Federal Government Cybersecurity Progress:

Obama Administration Report Card 2009-Present

Jim Ed Crouch, NSCI
Larry K. McKee, Jr., NSCI
Gen (Ret) Ron Keys, RK Solution Enterprises
January 18, 2011

In a May 2009 address from the East Room of the White House, President Obama announced the release of a 60-day Cyberspace Policy Review resulting from the president's direction to the National Security and Homeland Security Councils to "conduct a top-to-bottom review of the federal government's efforts to defend our information and communications infrastructure and to recommend the best way to ensure that these networks are able to secure our networks as well as our prosperity."

As usual, the President delivered a great speech, beginning with, "We meet today at a transformational moment – a moment in history when our interconnected world presents us, at once, with great promise but also great peril." He went on to say, "In short, America's economic prosperity in the 21st century will depend on cybersecurity," while describing the cyber threat as "one of the most serious economic and national security challenges we face as a nation." [1]

These were some very welcome words, primarily because they emanated from the White House, about Cyber, during a period in which the President was dealing with the financial crisis and the wars in Iraq and Afghanistan, along with making good on his campaign pledge to reform the health care insurance industry. If you've never read the speech in its entirety, we encourage you to do so; it is an excellent read. You can find it on the White House website here.

With the Obama administration approaching its two-year anniversary, we thought it might be helpful to examine its record of accomplishments in cybersecurity. What follows is an "Obama Administration Report Card," whereby we have awarded grades for progress against a number of the recommendations contained in the 60-Day Review, or "Hathaway Report" as it is commonly called. The Hathaway Report contained recommendations broken down into two categories of action plans, designated as Near-Term and Mid-Term, with neither plan being defined in terms of timing or projected dates of completion – perhaps its most glaring shortfall. Now that the administration is over halfway through their elected term, we believe enough time has passed to make it entirely reasonable to expect complete or near-complete implementation of action items described as "near-term." We've therefore evaluated the administration's progress against the ten recommendations contained in the Near-Term Action Plan while withholding judgment for now on the additional 14 recommendations in the Mid-Term Action Plan.

In assigning grades, we have established the following criteria:

- A – Item was fully implemented and is considered by the larger cyber community as an improvement over previous practices or fills a previous void; now requires only routine maintenance
- B – Item was significantly implemented and represents an improvement, but still requires some additional action to achieve fully-implemented status
- C – Item was implemented but has received mixed or negative reviews from the larger cyber community; or implementation has proven to have gaps or flaws in application.
- D – Item still in work; or item's implementation was delayed to the point that it suggests a lack of leadership or decisiveness in assigning priorities, or compounding delay in other areas.
- F – No progress shown against the item or item has received universal criticism for having no value to enhancing cybersecurity

Although we acknowledge the degree of difficulty involved in achieving a "A" grade, we also should note how hard it would be to score an "F." Only a complete disregard of the recommendation would have resulted in a failing grade. We awarded grades solely on our view of actual progress – not on good intentions, flowery rhetoric, the number of meetings held, commissions commissioned, or number of times administration officials have mentioned the word "cyber."

[1] "REMARKS BY THE PRESIDENT ON SECURING OUR NATION'S CYBER INFRASTRUCTURE," Press Release from the Office of the White House Press Secretary, 29 May 2009 available at http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/

Federal Government Cybersecurity Progress:
Obama Administration Report Card 2009-Present

Jim Ed Crouch, NSCI
Larry K. McKee, Jr., NSCI
Gen (Ret) Ron Keys, RK Solution Enterprises
January 18, 2011

Below are the ten Hathaway Report Near-Term recommendations with our grades and an explanation for each. Following the graded portion of this report card, we also offer some observations and recommendations on a few other areas.

1. Appoint a cybersecurity policy official responsible for coordinating the Nation's cybersecurity policies and activities.

