ARNOLD & PORTER LLP

ADVISORY

June 2009

THE NEW WHITE HOUSE "CYBER CZAR"

On Friday, May 29, 2009, President Obama created a new White House office devoted to the security of the nation's digital infrastructure, "the networks and computers we depend on every day."[1] The new office will be led by a Cybersecurity Coordinator (already referred to as the nation's "Cyber Czar") and is tasked with "orchestrating and integrating all cybersecurity policies for the government; working closely with the Office of Management and Budget to ensure agency budgets reflect those priorities; and, in the event of a major cyber incident or attack, coordinating our response." Simultaneously with his announcement, the President also released a "Cyberspace Policy Review" report of a 60-day "top-to-bottom" review of the federal government's cybersecurity efforts conducted by the National Security Council and Homeland Security Council.[2]

Emphasizing his Administration's commitment to cybersecurity (which he described as "a strategic national asset"), the President announced that he would personally select the new Cybersecurity Coordinator, and advised that the Cyber Czar would have regular access to the Oval Office.

The President has not yet announced who will serve as the new Cybersecurity Coordinator, and only time will tell the full impact of the new Cybersecurity office. That said, the Administration's efforts in the cybersecurity arena likely will generate both great opportunities and significant challenges for private companies. Among other things:

- Companies may face increased law enforcement activity in the cyber arena, which may enhance their efforts to tackle cyber- and intellectual property crimes, and, at the same time, may lead to increased burdens in the form of disruptive internal investigations or an increase in the number and scope of subpoenas.
- Companies will have to address how policy developments in the cybersecurity area affect their exposure in civil litigation or enforcement actions.
- The new attention to cybersecurity promises to provide opportunities for government contractors, as well as potential litigation risk in the event of security breaches.
- The new focus on cybersecurity may lead to increased scrutiny of foreign acquirers of US companies by the Committee on Foreign Investment in the United States (CFIUS) under Section 721 of the Defense Production Act of 1950.

1 The President's announcement of the new Cybersecurity Coordinator's office may be found at http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.

2 "Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure." The report is available at http://www.whitehouse.gov/asset.aspx?AssetId=1732.

Brussels
+32 (0)2 290 7800

Denver
+1 303.863.1000

London
+44 (0)20 7786 6100

Los Angeles
+1 213.243.4000

New York
+1 212.715.1000

Northern Virginia
+1 703.720.7000

San Francisco
+1 415.356.3000

Washington, DC
+1 202.942.5000

Market Volatility and the Changing Regulatory Landscape

For more information and access to Arnold & Porter's latest resources on this topic including client advisories, upcoming events, publications, and the Market Volatility & the Changing Regulatory Landscape Chart, which aggregates information on US government programs, please visit: http://www.arnoldporter.com/marketvolatility.

arnoldporter.com

On a positive note, the Administration has expressed a desire to partner with private actors in formulating cybersecurity policy. We believe this openness presents opportunities for private actors to help shape policy to best balance the often competing needs of ensuring the security of information and facilitating commerce.

Arnold & Porter LLP will continue to monitor developments closely, and will prepare additional advisories as the situation develops.

THE THREAT JUSTIFYING THE CREATION OF THE CYBERSECURITY OFFICE

In explaining the Administration's new approach to cybersecurity, the Cyberspace Policy Review cites "a growing array of state and non-state actors [who] are compromising, stealing, changing, or destroying information and could cause critical disruptions to US systems."[3] The President further explained:

> [E]very day we see waves of cyber thieves trolling for sensitive information—the disgruntled employee on the inside, the lone hacker a thousand miles away, organized crime, the industrial spy and, increasingly, foreign intelligence services. In one brazen act last year, thieves used stolen credit card information to steal millions of dollars from 130 ATM machines in 49 cities around the world—and they did it in just 30 minutes. A single employee of an American company was convicted of stealing intellectual property reportedly worth $400 million. It's been estimated that last year alone cyber criminals stole intellectual property from businesses worldwide worth up to $1 trillion.

The President also explained that he personally had been affected by a cyber attack, detailing how, during the recent general election campaign, hackers had managed to penetrate his campaign's computer systems.

The Administration believes that the nation's historical approach to cybersecurity was inadequate to address the ever-increasing threat. First, the "Federal government is not organized to address" the risks to the nation's digital infrastructure.[4] As the President observed, "when it comes to cybersecurity, federal agencies have overlapping missions and don't coordinate or communicate nearly as well as they should—with each other or with the private sector." The President pointed to the "disorganized response to" the recent Conficker worm as evidence of the shortcomings of the present system.

Second, the Cyberspace Policy Review describes the current legal landscape as a complex mixture of constitutional, domestic, foreign, and international law "enacted to govern what were very diverse industries and technologies."[5] The Administration hopes that a coherent executive policy "may prompt proposals for a new legislative framework to rationalize the patchwork of overlapping laws that apply to information, telecommunications, networks, and technologies, or the application of new interpretations of existing laws in ways to meet technological evolution and policy goals."

