Foundational Questions Regarding the Federal Role in Cybersecurity

Gus P. Coldebella* & Brian M. White**

During the last two years of the Bush administration, the senior leadership at the U.S. Department of Homeland Security (DHS) spent substantial time and effort in first helping to craft, and then attempting to implement, Homeland Security Presidential Directive 23/National Security Presidential Directive 54 (HSPD 23/NSPD 54), *Cyber Security and Monitoring*.[1]

As veterans of these efforts – and witnesses to both its successes and its failures – we have arrived at the view that the Obama administration must confront and resolve two thorny issues before its cybersecurity program can be successful: (1) the problem of bureaucracy – that is, who is ultimately responsible to the President and the public for implementing the program effectively and lawfully; and (2) the question of acceptance – that is, what technical tools are the American people comfortable having the government deploy, and what level of government involvement and interaction with the private sector will the people allow. Simply stated, before the government-led cyber initiative can move forward, the Administration must answer two questions: "Who?" and "How much?"

To be sure, there is a laundry list of other issues. One must only glance at the Obama administration's Cyberspace Policy Review (the Review), which contains the Administration's initial thoughts for addressing threats in cyberspace,[2] or the document that has a legitimate claim to be considered the Review's precursor, the Center for Strategic and

---

* Former Acting General Counsel of the U.S. Department of Homeland Security from February 2007 to January 2009, and its Deputy General Counsel from October 2005 to February 2007.

** Former counselor to the Deputy Secretary of the U.S. Department of Homeland Security from October 2007 to January 2009.

1. Homeland Security Presidential Directive 23/National Security Presidential Directive 54 is not publicly available, but it is described in a recent White House release concerning the Comprehensive National Cyber Security Initiative (CNCI), *available at* http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative. HSPD 23/NSPD 54 was issued by President George W. Bush on January 8, 2008, and directed the federal government to begin a national coordinated effort to protect and defend cyberspace, called the CNCI. The CNCI included twelve specific tasks. Many of these tasks remain classified, but some are public, including: (i) reduce the number of trusted internet connections that federal agencies have to external networks; (ii) detect and prevent federal civilian network intrusions with certain sensors; (iii) create a framework of standards to govern supply-chain security, or how and where technology related to the nation's communications backbone is procured; (v) re-examine information sharing between the government and industry to recommend changes necessary to foster greater collaboration.

2. 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.

International Studies' *Securing Cyberspace for the 44th Presidency* (the CSIS report) to understand the number of staggeringly difficult questions associated with attribution of threat, supply-chain security, and sharing of information between the government and the private sector, among other questions.[3]

The questions that we pose are foundational. Without a frank discussion of the program's limits, including privacy safeguards, the public will be justifiably reluctant to support the program. Without deciding which federal agency will take the lead, the private sector will neither invest in new and necessary technologies nor engage with the government on sensitive issues of network security. Only with the foundation in place can additional questions – some of which are posed below – begin to be answered.

While this article is largely prospective, it bears noting that often overlooked in discussions about federal cybersecurity is the Bush administration's resolution of the legal and policy questions related to one of the most critical, and most thorny, issues: the defense of civilian federal networks. These questions included which agency would lead the effort to implement an intrusion detection system (IDS), where the IDS would be deployed, and what legal safeguards would have to be in place to ensure compliance with constitutional and statutory obligations.[4] Policy makers knew that the building of the system – requiring significant coordination between various agencies – would not occur if interrupted by continual debates about policy.

One unfortunate byproduct of the readdressing of these legal and policy issues[5] by the Obama administration – now for more than a year – is substantial delay in implementation of the IDS.[6] We fear that the Administration is falling into a familiar trap on the wider cybersecurity initiative: it is failing to resolve questions such as where and how much, and it is losing time and momentum in the process.

---

3. CENTER FOR STRATEGIC AND INT'L STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY 12-13 (2008), *available at* http://csis.org/files/media/csis/pubs/081208_securing cyberspace_44.pdf.