Grade: D. (for timing) Although the President ultimately appointed Howard Schmidt to the cybersecurity coordinator position, he spent until December 2009 to reach his decision. The process was delayed by a number of internal squabbles over authorities, responsibilities, and chain of command, with several potential candidates declining the job because of concerns over insufficient authority to execute required responsibilities. Melissa Hathaway, who chaired the 60-Day review and was considered by many to be the odds-on favorite to win the coordinator's position, resigned from her cyber position on the National Security Council after waiting three months for the president to make a decision.[2] The president's lack of leadership and decisiveness were likely responsible for the resulting delays in getting started on the focused effort required for a problem he himself had described as "one of the most serious economic and national security challenges we face as a nation." We believe Mr. Schmidt has all the experience and qualifications necessary for the job. We also believe he made an excellent choice in June 2010 when he named Sameer Bholatra to serve as his deputy. However, it is our belief that the concerns expressed by many over the authority-versus-responsibility issue were valid in 2009 and remain valid today.[3]

2. Prepare for the President's approval an updated national strategy to secure the information and communications infrastructure.

Grade: D. Our research shows no such strategy document as having been released, although the WhiteHouse.gov website suggests it is in work. The White House plan calls for this document to be an updated version of the Comprehensive National Cybersecurity Initiative (CNCI) launched by the Bush administration in January 2008. Although we give the President credit for continuing to use the CNCI, we share his stated belief that the "CNCI and its associated activities should evolve to become key elements of a broader, updated national U.S. cybersecurity strategy."[4] The time for such a document to be delivered is past due.

3. Designate cybersecurity as one of the President's key management priorities and establish performance metrics.

Grade: B. Through the efforts of a task force consisting of representatives from the Federal CIO Council, Council of Inspectors General on Integrity and Efficiency, National Institute of Standards and Health, Homeland Security, Department of Defense, Director of National Intelligence, Government Accountability Office, and the Information Security and Privacy Advisory Board, performance metrics for measuring the cybersecurity effectiveness of federal agencies have been available since the end of 2009. However, until recently they were considered by many to be an expensive waste of time. As described by federal CIO Vivek Kundra in a recent conference call with reporters, "These reports ended up being more secure in the cabinets they were living in than were the systems they were meant to protect."[5] The White House recently announced an update to the Federal Information Security Management Act (FISMA) that shifts the focus from paper-based compliance reports to

---

[2] "Obama to name Howard Schmidt as cybersecurity coordinator," Story by Ellen Nakashima in the Washington Post, 22 Dec 2009 available at http://www.washingtonpost.com/wp-dyn/content/article/2009/12/21/AR2009122103055.html
[3] For example, see http://www.computerworld.com/s/article/9142445/White_House_cyber_czar_and_other_security_non_events_of_2009 .
[4] Introduction to Comprehensive National Cybesecurity Initiative (CNCI); http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative
[5] "White House Updates Cybersecurity Orders," article by J. Nicolas Hoover in Information Week, 21 Apr 2010 available at http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=224500173

Jim Ed Crouch, NSCI
Larry K. McKee, Jr., NSCI
Gen (Ret) Ron Keys, RK Solution Enterprises

continuous, real time monitoring of Federal networks. Performance metrics are risk-based, which we believe is a viable approach. The change in approach provides for faster identification and response to vulnerabilities. The administration believes the new approach builds on best practices from both government and industry, thus making our cybersecurity efforts more effective. Although work remains to be done, we view these changes as steps in the right direction. We are further hopeful that the Obama administration will continue to collaborate with the private sector on additional improvements in this area and produce useful metrics that actually can be tracked and compared across the federal networks and actually used to make decisions based on facts, not anecdotal information.

4. Designate a privacy and civil liberties official to the NSC cybersecurity directorate.

Grade: C. A July 2010 posting on the WhiteHouse.gov website says that a privacy and civil liberties official has been assigned to the National Security Staff. Although the individual was unnamed – perhaps because of privacy and civil liberties concerns – we're willing to trust the administration's claims that such a person exists. However, we're unable to go so far as to assign any grade above a "C" since it seems the anonymous official's activities and accomplishments remain as stealthy as his or her name.

