New Federal Initiatives Project

Federal Cybersecurity Programs

By

Adam R. Pearlman*

August 12, 2010

The Federalist Society
for Law and Public Policy Studies

The Federalist Society takes no position on particular legal or public policy initiatives. Any expressions of opinion are those of the author or authors. We hope this and other publications will help foster discussion and a further exchange regarding current important issues.

www.fed-soc.org

Federal Cybersecurity Programs

On March 2, 2010, the White House declassified a summary of the Comprehensive National Cybersecurity Initiative (CNCI).[1] Initially promulgated by President Bush in January 2008 in National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), CNCI lays the groundwork for overhauling, uniting, and coordinating efforts to protect our nation's cyber infrastructure.

The declassified summary briefly lays out a series of twelve initiatives that bring together the resources of federal law enforcement, intelligence, and defense communities, as well as state and local authorities and private-sector players, to fulfill three goals that serve to protect national security and economic interests. These goals include: enhancing government-wide situational awareness of present network vulnerabilities; improving counterintelligence capabilities to defend against cyber threats; and coordinating future research and development efforts to deter the constantly-evolving hostile and malicious activities of some cyberspace actors.

The twelve initiatives call for:

- Consolidation of the federal government's external access points via the Trusted Internet Connections (TIC) initiative, overseen jointly by the White House Office of Management and Budget and the Department of Homeland Security (DHS);
- Deploying the EINSTEIN 2.0 system to detect unauthorized access and malicious content on federal systems by analyzing network flow information, and reporting that activity to DHS' Computer Emergency Readiness Team (US-CERT) so it can share the necessary information with all potentially affected government and private entities;
- Development of the EINSTEIN 3.0 intrusion prevention system by DHS and the National Security Agency, which will automatically detect and respond to activity exhibiting threat-signatures using real-time analysis of full packets of data entering or leaving government networks, and immediately share that information with appropriate agencies. The initiative also calls for increasing national intelligence capabilities to determine foreign cyber threats and adapt threat-signatures as necessary;
- Prioritization and coordination of cyber research and development projects, including eliminating redundant projects and identifying research gaps;
- Empowering the National Cybersecurity Center (NCSC) with coordinating and integrating information from the six centers responsible for U.S. cyber activities, to provide greater situational awareness of malicious activities;
- Improving cyber counterintelligence capabilities through establishing or expanding educational and awareness programs, and workforce development, in accordance with the National Counterintelligence Strategy of the United States of America;
- Increasing the security of federal classified networks;
- Expanding cyber education programs;
- Partnering with the private sector to invest in "high-risk/high-payoff solutions to critical cybersecurity problems";
- Developing strategies to deter cyber attacks by "improving warning capabilities, articulating roles for private sector and international partners, and developing appropriate responses for both state and non-state actors";

- Finding ways to protect the domestic and globalized supply chain from malicious actors; and
- Determine the federal government's role in ensuring the protection of and information sharing with privately owned and operated Critical Infrastructure and Key Resources.

The CNCI summary was declassified by the White House's Cybersecurity Coordinator, Howard Schmidt. Mr. Schmidt's appointment as Special Assistant to the President and Cybersecurity Coordinator on December 22, 2009 filled a void left by Melissa Hathaway's departure in August after serving in an acting capacity as a senior director at the White House for only six months.[2]

Recognized as "one of the most challenging threats that we must face,"[3] concern over cybersecurity issues has continued to grow since CNCI was initially adopted. In addition to reported attacks against government systems,[4] attacks directed at corporate systems and private individuals are also occurring more often, on larger and more sophisticated scales, and with potent results. These include the mass-theft of Hotmail email account passwords[5] and China's hacking of Google programmers' *personal computers* (rather than the corporate networks) to steal source code.[6] Although none of these attacks have caused immediately grave results, it is acknowledged at the highest levels that the United States is particularly vulnerable to crippling cyber attacks.[7]

The above begs a basic definitional question: what *is* cybersecurity?[8] More accurately, how should the government determine who or what constitutes a legitimate national security or economic threat against which our networks must be protected? The answer seems crucial to determine which authorities are appropriate to exercise in any given threat and response scenario (e.g. email phishing vs. denial of service attacks), and ever more important in an age that has seen the dismantling of the wall between intelligence and law enforcement operations, and the disappearance of battle lines that has come with the increasing prevalence of asymmetric warfare.