4. *See* Memorandum for Fred F. Fielding, Counsel to the President, from Steven G. Bradbury, Principal Deputy Assistant Attorney General, Office of Legal Counsel, *Re: Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System (EINSTEIN 2.0) To Protect Unclassified Computer Networks in the Executive Branch,* Jan. 9, 2009, http://www.justice.gov/olc/2009/e2-issues.pdf.

5. This reexamination included an out-of-the-ordinary written review of the Office of Legal Counsel's original opinion. *See* Memorandum Opinion for an Associate Deputy Attorney General, from David J. Barron, Acting Assistant Attorney General, *Legality of an Intrusion Detection System To Protect Unclassified Computer Networks in the Executive Branch,* August 14, 2009, http://www.justice.gov/olc/2009/legality-of-e2.pdf.

6. Ellen Nakashima, *Cybersecurity Plan To Involve NSA, Telecoms; DHS Officials Debating the Privacy Implications*, WASH. POST, July 3, 2009, at A1.

We argue that, contrary to the recommendation of the CSIS report, the locus of the federal government's cyber effort should continue to be DHS. The Secretary already has the authority to protect information shared by the private sector,[7] to lead a civilian response to a cyber attack,[8] to obtain intelligence and law enforcement information from other agencies,[9] to develop standards for cybersecurity across the eighteen critical infrastructure sectors,[10] and to shield sellers and purchasers of technology designed to ward off cyber-terrorism from certain types of liability.[11] If stricter government control is necessary (and we do not argue that it is), DHS has paradigms of regulatory authority that are more well-suited to cybersecurity than other departments' authorities. The DHS has oversight mechanisms already in place to ensure that it handles Americans' private information sensitively and is held accountable if it does not.

We further argue that greater transparency is essential to the program's acceptance by the public. Certain information, such as how the intelligence community identifies a cyber threat, cannot and should not be shared. But for example, the Administration should describe how lawful communications with federal agencies are examined for malicious code, as well as the controls and procedures in place for protecting private information that has nothing to do with any threat. The public has heard so many reports of bureaucrats improperly accessing private information – such as the unfortunate episode of State Department employees searching passport records[12] – that it is unlikely to sign off based on faith alone.

This is not an argument in support of the status quo. It is a call to resolve these issues wisely (and quickly) so the nation may address more difficult questions that await.

I. CYBERSECURITY: A BROAD TERM, A DISTRIBUTED FUNCTION

The same term that describes the effort to encourage individuals to devise passwords that are difficult to guess and to refrain from clicking on unverified links in phishing e-mails also comprehends the mobilization of a nation to guard against terrorists or foreign powers disabling or destroying

7. *See, e.g.*, 6 U.S.C. §§131-133 (2006). The Secretary may utilize the entire set of Protected Critical Infrastructure Information (PCII) authorities created by the Homeland Security Act and the implementing regulations.

8. *See* Homeland Security Presidential Directive 5, *Management of Domestic Incidents*, Feb. 23, 2003, *available at* http://www.fas.org/irp/offdocs/nspd/hspd-5.html.

9. *See, e.g.*, 6 U.S.C. §§121-122 (2006).

10. 6 U.S.C. §321m (2007).

11. 6 U.S.C. §§441-444 (2006). The authors are referencing the entire set of the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act) authorities and all subsequent regulations.

12. For a report of State Department employees accessing candidates' passport files without authorization, see www.msnbc.msn.com/id/23736254/.

critical infrastructure as part of a physical attack, and the prevention of intrusions into classified systems containing national security information. We must recognize that cybersecurity spans measures that are personal, corporate, federal, and international. It is necessarily a distributed function: one that is not solely a mission of government, the private sector, or individuals, but is a function shared among them.