5. Conduct interagency-cleared legal analyses of priority cybersecurity-related issues identified during the policy-development process and formulate coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the Federal government.

Grade: B. In a July 2010 progress report[6] issued by the White House, this item was skipped entirely, implying an administration reluctance to claim substantive progress in this area. We're nevertheless willing to award extra credit for several accomplishments we believe to be noteworthy. First, there's the standup of U.S. Cyber Command, which will at least centralize roles and responsibilities within DoD. We're further encouraged by the Memorandum of Understanding recently signed by DoD and DHS. The memorandum's stated purpose is to improve cybersecurity collaboration regarding strategic planning, capabilities development, and mission activities through personnel exchanges and easier access for DHS to DoD-owned resources. There's also an agreement reached last year that clarifies responsibilities and purview of cyber coordinator Schmidt, the Office of Management and Budget, and DHS. Finally, the Nuclear Regulatory Commission (NRC) and the Federal Energy Regulatory Commission (FERC) will cooperate to ensure cybersecurity for nuclear power plants. Their agreement lays out the basic principles and guidelines for how the commissions will work together to ensure the reliability of the electric power grid and nuclear power plants. According to the agreement, areas for cooperation include cybersecurity and information sharing during emergency responses. Although it remains to be seen whether these agreements will fulfill their goals, there is potential for increased cooperation among the different federal government signatories to these memoranda.

6. Initiate a national awareness and education campaign to promote cybersecurity.

Grade: B. We applaud the administration's efforts to not only increase public awareness, but also in implementing programs to recruit and train cyberspace professionals. The National Initiative for Cybersecurity Education (NICE) program, consisting of four tracks – Awareness, Education, Federal Workforce Structure, and Training and Professional Development – has spread from government and high-tech industry to colleges, high schools, and libraries throughout the country. As NICE has expanded its scope, a number of similar private industry-sponsored programs have also been implemented – something for which we should grant partial credit to the federal government. There

[6] "Cybersecurity Progress after President Obama's Address," Release from the National Security Council, 14 July 2010,available at http://www.whitehouse.gov/administration/eop/nsc/cybersecurity/progressreports/july2010

Jim Ed Crouch, NSCI
Larry K. McKee, Jr., NSCI
Gen (Ret) Ron Keys, RK Solution Enterprises

are now a number of programs that either fall under the overarching NICE initiative or were inspired by it. These programs are aimed at recruitment, training, and retention of cyber professionals, while also increasing cybersecurity awareness in the workplace. All of these efforts are laudatory, and the administration deserves ample credit for continuing the NICE program despite the fact that it was invented during the Bush administration. The "B" grade is based on our opinion that our public awareness efforts thus far have been primarily targeted toward the workplace. These efforts now need to be expanded, through public service announcements and other methods, to reach casual users of the internet. Too many of these people remain unaware of the threats – spyware, malware, viruses, and others – not only to their own computers, but also to the larger networks on which those computers and mobile devices reside. One such initiative that might serve as an example for the administration to follow is the Safe and Secure Online program, launched in 2006 by the International Information Systems Security Certification Consortium (ISC)[2]. This program reaches down to the middle school level to educate students on ways to protect themselves against identity theft, cyber bullying, and threats associated with social networking.

7. Develop an international cybersecurity policy framework and strengthen our international partnerships.

Grade: B. We give the Obama administration a "B" for continuing the dialogue for international agreements while not surrendering all of the technological advantages and capabilities we currently enjoy. One accomplishment of note was an arrangement involving the U.S. Secret Service teaming with the European Electronic Crime Task Force to bolster defenses against computer attacks on embassies and other government sites. It will also monitor computer networks for threats and deal with attacks once they happen. Also included in the arrangement is the use of software, designed by the national postal system of Italy, which monitors computer networks and combs through money transfers for signs of criminal activities.