The cybersecurity threat includes actions by "[s]pies, hired cyber mercenaries, and criminal syndicates worming their way into government networks" in a way that requires both law enforcement and intelligence agency capabilities, which the FBI is trying to maximize via its National Cyber Investigative Joint Task Force.[9] Sophisticated criminal groups can now wage attacks nearly as complex and damaging as those of powerful states like China and Russia.[10] It is becoming increasingly clear that "[w]hether the perpetrator is a terrorist organization or a state actor, the threat to our energy, financial, communications, and security infrastructures remains the same."[11] And just as the intelligence community has an important role to play in protecting against those threats,[12] law enforcement agencies seek to leverage their own tools, and gain new powers to ensure success.[13]

Acknowledgement of our critical vulnerability, however, has not slowed the constant evolution of cyberspace and information technology, which in turn further complicates the myriad of legal and policy issues that coexist with our efforts to secure cyberspace. Funding requests for the CNCI initiatives constituted "the single largest request and most important initiative of the President's fiscal year 2009 budget request," and the House Permanent Select Committee on Intelligence conducted three hearings on the Initiative in 2008 alone.[14] Separately, in 2009 the

Federal Communications Commission (FCC) began developing a nationwide broadband plan to bring 100 megabit-per-second transfer rate capabilities to 100 million American homes in the next ten years, along with free public WiFi access.[15] Attempts to achieve greater cybersecurity for our nation have also been occurring alongside an acceleration of global internet governance. The Internet Corporation for Assigned Names and Numbers (ICANN),[16] the California-based organization that has had de facto control over the Internet's architecture for years and which is currently headed by Rod Beckstrom, the former head of the Department of Homeland Security's National Cybersecurity Center, recently severed agreements with the United States government which had cemented America's preeminence in the network's organization, and now plans for greater involvement of foreign governments and international entities in how the Internet develops.[17]

The President's Cyberspace Policy Review defines "cybersecurity policy" as including:

> strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.

This inclusive definition, and the operational necessities of coordinating efforts across many agencies, strengthening public-private partnerships, and building robust relationships with other nations, presents a plethora of structural and substantive issues: constitutional, statutory, regulatory, contractual, and jurisdictional.[18] Debate is robust and dynamic even over who will lead the effort: the White House promotes keeping cyber leadership within its ranks,[19] while Senate Homeland Security and Governmental Affairs Committee ranking member Susan Collins has called for a Senate-confirmed position housed in the Department of Homeland Security.[20] The proposed National Cybersecurity Advisor Act, S.778, offers a compromise by creating a Senate-confirmed National Cybersecurity Advisor within the Executive Office of the President.

The White House, however, seems unlikely to accept a Senate-confirmed appointee within the Executive Office of the President. Meanwhile, there have been delegation challenges within executive departments, as well, perhaps best highlighted by the uncertainties over the past four years relating to the leadership of a long-proposed Department of Defense cyber command, which the Air Force announced in 2006,[21] halted in 2008,[22] and reinstated on a reduced scale in 2009[23] before finally being established as a sub-unified command under U.S. Strategic Command.[24] General Keith Alexander, director of the National Security Agency (NSA) was recently promoted and confirmed by the Senate to head the new command, which is scheduled to become fully operational in October,[25] while the rules, policies, and multitude of operational issues concerning the potential and conduct of cyber warfare are being worked out by the Department of Defense.[26]