And what threat is cybersecurity supposed to guard against? The threat of criminal activity, such as identity theft or stealing money from a bank account? Or espionage – extracting sensitive information from government agencies or from the private sector? Attacks on infrastructure through the Internet or through insider access to computers, and resilience in case an attack occurs? The answer to all these questions is, of course, yes. A cybersecurity policy must be concerned with criminality of all stripes, nation state and corporate espionage, and attack.[13]

II. DUELING INCENTIVES, AN IMPETUS FOR CHANGE

So why the fuss over cybersecurity? After all, each actor plays (and has incentives to play) its role well, more or less: individuals who don't want their bank accounts raided devise strong, unique passwords; companies that don't want information stolen or infrastructure destroyed install systems to prevent intrusions and develop policies to minimize insider threats; and the federal government continues to investigate cyber crime (through the FBI and the Secret Service), collect intelligence on bad actors (through the National Security Agency and other members of the intelligence community), if necessary, wage cyber war (through the Department of Defense), and talk to our international partners (through the State Department).

Here is what the fuss is about. The cybersecurity system is not working. Terabytes of information continue to flow out of federal systems and private companies. Critical infrastructure is still vulnerable to attack.[14] And one reason that cybersecurity is not working – even though everyone knows it would be easier to accomplish if key players shared information, best practices, and assistance – is that structural disincentives work to prevent the various actors from sharing information.

While the government has information about malicious code and the behavior of criminal networks gained through its intelligence and law enforcement functions, fears of botching investigations or compromising sources and methods make sharing with the private sector (or even with other government agencies) difficult. While investment banks, defense contractors, and other critical infrastructure owners have information about

13. Cybersecurity comprehends even more, including, for example, the effort to motivate young American students to pursue education and expertise in computer science.

14. *See, e.g*, Ellen Nakashima, *Large Worldwide Cyber Attack Is Uncovered*, WASH. POST, Feb. 18, 2010, at A03.

intrusions into their own systems and networks, they fear enforcement actions by regulators, suits by plaintiffs' lawyers, and criticism associated with public disclosure of security failures. Concerns such as these make these private entities reluctant to share information with the federal government. While federal agencies know that their networks should be protected in many of the same ways that private sector networks are, concerns – including the opposition of privacy advocates to technology that sniffs traffic in and out of government systems – have slowed progress.

III. WHAT THE FEDERAL GOVERNMENT SHOULD DO, AND WHY DHS IS THE PROPER AGENCY TO DO IT

In order to overcome these systemic obstacles, we believe that the federal government must take six actions: (1) coordinate its cyber functions and attain situational awareness of the cyber domain across all federal agencies, (2) shore up its own systems, (3) provide a "safe space" for collaboration with the private sector, (4) encourage development of private sector standards, (5) reduce liability, and (6) be transparent.[15]

These six steps are essential to getting our not just federal, but our national, cybersecurity effort out of the starting blocks. And, without any change in law or doctrine, DHS can perform each of these functions today. Here's a description of each of the tasks, and why it makes sense that DHS be the locus of each of them.

A. Coordinate Action and Attain Situational Awareness (or, "Get Its Own House in Order")

A central criticism of the federal government's approach prior to the 9/11 attacks was that information was "stove-piped." A wall separated law enforcement and intelligence, and agencies had no incentive to share information. The "dots" could not be connected because no one had access to all of them. The creation of DHS and the Office of the Director of National Intelligence, and a sea change in attitudes, have created an environment more conducive to sharing information useful to thwarting terrorism.[16]

No effective mechanism exists, however, to share information about cybersecurity across the federal government. As a result, the government is missing opportunities to connect the dots on a daily basis. The federal government should aggregate and share information in real time about cyber incidents – including network intrusions at various federal systems,

15. The DHS's transparency tools are discussed in Part IV of this article.

16. The failures that led up to the Umar Farouk Abdulmutallab's 2009 Christmas Day bombing attempt make clear that work remains to be done. *See, e.g.,* Charlie Savage, *Nigerian Man Is Indicted in Attempted Plane Attack*, N.Y. TIMES, Jan. 7, 2010, at A14.

intelligence gathered by the NSA and other members of the intelligence community, information in criminal investigation files from the FBI and the Secret Service, and information from the private sector. In that way, the government can form a picture of everything that is going on in the cyber domain. The National Cyber Security Center (NCSC) created as part of HSPD 23/NSPD 54[17] was designed to fill that role.