We do not, however, see much progress towards establishing agreement on “normative” behavior on the net… what is plausible deniability versus what is good enough for high quality attribution; what is a “witting or unwitting” host’s responsibility; what is the agreed definition of Personally Identifiable Information versus Non-PII? We refer you to the following excerpt from a white paper we wrote last year. It explains our position on the international issue – an opinion we believe is fundamentally shared by our national leadership, but is lacking in progress.

"... a case can be made for continued work toward international standards, especially in the area of cybercrime. Nations should cooperate on identification, arrest, and prosecution of cybercriminals. It may not be easy to reach consensus on everything that constitutes a cyber crime, but there should be common agreement on the most obvious. For example, some of the U.S.'s closest allies have placed restrictions on so-called "hate speech" – something that most Americans would consider a violation of the First Amendment. But there's no reason why the U.S. and others shouldn't be able to reach agreement on some activities – theft of financial resources or intellectual property and trafficking in child pornography, for example – that constitute criminal activity. Rather than rejecting all international agreements outright, the U.S. and international partners should be able to find common ground on these and other issues while continuing to work at resolving the larger differences – the "one bite at a time" way to eat the elephant.

Other areas for international cooperation include education, training, and information sharing. It seems nearly everyone in the international cyber community recognizes that increased situational awareness is critical to getting in front of cyber actors with aggressive intent. The U.S. should encourage sharing vulnerability discoveries and defenses against new malware and viruses. In addition, the U.S. should encourage providing assistance to other countries in determining attribution following a cyberspace criminal activity.

Jim Ed Crouch, NSCI
Larry K. McKee, Jr., NSCI
Gen (Ret) Ron Keys, RK Solution Enterprises

In short, the U.S. should be collaborating with other nations with the intent of achieving agreement on defining common cyberspace terms and on what constitutes normative behavior regarding such areas as nation-state liability and accountability for cyber criminal activity.

Increased mutual understanding regarding international views of cyberspace will help to better define ideas such as "use of force" and "armed attack" in the context of cyberspace. Both formal and informal relationships between the U.S. and other nations should be encouraged, in both the public and private sectors. U.S. leadership with the international cyber community will help to build the confidence and trust necessary to enhance transparency and cooperation.

Although we do not advocate for a full-speed-ahead approach to signing international agreements, we remain strongly in favor of individual nations doing everything possible – bilateral agreements with like-minded countries, and other actions on the low-hanging fruit from the endless list of recommendations produced from the multiple studies conducted over the past few years – to defend their sovereign rights, manage risks, and ultimately protect personal freedoms, financial prosperity, and national security in cyberspace." [7]

8. Prepare a cybersecurity incident response plan and initiate a dialog to enhance public-private partnerships.

Grade: C. In September 2010 The Department of Homeland Security released an interim version of a National Cyber Incident Response Plan, a mere 16 months after President Obama's declaration of cybersecurity as a top administration priority. That's hardly a fast-track agenda. As for progress in public-private partnerships, we concur with the following excerpt from an opinion piece by William Jackson, published in Federal Computer Week: "After years of lip service, information is being shared, but not on a scale or with a speed that is necessary to meet the demands of cyberspace. The private sector complains that government is unwilling to share intelligence with industry, and industry is unwilling to share with government because of concerns about liability and the possible exposure of proprietary information As a result, we are still waiting for a real public-private partnership." [8] As one industry CEO remarked, "…when we do pass information to U.S. CERT on an emerging threat, the room often fills with lawyers asking us, 'Where did you get that?!'" In a mid-September speech to an Interpol audience in Hong Kong, Melissa Hathaway expressed her belief that although the U.S. has engaged in multiple public-private partnerships, they've been largely ineffective, primarily because of a lack of government focus.[9]

Emblematic of this lack of trust are the concerns, shared by many private cybersecurity firms, that government-imposed standards can have a detrimental effect on innovation. "The government needs to be very careful about imposing too much of a top-down standards process," said McAfee's vice-president of government relations, Tom Gann. "We need to bring products to market very quickly. They need to make sure we can get latest technology." As reported by HomelandSecurityNewswire.com, Gann believes "...information technology standards developed by private industry are often more effective because they apply internationally and adapt to technological changes more rapidly than government institutions."[10]

