity with very limited authority that leaves the current regime largely intact. The

reorganization of the U.S. Intelligence Community following the terrorist attacks of September 11, 2001, may prove instructive, as this too required Congress to decide how best to coordinate the activities of disparate agencies with a variety of missions. The Program Manager for the Information Sharing Environment (PM-ISE) was created as part of this effort and can serve as a model for a less draconian approach to cybersecurity governance.[53] Under this system, there would be little, if any, change in the division of authorities. Instead, the head of this office would be responsible for developing strategies, working to resolve disputes where individual authorities appear to clash, and establishing policies and procedures that will facilitate information sharing and coordination among agencies. The office would have no authority to impose its will on other agencies but would, like the PM-ISE, either seek to influence the issuance of executive orders, OMB memoranda, and other binding instruments, or to negotiate with and among agencies to encourage the implementation of cybersecurity policies. As with the PM-ISE, to the extent that the entity creates new programs and administrative structures, they can be handed off to agencies for full implementation and oversight.

This approach has the advantage of requiring a much smaller staff and infrastructure, substantially reducing the implementation costs. It also avoids the complexity issue because it does not require Congress to make decisions about who should get what authority to respond to what vulnerability, but instead requires only the establishment of a basic decision-making framework. This approach should also avoid congressional committee jurisdictional conflict as there will be no reorganization of the existing power structure.

However, while the relative ease with which this structure can be established may make it seem attractive, there is a distinct possibility that it would not be an effective means of securing the information infrastructure. While the PM-ISE has notched some successes (for example, the development of a nationwide protocol as part of the the Suspicious Activity Reporting Initiative that allows federal, state, and local authorities to easily report, share, and analyze terrorism-related suspicious activities reports), it continues to report difficulty in accomplishing its primary mission of facilitating information sharing among federal agencies, state, local, and tribal authorities, the private sector, and international partners. In particular, it has had limited success in breaking the entrenched agency barriers to information sharing. With no direct authority to compel agency action or adoption of policies, the PM-ISE has had little leverage. The director of a similar cybersecurity entity would likely encounter even greater obstacles, particularly as he or she attempts to reconcile the often competing imperatives of providing greater security and of promoting technological innovation. Without any authority to compel action, the

53. *See generally* Information Sharing Environment, http://www.ise.gov/.

director would be largely impotent and few, if any, of the problems that Congress seeks to address would be resolved.

CONCLUSION

In light of the limitations on Congress's ability to act that are described above, this article concludes that any congressional action will eventually fall toward the lower end of the authority spectrum. How far in that direction it will go, however, is largely dependent on any number of legislative "x-factors." Will consideration of comprehensive cybersecurity fall in the shadow of a significant cyber attack, pushing legislation closer to the direct authority model? Might consideration of such legislation come in the shadow of revelations of inappropriate monitoring of Internet communications by the federal government, fostering mistrust of the government and making it difficult to pass *any* cybersecurity bill that increases the government's role in information infrastructure security?

As with information technology itself, the circumstances surrounding cybersecurity legislation are changing so rapidly that an accurate prediction is difficult to make. The door remains open for cybersecurity policy to flow not down from the federal government but up from the information technology industry. If the industry were to develop and implement consensus standards that addressed most of the cyber vulnerabilities that have been identified, that might obviate the need for congressional action. Given the industry's copious expertise and resources, this may indeed be an ideal solution.