The multitude of substantive legal issues, of course, are even more complex and will likely remain subject to a wide array of arguments for many years to come. Chief among these are issues related to monitoring of internet communications: Americans' privacy,[27] and governmental control.[28] Recently declassified Department of Justice Office of Legal Counsel opinions from both the Bush and Obama Administrations regarding the EINSTEIN 2 system conclude that EINSTEIN 2's passive sensing for specific threat signatures on government systems satisfy the requirements of the Fourth Amendment, and applicable statutes.[29] Any opinions regarding EINSTEIN 3's development and capabilities, if they exist, are still classified. However, as a threshold matter, it is likely that OLC either has or will determine that NSA's role in the system's development does not violate the Posse Comitatus Act;[30] in response to a sufficiently similar interagency operation, a 1998 OLC opinion determined that it did not violate the act to detail a Department of Defense employee to serve as deputy chief of the FBI's National Infrastructure Protection Center.[31]

Concerns relating to the federal government's control of the internet are perhaps best highlighted by provisions of the Cybersecurity Act of 2009, S. 773, which give the president the ability "to initiate . . . network contingency plans to ensure key federal or private services did not go offline during a cyberattack of unprecedented scope."[32] The same bill has also included various versions of a "kill-switch" authority over the internet to protect critical infrastructure and government systems in the wake of a cyber attack.[33] And with the FCC pushing its authority to regulate commercial and consumer broadband service,[34] along with the internationalization of ICANN, there is sure to remain a minefield of political, policy, and legal issues as the federal government attempts to unify its cybersecurity standards and operations.

* *Adam R. Pearlman is a member of the International & National Security Law Practice Group Executive Committee and a graduate of the George Washington University Law School. The views expressed in this article are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.*

[1] The full summary is available at http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

[2] Siobhan Gorman, "Security Cyber Czar Steps Down," The Wall Street Journal, Aug. 4, 2009, available at http://online.wsj.com/article/SB124932480886002237.html (last visited Oct. 2, 2009).

[3] See "DHS Under Secretary Discusses Terrorism and the Cyber Realm," Tech Law Journal Daily E-Mail Alert, May 6, 2008, available at www.techlawjournal.com/alert/2008/05/06.asp (quotation attributed to former DHS Under Secretary for Intelligence and Analysis Charles Allen); Securing Cyberspace in the 44th Presidency, study by the Center for Strategic International Studies, at 11 ("America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration.").

[4] *See, e.g.*, Remarks by the National Counterintelligence Executive Dr. Joel F. Brenner, 4th Annual Multi-INT Conference, Institute for Defense and Government Advancement, February 24, 2009, available at http://www.dni.gov/speeches/20090224_speech.pdf (last visited July 29, 2010) ("[In 2008,] there were 5,499 tracked incidents of unauthorized access to US government computers and installations of malicious software. This is against 3,928 such incidents in 2007 and 2,172 in 2006.").

[5] See "Hackers Expose Slew of Hotmail Account Passwords," Breitbart.com, Oct. 5, 2009, available at

http://www.breitbart.com/article.php?id=CNG.78eddf1f537d8956756a2a2b646264db.ba1&show_article=1 ; Kate Loveys and Graham Smith, "Hotmail Security Breach Spreads as 30,000 Gmail and Yahoo! Passwords are Posted Online," MailOnline, Oct. 7, 2009, available at http://www.dailymail.co.uk/news/article-1218272/Microsoft-Hotmail-accounts-hacked-posted-online.html

[6] See Jim Finkle, "Google China Hackers Stole Source Code," Reuters, March 3, 2010, available at http://www.reuters.com/article/idUSN0325873820100303 (last visited May 17, 2010).

[7] See, e.g. President's Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, The White House, at i ("The architecture of the Nation's digital infrastructure . . . is not secure or resilient."); Testimony of Dennis Blair, Director of National Intelligence, Annual Threat Assessment Hearing, House Permanent Select Committee on Intelligence, February 3, 2010 (also reported at "Intel Chief: U.S. at Risk of Crippling Cyber Attack," FoxNews.com, Feb. 4, 2010 – available at http://www.foxnews.com/politics/2010/02/03/intel-chief-risk-crippling-cyber-attack/)

[8] See, e.g. Jill R. Aitoro, Cybersecurity, Oct. 1, 2008, available at http://www.nextgov.com/the_basics/tb_20090601_8569.php?oref=basics. Indeed, even "cyberspace" itself has been defined several different ways. See, e.g. Christopher J. Castelli, "Defense Department Adopts New Definition of 'Cyberspace'," Inside the Air Force, May 23, 2008 (describing a May 12, 2008 Deputy Secretary of Defense directive which defined the term as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."). DOD continues to use that definition. See, e.g. Statement of Lt. Gen. Keith Alexander before the House Armed Services Committee's Terrorism, Unconventional Threats, and Capabilities Subcommittee, May 5, 2009, available at http://www.nsa.gov/public_info/speeches_testimonies/5may09_dir.shtml.