---

[7] "International Cyberspace Considerations," Gen (Ret.) Ron Keys and Jim Ed Crouch, 17 May 2010, available at http://nsci-va.org/WhitePapers/2010-05-17-International%20Cyber%20Paper-Keys-Crouch-final.pdf
[8] "Public-private effort on cybersecurity needs a push from Congress," article by William Jackson in Federal Computer Week, 2 August 2010, available at http://fcw.com/articles/2010/08/02/cybereye-cybersecurity-public-private-partnerships.aspx
[9] "Melissa Hathaway: America Has Too Many Ineffective Private-Public Partnerships," story in The New New Internet, October 2010 available at http://www.thenewnewinternet.com/2010/10/12/melissa-hathaway-america-has-too-many-ineffective-private-public-partnerships/
[10] "Industry concerned about DHS standards on cybersecurity," article in Homeland Security Newswire, 23 June 2010, available at http://homelandsecuritynewswire.com/industry-concerned-about-dhs-standards-cybersecurity

Jim Ed Crouch, NSCI
Larry K. McKee, Jr., NSCI
Gen (Ret) Ron Keys, RK Solution Enterprises

On a positive note, DHS's appointment last March of a former Microsoft Corporation executive to lead a key division may prove instrumental in improving the relations between the government and private sectors. While overseeing the protection of government networks, Phil Reitinger will also be responsible for coordinating outreach programs to private companies that own and operate the nation's most vital information assets. These digital assets power everything from water and electricity distribution systems to telecommunications and transportation networks. As reported in the *Washington Post*, Reitinger brings to the job a wealth of cyberspace experience in both public and private sector jobs.[11]

There was also a report last July that the President had convened a meeting with private industry executives and members of his Cabinet to discuss possible financial incentives to companies for partnering with the government in cybersecurity. As reported on the Nextgov website, the goal was to "...encourage companies to support broad cybersecurity initiatives that relied on partnerships with federal agencies and the deployment of safeguards to ensure their private computer networks and systems were adequately protected."[12] Although the meeting failed to produce any tangible results, the fact that such a meeting took place is encouraging.

9. Develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure.

Grade: C. The Department of Energy has devised a program that allows for Cyber Security defense systems to communicate when attacked and transmit that information to cyber systems at other institutions. This is a good example of the use of technology to perform tasks that heretofore have been accomplished by humans. According to the DOE's Michael Skwarek, "The Federated Model for Cyber Security acts as a virtual neighborhood watch program. If one institution is attacked, secure and timely communication to others in the Federation will aid in protecting them from that same attack through active response."[13]

This success story notwithstanding, the Government Accountability Office (GAO) is less than impressed. The GAO released a report last year saying the White House Office of Science and Technology Policy (OSTP) had failed to live up to its responsibility to coordinate a national cybersecurity R&D agenda. As reported in Computer World, there are five federal agencies involved with funding and executing the government's cybersecurity R&D work. Several private sector companies also carry out either federally-funded or self-funded cybersecurity R&D projects for the government. Over the years, there have been numerous calls for more centralized oversight and coordination of these various R&D efforts to ensure that the projects are meeting a focused national cybersecurity agenda. The GAO report urged the OSTP to show more leadership in pulling together a focused and prioritized short, medium- and long-term R&D strategy for cybersecurity.[14]

In December 2010, the administration announced "... a Memorandum of Understanding signed by the National Institute of Standards and Technology (NIST) of the Department of Commerce, the Science and Technology Directorate of the Department of Homeland Security (DHS/S&T), and the Financial Services Sector Coordinating Council (FSSCC). The goal of the agreement is to speed the commercialization of cybersecurity research innovations that support our Nation's critical