The NCSC was to leverage the authorities of and information within DHS, the members of the intelligence community, the Department of Defense, and the Department of Justice. It was also to provide situational awareness and a common picture of all cyber events and operational information in the possession of the federal government.

HSPD 23/NSPD 54 placed the NCSC in DHS for a number of reasons. Primarily, the DHS Secretary has the statutory right to access to all information, including intelligence, regarding threats of or vulnerability to terrorism in the possession of any agency of the federal government.[18] Sadly, the NCSC was plagued by funding issues as well as turf wars during the last few months of the Bush administration and the first few months of the Obama administration, and is moribund.[19] This must change.[20]

The ameliorative effects of DHS's creation stretch far beyond information sharing. In 2003, President Bush decided that federal agencies working separately would not be able to handle a 9/11-scale catastrophe as well as agencies working in concert, and wisely determined that the coordinator of that response should not be the President or the White House. In HSPD 5, *Management of Domestic Incidents*, the DHS Secretary became the principal federal official for domestic incident management.[21]

---

17. HSPD 23/NSPD 54*, supra* note 1.

18. *See, e.g.*, 6 U.S.C. §122(a)(1) (2006): "[T]he Secretary shall have such access as the Secretary considers necessary to all information, including reports, assessments, analyses, and unevaluated intelligence relating to threats of terrorism against the United States and to other areas of responsibility assigned by the Secretary, and to all information concerning infrastructure or other vulnerabilities of the United States to terrorism, whether or not such information has been analyzed, that may be collected, possessed, or prepared by any agency of the Federal Government."

19. The NCSC's first director, Rod Beckstrom, detailed the reasons for NCSC's slow start in his resignation letter, *available at* http://online.wsj.com/public/resources/documents/BeckstromResignation.pdf.

20. DHS's record for retaining cybersecurity leadership has not been good. A number of different individuals have served as the director of the National Cyber Security Division (NCSD). Yet while the leadership turnover holds DHS back, it is not a substantial reason to transition responsibility for this mission away from DHS; instead, it is a call for renewed focus on the hiring and the retention of skilled cyber experts government-wide. Many of the lessons learned in hiring intelligence analysts after September 11, 2001 could be applied to this problem.

21. HSPD 5, *supra* note 8, states:

> The Secretary of Homeland Security is the principal Federal official for domestic incident management. Pursuant to the Homeland Security Act of 2002, the Secretary is responsible for coordinating Federal operations within the United States to prepare for, respond to, and recover from terrorist attacks, major

This was no small pronouncement. Cabinet secretaries and cabinet departments were not used to having anyone or anything interposed between them and the President or the President's most senior policy advisers. In HSPD 5, President Bush said that during incidents of national significance, the DHS Secretary would have the responsibility and authority to coordinate the incident-related functions of each of the federal departments, making the DHS Secretary first among equals in domestic incident management. HSPD 5 brought into full maturity one of the promises of DHS's creation: that it was to coordinate (rather than command and control) federal assets to deal with all hazards that the nation faces.

In the six years since HSPD 5 was issued, federal policy and disaster-response doctrine have been built around this basic principle. In the context of domestic incident management, the question of leadership – that is, who is in charge of coordination of federal assets – has already been resolved by HSPD 5. In our opinion, it should not be changed for cyber incidents. In fact, it should be expanded. DHS should maintain the lead role in coordinating public and private cybersecurity response, as was contemplated in HSPD 23/NSPD 54.

B. Secure Federal Networks (or, "Get Its Own House in Order II")

Federal agencies with primary responsibility for cybersecurity-related missions do their jobs fairly well, but cybersecurity flows through everything the government does. The IRS accepts electronic tax returns. The Department of Health and Human Services keeps personally identifiable health records on Americans who receive Medicare and Medicaid benefits. And so on. Every agency has an Internet presence that is vulnerable to exploitation. Even so, the best most federal agencies have is a forensic system that tells the government about an intrusion long after it happened. That is not sufficient.