[9] See The Cyber Threat: Using Intelligence to Predict and Prevent, March 4, 2010, http://www.fbi.gov/page2/mar10/cyberintel030410.html (last visited March 7, 2010) (summary of Director Mueller's remarks of March 4, 2010 at the annual RSA computer security conference in San Francisco).

[10] See Ellen Nakashima, "More Than 75,000 Computer Systems Hacked in One of Largest Cyber Attacks, Security Firm Says," Washington Post, pg A03, Feb. 18, 2010, available at http://www.washingtonpost.com/wp-dyn/content/article/2010/02/17/AR2010021705816_pf.html

[11] Opening Statement of Chairman Reyes, Annual Threat Assessment Hearing, Feb. 3, 2010, available at http://intelligence.house.gov/Media/PDFS/CSRSFR020310.pdf; K.A. Taiple, Power on the Edge: New Threats, New Responses, 1 Global Strategic Assessment 2009 61, National Defense University.

[12] *Id.*

[13] See, e.g. Declan McCullagh, "Police Want Backdoor to Web Users' Private Data," CNet, Feb. 3, 2010, available at http://news.cnet.com/8301-13578_3-10446503-38.html

[14] See Report accompanying H.R. 5959, the proposed Intel Authorization Request for FY 2009, at 33-34, available at http://intelligence.house.gov/Media/PDFS/IAAFY09.pdf

[15] See Grant Gross, "FCC's Nationwide Broadband Plan: What's in it?," PC World, March 12, 2010, available at http://www.pcworld.com/businesscenter/article/191438/fccs_national_broadband_plan_whats_in_it.html

[16] http://www.icann.org/ (last visited Oct. 2, 2009)

[17] Bobbie Johnson, "U.S. Relinquishes Control of the Internet," The Guardian http://www.guardian.co.uk/technology/2009/sep/30/icann-agreement-us (last visited Oct. 2, 2009) ; the text of the new agreement can be found here: http://www.icann.org/en/announcements/announcement-30sep09-en.htm#affirmation

[18] See John Rollins and Anna Henning, Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations, CRS Report R40427, March 10, 2009; Report accompanying H.R. 5959, the proposed Intel Authorization Request for FY 2009.

[19] See President's Cyberspace Policy Review at pgs. iii, v.

[20] Chris Strohm, CongressDaily, "Collins Details Plan for Cybersecurity Director," Nov. 2, 2009, available at http://www.nextgov.com/nextgov/ng_20091102_1184.php

[21] See Staff Sgt. C. Todd Lopez, "8th Air Force to Become New Cyber Command," Air Force Print News, November 3, 2006, available at http://www.af.mil/news/story.asp?storyID=123030505

[22] See Michael Hoffman, "Final word: One Nuclear, But No Cyber Command," Air Force Times, Oct. 8, 2008, available at http://www.airforcetimes.com/news/2008/10/airforce_corona_decision_100708w/

[23] See David Axe, "Air Force Establishes 'Reduced' Cyber-War Command," Wired.com, Aug. 18, 2009, available at http://www.wired.com/dangerroom/2009/08/air-force-establishes-new-reduced-cyber-war-command/

[24] See Memorandum by Secretary of Defense Robert Gates re Establish of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations, available at http://www.govexec.com/nextgov/0609/gates_cybercommand_memo.pdf

[25] See Ellen Nakashima, "Gen. Keith Alexander Confirmed to Head Cyber-Command," Wash. Post, May 11, 2010, available at http://www.washingtonpost.com/wp-dyn/content/article/2010/05/10/AR2010051005251.html?wprss=rss_business.