Third, the scope of the cybersecurity problem "transcends the jurisdictional purview of individual departments and agencies,"[6] or even the capacity of the federal government, all of which argues for the need to coordinate with private, state, local, tribal, and international actors to comprehensively secure America's information infrastructure.

THE CYBERSECURITY COORDINATOR'S RESPONSIBILITIES

The new Cyber Czar will be situated in the White House and will serve as a member both of the National Security Staff and of the National Economic Council. In his remarks, President Obama outlined five main areas of focus that the Administration will address in the cybersecurity area:

- **Securing Information and Communications Networks:** The Cybersecurity Coordinator is tasked with developing a "comprehensive strategy to secure America's information and communications networks." The President made plain that the process of developing the strategy will be "open and transparent," and that its progress will be measured

3 Cyberspace Policy Review at iii.

4 Cyberspace Policy Review at i.

5 Cyberspace Policy Review at 10.

6 Cyberspace Policy Review at iv.

by "[c]lear milestones and performance metrics." The Cyberspace Policy Review further advocates that "state, local and tribal governments" also "should consider the need to elevate cybersecurity as an issue" by designating point-persons to coordinate on cybersecurity issues.[7]

- **Responding To Cyber Attacks:** The Cyber Czar will work with "key players, including state and local governments and the private sector" to develop both effective defenses and coherent responses to future cybersecurity breaches. The President emphasized that, "[j]ust as we do for natural disasters, we have to have plans and resources in place beforehand—sharing information, issuing warnings and ensuring a coordinated response."
- **Fostering Public/Private Partnership:** The Cybersecurity Office will work to strengthen the cooperation between the public and private sectors in securing the nation's digital infrastructure. The President emphasized that his "administration will not dictate security standards for private companies. On the contrary, we will collaborate with industry to find technology solutions that ensure our security and promote prosperity."
- **Research And Development:** The President envisions increased investment in the development of the nation's digital infrastructure and other technological innovations. He mentioned a number of specific policy initiatives, including expanding America's broadband infrastructure, developing a smart electrical grid, developing next-generation air traffic control systems, and implementing electronic medical records.
- **Cybersecurity Education And Awareness:** The President announced that he would commence a national campaign to promote greater "cybersecurity awareness and digital literacy" among the public, and to develop an educational system that will train a technologically adept modern workforce.

POLICY CONSIDERATIONS

The President sought to reassure constituents that any new cyber policies will be developed with a careful eye on their potential impact on economic actors, national security concerns, individual civil liberties, government transparency, and the public's participation in government. He emphasized that numerous stakeholders were consulted during the 60-day review he had directed. The Cyberspace Policy Review detailed considerable debate about how to achieve a secure national digital infrastructure without stifling innovation and commerce.[8] The President's comments and the Policy Review make clear that the White House aspires for the new office to develop its policies in conjunction with government, industry, and individual stakeholders.

The President also stated that his Administration's cybersecurity policy will not include "monitoring private sector networks or Internet traffic." He reiterated his commitment to the policy of net neutrality, stating that the Internet should remain "open and free."

NEAR AND LONG-TERM PROSPECTS

The President is expected to name a new Cybersecurity Coordinator in the next several weeks. Whoever is appointed will face some formidable challenges, especially in light of the numerous federal and state agencies and private entities involved in the world of cyber security, the breadth of the new office's portfolio, and the disparate policy goals this office will serve. To bolster the authority of the new position,[9] the President stated that the new Cyber Czar "will have my full support and regular access to me as we confront these challenges." The Cyber Czar's effective powers will be substantially augmented by his or her involvement in the budgetary process: the President explained that the new Cybersecurity office will be charged with "working closely with the Office of Management and Budget to ensure agency budgets reflect" the Administration's cybersecurity policies. What remains to be seen, however, is whether the new Cybersecurity Coordinator will have greater success in overcoming inherent agency territoriality and bureaucratic inertia than other so-called "czar" positions have had in the past.

7 Cyberspace Policy Review at 11.

8 *See* Cyberspace Policy Review at 31-35.

9 Some commentators have expressed concern that the Cybersecurity Coordinator will not be sufficiently powerful to promote the President's agenda. *See* "Security Experts React to Obama's Cybersecurity Report," WSJ.com (May 29, 2009).