In order to protect the cyber aspects of every agency's work, the Obama administration must follow through on the "Einstein" initiative begun in the Bush administration.[22] Einstein is designed to monitor all traffic in and out

---

disasters, and other emergencies. The Secretary shall coordinate the Federal Government's resources utilized in response to or recovery from terrorist attacks, major disasters, or other emergencies if and when any one of the following four conditions applies: (1) a Federal department or agency acting under its own authority has requested the assistance of the Secretary; (2) the resources of State and local authorities are overwhelmed and Federal assistance has been requested by the appropriate State and local authorities; (3) more than one Federal department or agency has become substantially involved in responding to the incident; or (4) the Secretary has been directed to assume responsibility for managing the domestic incident by the President.

22. In March 2010, the Administration released details concerning the implementation of the latest version of the Einstein program, "Einstein 3." *See* http://fcw.com/articles/2010/03/19/einstein-3-test-intrusion-prevention-system.aspx.

of federal networks in real time, and – with the help of hardware and information provided by sources including the intelligence community – stop malicious traffic from making its way in and sensitive information from making its way out. The U.S. Computer Emergency Readiness Team (U.S. CERT), a component of the DHS's National Protection and Programs directorate, is leading the initiative to implement Einstein in all executive branch agencies.

C. Provide a Safe Space for Private Sector Collaboration

In many ways, the private sector is ahead of the public sector in cybersecurity. Large enterprises generally have real-time intrusion detection and prevention procedures and uniform anti-insider threat policies, for example. But, as mentioned above, the private sector is reluctant to share information with the government about its practices, and especially its security shortcomings, for fear of regulatory action, lawsuits, or bad press. The government's situational awareness of the cyber domain is incomplete without information about what is affecting the private sector's networks, yet significant disincentives hamper sharing of that information.

The most cyber-savvy nongovernmental entity, however, still lacks access to information gained from the activities of the United States in intelligence, law enforcement, and other areas. As one government official told *The Washington Post*, "That's the secret sauce. . . . It's the stuff they have that the private sector does not."[23] The security of our critical infrastructure – 85 percent of which is owned by members of the private sector – would be significantly enhanced by devising ways to allow the private sector to obtain the benefits of that information without compromising sources and methods of intelligence collection or successful prosecutions.

DHS has unique statutory authority to interact with the private sector on issues of critical infrastructure protection; another reason that the HSPD 23/NSPD 54 assigned the lead role to DHS. Section 211 of the Homeland Security Act, titled the Critical Infrastructure Information Act of 2002,[24] and the regulations that DHS promulgated under that statute, allow DHS to receive information from the private sector regarding the protection of critical infrastructure – including cyber vulnerability information – without exposing that information to Freedom of Information Act requests, snooping by competitors, or enforcement actions by other agencies. This removes a major disincentive to cooperation and joint action with the government, and it is an authority that is uniquely DHS's.

In addition, DHS has already established a structure for discussing critical infrastructure protection with the private sector. The Critical

23. Nakashima, *supra* note 6.

24. *See supra* note 7.

Infrastructure Protection Advisory Council (CIPAC) and its constituent parts, the eighteen Sector Coordinating Committees (SCCs) include owners and operators of critical infrastructure and their industry representatives.[25] DHS created the CIPAC and the SCCs with the intention that they be exempt from the reporting requirements of the Federal Advisory Committee Act, which means the discussions between them and DHS do not have to be publicly reported. This is another DHS authority that creates incentives to sharing.

Under the protection of PCII and through CIPAC, owners of critical infrastructure may share information with DHS about network intrusions without significant risk. Armed with that information, DHS may shore up government networks against the threat via Einstein, inquire whether other companies are facing similar intrusions through the relevant SCCs, and, if warranted, issue "sanitized" warnings (that is, without any company-identifying information) to private sector entities via U.S. CERT. No other federal agency currently has the ability to interact with the private sector in this fashion.