[11] "Microsoft Executive Tapped For Top DHS Cyber Post," Brian Krebs reporting in the *Washington Post*, 11 March 2009, available at http://voices.washingtonpost.com/44/2009/03/11/microsoft_executive_tapped_for.html
[12] "White House, executives discuss economic incentives for cybersecurity," Jill Aitoro, NextGove.com, 15 July 2010, available at http://www.nextgov.com/nextgov/ng_20100715_4890.php
[13] "National Defense Network Created to Fight Cyber Attacks" by Brock Cooper, *The Cutting Edge*; 24 August 2009, available at http://www.thecuttingedgenews.com/index.php?article=11513
[14] "GAO slams White House for failing to lead on cybersecurity," Jaikumar Vijayan, *ComputerWorld*, 8 July 2010, available at http://www.computerworld.com/s/article/9178959/GAO_slams_White_House_for_failing_to_lead_on_cybersecurity?taxonomyId=82&pageNumber=1

Jim Ed Crouch, NSCI
Larry K. McKee, Jr., NSCI
Gen (Ret) Ron Keys, RK Solution Enterprises

infrastructures. The agreement establishes a framework for collaboration between the public and private sectors as directed by President Obama in his cybersecurity policy address." [15] We believe more work to establish trust between the public and private sectors remains to be done and that by doing so, we can reap further benefits in the R&D arena. However, without a clear set of priorities on what part of the game needs to be changed, or to bring about what sort of improved effects, there is the real danger of falling into the technology trap of "more is good," "faster is better," and ending up with one more flashlight or flatulence application for smartphones.

10. Build a cybersecurity-based identity management vision and strategy, leveraging privacy-enhancing technologies for the Nation.

Grade: C. In June 2010, Cybersecurity Coordinator Howard Schmidt announced release of The National Strategy for Trusted Identities in Cyberspace, " ...a blueprint to reduce cybersecurity vulnerabilities and improve online privacy protections through the use of trusted digital identities." [16] According to a 6 January 2011 announcement from the National Institute of Standards and Technology (NIST), the strategy is currently being reviewed by the agencies responsible for implementation and is expected to be finalized and ready for the President's signature within a few months.

Also in early January was an announcement that the Commerce Department would be assuming overall authority for an internet ID for Americans. Cybersecurity Coordinator Howard Schmidt has described this move as "the absolute perfect spot in the U.S. government" to centralize efforts toward creating an 'identity ecosystem'."[17] The decision to assign this responsibility to Commerce – rather than NSA or DHS – is likely to be met with approval from civil liberties and privacy groups.

Our "C" grade is based on the amount of time it's taken to get the strategy to its current status.

Other Observations: Although we've graded only the ten areas above, we would be remiss to ignore other cyber-related accomplishments by the administration. Credit is due for implementing, expanding, or influencing other nationwide initiatives to enhance cybersecurity, not only within the federal sector but also within the private sector and academia. The Einstein intrusion detection system, first fielded on a voluntary basis in the mid-2000s, has been expanded and is projected to be deployed by 21 federal agencies within the next year. In an effort to get all of us on the same sheet of music, the Joint Staff in 2010 published a "Joint Terminology for Cyber Operations" document, which will provide "...a starting point for normalizing terms in all cyber-related documents, instructions, CONOPS, and publications..."[18] We also believe events such as DHS's CyberStorm and the Bipartisan Policy Center-sponsored Cyber Shockwave are excellent venues for increasing cybersecurity capabilities and awareness. However, as we continue to expand on these and other exercise and experimentation activities, we need to ensure there is a system in place to capture and disseminate lessons learned and best practices. There's also an important role to be played in these exercises at the state and local levels. The administration should give serious consideration to providing funding for such participation.

During the course of our research, we discovered a number of cyber-related news items that aren't relevant to the grading criteria we used in preparing this report, but are interesting to note, nonetheless. Most of these items are demonstrative of the administration's intent, but it is too early to determine whether any positive results will be achieved if and when they are further pursued. Rather than adding them to this section of the report, we've elected to attach an appendix as an optional reading item.