OPPORTUNITIES AND RISKS

We believe that the Administration's new approach offers significant opportunities for actors in the private sector, but also offers some potentially significant pitfalls. Some of these opportunities and risks include:

- **Increased Law Enforcement Coordination and Activity:** The new Cybersecurity office and the Administration's attention to cyber issues may well increase the ability of law enforcement to tackle cyber- and intellectual property crimes, especially if the Administration's effort is accompanied by increased or better coordinated funding. Enhanced law enforcement activity will present new opportunities for our clients to work with the authorities to prevent, combat and address the effects of cybercrime. It also may present challenges as companies shoulder the burdens of additional law enforcement activity, which may include a ramp-up in the frequency of disruptive internal investigations, or an increase in the number and burden of subpoenas.
- **The Role of Civil Liability:** The Cyberspace Policy Review on several occasions discusses the role of civil liability as a mechanism for adjusting private sector incentives relating to electronic data security. The Review states: "The Federal government should consider options for incentivizing collective action and enhance competition in the development of cybersecurity solutions. For example, the legal concepts for 'standard of care' to date do not exist in cyberspace. Possible incentives include adjustments to liability considerations (reduced liability in exchange for improved security or increased liability for the consequences of poor security), indemnification, tax incentives, and new regulatory requirements and compliance mechanisms."[10]
- **Intellectual Property:** New cybersecurity policy should present companies with additional opportunities for safeguarding intellectual property and proprietary information and, as noted, may well lead to additional law enforcement attention to intellectual property concerns. It also raises the possibility that authorities will focus more on allegations of industrial espionage—an area that the President expressly singled out in his address. This may well have the effect of drawing law enforcement to an area that more commonly has been handled in the civil arena.[11]
- **Technology and Education Providers:** The technological and educational aspects of the administration's cybersecurity initiative no doubt will offer significant business opportunities for private corporations, including companies that provide technological solutions and services.[12] However, as with any complex and novel area of government contracting, these new opportunities may be accompanied with increased litigation risk. Such risks seem especially daunting in the area of cybersecurity, where hackers historically have proven themselves adept at defeating security measures, often shortly after a new security measure is introduced. It is also likely that government contractors may find their cybersecurity measures subject to increased scrutiny by the government.
- **CFIUS:** Cybersecurity has taken on special significance in the context of reviews of foreign acquisitions of US companies by CFIUS under Section 721 of the Defense Production Act of 1950. Under new CFIUS regulations, a potential foreign acquirer of a US company must now certify as to what cybersecurity protections will be in place with respect to the US company. US government contractors, and in particular any US company engaged in work for an intelligence agency, will be under particularly close scrutiny. It is possible that CFIUS could hold up an acquisition until satisfactory cybersecurity measures are in place, and the President's new initiative may set standards for, and even increase further, CFIUS's considerations in this regard.
- **Participation In Formulating Cybersecurity Policy:** The Administration's transparent approach presents

10 *See* Cyberspace Policy Review at 28.

11 The Economic Espionage Act of 1996 (the EEA), which primarily provides for criminal prosecution of industrial espionage, was passed in large part because existing federal and state remedies, primarily civil, were judged inadequate. *See* S. Rep. No. 104-359, at 11-12 (1996). However, since its passage, relatively few criminal prosecutions hav`e been brought under the EEA. *See* Susan W. Brenner & Anthony C. Crescenzi, "State Sponsored Crime: The Futility of the Economic Espionage Act," 28 Hous. J. Int'l L. 389, 432 (2006) (34 cases as of 2006). *See also* http://www.usdoj.gov/criminal/cybercrime/ipcases.html#eea (listing EEA cases brought by the US Department of Justice).

12 *See* Christopher Drew & John Markoff, "Contractors Vie for Plum Work, Hacking for US," *New York Times* (May 31, 2009)

opportunities for our clients to participate in developing industry-friendly cybersecurity policies and standards. The private sector consistently struggles between the often competing needs of ensuring the security of information and facilitating commerce. Any national policy that will not overly burden commerce must remain cognizant of these tradeoffs. Moreover, the Cybersecurity office will be well-positioned to assure that US domestic practices are coordinated with international standards and practices, which will help foster American competitiveness abroad.

We will be closely monitoring any developments in this area, including public comments, and will prepare additional advisories as new information is provided. We hope that you have found this advisory useful. If you have additional questions, please contact your Arnold & Porter attorney or:

Marcus A. Asner
+1 212.715.1789
Marcus.Asner@aporter.com

Ronald D. Lee
+1 202.942.5380
Ronald.Lee@aporter.com

John B. Bellinger III
+1 202.942.6599
John.Bellinger@aporter.com

Jeffrey H. Smith
+1 202.942.5115
Jeffrey.Smith@aporter.com

Ronald L. Johnston
+1 213.243.4256
Ronald.Johnston@aporter.com

Nancy L. Perkins
+1 202.942.5065
Nancy.Perkins@aporter.com

Beth S. DeSimone
+1 202.942.5445
Beth.DeSimone@aporter.com

Mark A. Kleyna
+1 212.715.1344
Mark.Kleyna@aporter.com

Nicholas L. Townsend
+1 202.942.5249
Nicholas.Townsend@aporter.com