D. Encourage Development of Private Sector Standards and Reduce Liability

Both the Review and the CSIS report suggest that government regulation of private-sector cyber security could be necessary, and, at a minimum, regulation of cybersecurity at privately-owned critical infrastructure.[26] We disagree. For years, owners of critical infrastructure have had the incentive to develop cybersecurity measures that are suited to their businesses. A centrally planned, one-size-fits-all regulatory scheme would almost certainly eliminate useful, industry-developed security measures and replace them with an ill-fitting, nondynamic slate of requirements.

A better approach would be to encourage private owners of critical infrastructure to develop and adopt for themselves – with the help and special expertise of the federal government – standards for cyber preparedness. In the Act Implementing the Recommendations of the 9/11 Commission of 2007, P. L. No. 110-53, Congress gave DHS the authority to adopt private sector preparedness standards. DHS created the program via a *Federal Register* notice, named it PS-Prep, and described how it may be used: private sector groups develop and propose standards to DHS,

25. 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.

26. CYBERSPACE POLICY REVIEW, *supra* note 2; CSIS Report, *supra* note 3.

which can choose to adopt them. Once these standards are adopted, DHS can certify private sector entities' compliance with the standards.[27]

Liability is always a concern for private sector actors when they are considering the development or adoption of new technology. This is especially so with technology that is designed to guard against catastrophic loss, because if the technology fails the liability for manufacturing or deploying the technology could be astronomically high. Certainly, if an entity is certified as compliant with a standard adopted by the DHS Private Sector Preparedness Program, and that entity is subsequently sued, the entity can argue that it met the relevant standard of care because it had complied with a DHS standard.

But there is protection in the Homeland Security Act that can more directly tamp down outsized liability. Congress recognized that the private sector would be reluctant to manufacture, market, and adopt anti-terrorism technology without liability protection, and thus passed the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002, or SAFETY Act.[28] The SAFETY Act limits liability associated with a qualified anti-terrorism technology, or QATT, to a predetermined amount if the QATT fails during a terrorist attack. Companies that market cybersecurity technologies should seek the protection of the SAFETY Act. In addition, because the SAFETY Act limits liability only in terrorist attacks, Congress should consider expanding protection for other types of cyber risk.[29]

IV. MEET THE NEW BOSS, THE SAME AS THE OLD BOSS

Most of the authorities that the federal government needs in order to form a solid foundation for a national cybersecurity strategy are already in place at DHS. HSPD 23/NSPD 54 assigns the main role – coordination of all of the nation's cybersecurity assets in both federal and private sectors – to DHS. However, as is so often the case when a problem requires leadership, Washington has focused on rearranging the bureaucracy rather than addressing the fundamental issue. Ever since it was issued in 2007, critics of HSPD 23/NSPD 54 both within and outside of the government have argued that the function belongs elsewhere – in the intelligence community (mostly because of the NSA's expertise in high-tech network defense), at DoD, or at the White House.

---

27. *See* Voluntary Private Sector Accreditation and Certification Preparedness Program, 74 Fed. Reg. 57,186 (Nov. 4, 2009).

28. *See supra* note 11.

29. Some argue, as they did at the time of the SAFETY Act's passage, that liability is an important structural incentive to make actors – in this case, manufacturers of cybersecurity-related equipment – take responsibility for what their products do. We agree. However, *unlimited* or *unquantifiable* liability – the type that might arise in the context of a significant terrorist attack or cyber event – causes rational actors to refrain from entering a market altogether, depriving us of new and important ways to guard against threat.

These criticisms are ill-founded. As argued above, DHS has most of the tools to play the lead role today – with perhaps the exception of a stronger liability protection scheme for cyber technologies. No other entity, new or existing, would have the authority that DHS has now. Further delay – while another agency is given the authorities required to push forward – would result.