[26] Pentagon Says Military Response to Cyber Attack Possible, BreitBart.com, May 12, 2010, available at http://www.breitbart.com/article.php?id=CNG.7c80ff42024d3ea21b818758f7a7eb3a.bf1&show_article=1

[27] See Jaikumar Vijayan, "Feds Downplay Privacy Fears on Plan to Expand Monitoring of Government Networks," Computerworld.com, Feb. 28, 2009, available at http://www.computerworld.com/s/article/9065698/Feds_downplay_privacy_fears_on_plan_to_expand_monitoring_of_government_networks?taxonomyId=145&taxonomyName=security_hardware_and_software

[28] Declan McCullagh, "Bill Would Give President Emergency Control of Internet," C-Net News, Aug. 28, 2009, available at http://news.cnet.com/8301-13578_3-10320096-38.html

[29] See Op. Off. Legal Counsel, "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, available at http://www.justice.gov/olc/2009/e2-issues.pdf; Op. Off. Legal Counsel, "Legality of Intrusion-Detection System to Protect Unclassified Computer Networks in the Executive Branch," Aug. 14, 2009, available at http://www.justice.gov/olc/2009/legality-of-e2.pdf.

[30] 18 U.S.C. § 1385.

[31] Op. Off. Legal Counsel, "Effect of Posse Comitatus Act on Proposed Detail of Civilian Employee to the National Infrastructure Protection Center," May 26, 1998, available at http://www.justice.gov/olc/pca1fnl.htm. Although the DOD/FBI agreement involved a detailed civilian employee, as opposed to the NSA's likely use of both civilian and military assets in assisting DHS develop EINSTEIN 3, OLC is likely ultimately to come to the same conclusion here, i.e. that DOD's (and therefore NSA's) role in protecting the nation's cybersecurity infrastructure is lawful. Three key factors make this the likely conclusion: 1) EINSTEIN 3 is being designed primarily as an intelligence, rather than a law enforcement tool; 2) a central, if not the foremost concern, regarding cyberthreats against which EINSTEIN 3 will guard are ones that originate overseas; and 3) to the extent that law enforcement action may be taken at a later date if the source of a threat is successfully tracked, it is foreseeable that apprehension of the suspect(s) will be handled by the appropriate law enforcement agency, with only intelligence support coming from military personnel. Incidentally, it is not only DHS that is taking advantage of the NSA's expertise in this area. Private sector companies, too, are seeking the NSA's help in protecting their networks. See "Google, NSA to Team Up in Cyberattack Probe," Reuters.com, Feb. 4, 2010, available at http://www.reuters.com/article/idUSTRE6130M120100204?type=technologyNews?feedType=RSS&feedName=technologyNews&rpc=22&sp=true

[32] See Tony Romm, "Cybersecurity Bill to Give President New Emergency Powers," The Hill, Feb. 26, 2010, available at http://thehill.com/blogs/hillicon-valley/technology/83961-forthcoming-cybersecurity-bill-to-give-president-new-powers-in-cyberattack-emergencies. A summary of the latest incarnation of S. 773 is available at http://commerce.senate.gov/public/index.cfm?p=Legislation&ContentRecord_id=f2256d47-85a9-4c64-b9e0-40ab01564735&ContentType_id=03ab50f5-55cd-4934-a074-d6928b9dd24c&Group_id=6eaa2a03-6e69-4e43-8597-bb12f4f5aede.

[33] See, e.g. "Should Obama Have an Internet Kill Switch?," Fox News.com, Sept. 28. 2009, www.foxnews.com/printer_friendly_story/0,3566,556362,00.html

[34] See Grant Gross, "FCC Chairman Defends Broadband Regulation Move," FoxBusiness.com, May 6, 2010, available at http://www.foxbusiness.com/story/personal-finance/lifestyle-money/personal-technology/fcc-chairman-defends-broadband-regulation/

Related Links

The White House's cybersecurity page
http://www.whitehouse.gov/cybersecurity

"Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency" by The Center for Strategic and International Studies, December 2008
http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

"Bill would give DHS emergency cyber powers,"Federal News Radio, June 3, 2010
http://www.federalnewsradio.com/?nid=15&sid=1971691