The intelligence community, especially the NSA, offers an unparalleled level of technical expertise, as well as access to the "special sauce" of intelligence about cyber threats. But the intelligence community operates, as it should, largely out of public view. DHS does not. Because of the DHS Secretary's unfettered access to intelligence, DHS can tap into this information while disclosing its activities to its oversight committees and engaging with Congress and the public on issues of privacy.

DoD has two very clear cyber missions. It protects its own top-level "mil" domain networks and prepares to engage in cyber warfare if necessary. Key parts of a national cyber strategy – such as engaging with the private sector owners of critical infrastructure and leading other agencies in response efforts – are not part of DoD's mission.

The lead agency must be a coordinator, and DHS was designed to coordinate action across the executive branch and with the private sector. Different departments will lead various aspects of the cybersecurity effort. DHS will engage with the private sector and shore up civilian federal networks; DOJ will continue to enforce the criminal laws; NSA and the other members of the intelligence community will gather information about threats; and DoD will secure its own networks and prepare for cyber warfare. This is not a call to remove functions from other agencies. DHS is the only agency that is equipped to coordinate all of this activity, as it does under HSPD 5.

And what of the calls for a new cyber "czar" at the White House? It is our opinion that we have already met the true cyber czar: the DHS Secretary. The conduct of the Obama administration over the past few months seems to confirm that it believes, as we do, that DHS is the lead agency, and the DHS Secretary is the coordinator of federal action in this area. One must only look back at the incredible volume of Secretary Napolitano's press releases, public appearances, webcasts, and other activities during National Cyber Security Month in October 2009 to see that a leader is already in place.

Executive branch lawyers often cringe when the White House is mentioned as the locus of something so intensely operational as coordinating a national cybersecurity program. Congress would have to authorize such a change and appropriate funds for the operation, and with that comes the potential for requests for testimony and documents, and potentially subpoenas: matters that cause separation-of-powers battles between the branches.

The appointment of Howard Schmidt to the National Security Council staff does not change this assessment.[30] The White House has a key role to play, and we believe that the structure of the President's policy coordination process should be modified – as it already has been, in part, through the appointment of Schmidt – to highlight cybersecurity's urgency and continuing importance. As recommended by the Review and the CSIS report, an NSC staffer should be assigned this portfolio, and should coordinate this issue on behalf of the National Security Adviser and the President.[31] Presumably, this is Schmidt's role. Also, however, Congress should make DHS a permanent member of the National Security Council. That would allow DHS to call meetings and present important cybersecurity policy initiatives to the President through the National Security Adviser and his staff, including Schmidt.

The White House's most crucial role is more ephemeral. It is the nature of bureaucracy to reject "lead agencies," and the battles over DHS's role under HSPD 5 were significant. Because of the working relationship between DHS and the White House in the Bush administration, and the importance the White House placed on supporting the nascent DHS, the administration was able to affirm and strengthen DHS's role as the principal federal official in events of national significance. A similar level of support will be necessary if DHS is to be successful as the lead agency in cybersecurity. Specifically, if other agencies dismiss DHS's leadership, or challenge its role, or refuse to share information through the NCSC, no lesser authority than the President or his chief of staff must provide a swift correction.

Only after the government has established the foundation that we have outlined can it, working together with the private sector, begin the more difficult tasks:

1. Guiding the private sector on technological developments necessary for the cyber program to succeed.
2. Considering, with the private sector, how best to secure the supply chain of cyber equipment.
3. Constructing, with the intelligence and law enforcement communities, an effective means of sharing actionable information with the private sector.
4. Hiring talented cyber personnel and encourage more American students to pursue careers in cybersecurity.

30. *See* Ellen Nakashima & Debbi Wilgoren, *Obama To Name Former Bush, Microsoft Official as Cyber-Czar*, WASH. POST, Dec. 22, 2009, at A04.

31. CYBERSPACE POLICY REVIEW, *supra* note 2; CSIS Report, *supra* note 3.

Our fear? That the momentum of the last two years of the Bush administration may have been lost. While programs invariably flag during presidential transitions, that is no longer an excuse. To regain the momentum, we urge the President to affirm that DHS will lead this important twenty-first century mission.