---

[15] "Partnership for Cybersecurity Innovation," Aneesh Chopra and Howard A. Schmidt, announcement from the Office of Science and Technology Policy, 6 December 2010, available at http://www.whitehouse.gov/blog/2010/12/06/partnership-cybersecurity-innovation?utm_source=related

[16] "The National Strategy for Trusted Identities in Cyberspace," Howard A. Schmidt post on The White House Blog, 25 June 2010, available at http://www.whitehouse.gov/blog/2010/06/25/national-strategy-trusted-identities-cyberspace?utm_source=related

[17] "Obama to hand Commerce Dept. authority over cybersecurity ID," Declan McCullagh, *CNET,* 7 January 2010

[18] Memorandum of transmittal, "Joint Terminology for Cyber Operations," signed by General James E. Cartwright, USMC, Vice-Chairman, Joint Chiefs of Staff (undated)

Federal Government Cybersecurity Progress:

Obama Administration Report Card 2009-Present

Jim Ed Crouch, NSCI
Larry K. McKee, Jr., NSCI
Gen (Ret) Ron Keys, RK Solution Enterprises
January 18, 2011

Summary: We've awarded decidedly mixed grades to President Obama at the halfway point of his term. It appears we're making progress in cybersecurity on those issues that can be resolved through technological means or by development of agreed-to standards of compliance and performance worked at the mid-management level. However, the keys to sustained progress lie in deciding at the policy level what we want to achieve…with an implementable set of actions containing agreed-to definitions and a prioritized list for action. Included should be decisions on net neutrality, public-private partnerships, , personally identifiable information standards, personal-private-public responsibility standards, legal liability standards, some standard of net resiliency and recoverability, agreements on what is cyber war, cyber crime, cyber "hacktivism" and what do we do about it…and more. From there focus can be brought to the technical needs to actually implement policy, and the regulations/laws needed to support execution. We're encouraged by the Obama administration's continuation of actions recommended by the CNCI. Specifically, better connectivity among cyber operations centers, increased network security, improvements in information sharing, and enhanced focus on the cyber supply chain are all demonstrations of a solid understanding of the problem. We believe Howard Schmidt is highly qualified to serve as the Cyber Coordinator and is doing a commendable job in spite of the lack of clarity that exists with his role. Further, the DoD standup of Cyber Command, the consolidation of all DHS cyber responsibilities under one directorate, and the Secret Service and FBI's stepped-up approach to pursuing cyber criminals are reasons for optimism. However, for those areas that require top-level direction and leadership, people skills, tough decision making, and someone to serve as a referee for competing priorities among the various government agencies and departments – in short, the President – there's a significant drop-off. We hope this is not the result of Mr. Obama's lack of any real interest in the subject.

Roles, responsibilities, and legal authorities across the various agencies are critical components of cybersecurity. They are also difficult and complicated issues. Top-down leadership is required to ensure "lanes in the road" are clear to all players. Without it, we'll experience a continuation of the intramural squabbles that characterized the President's Cyber Coordinator selection process. Thus far, it appears the President gave a great pep talk before the team took the field, but hasn't had much to offer in terms of in-game coaching. The degree of effectiveness of our interagency cooperation and collaboration will ultimately determine our ability to deter or respond to cyber incidents and attacks.

Jim Ed Crouch, NSCI
Larry K. McKee, Jr., NSCI
Gen (Ret) Ron Keys, RK Solution Enterprises
January 18, 2011

Appendix A - Additional Work in Progress

In conducting our research, we found a number of items that we couldn't really use in the evaluation of the administration's progress against the ten near-term recommendations in the Hathaway Report, but were interesting enough to include as general information for our readers. We offer them here – in no particular order – to enhance your overall awareness and to demonstrate that the administration is making incremental progress in the area of cybersecurity. It is our hope that we will soon see positive results from the initiatives below.

One of the recommendations resulting from the Bush administration's Comprehensive National Cyber Initiative (CNCI) was the creation of a National Cyber Range (NCR), a testbed serving several purposes: assessing information assurance and survivability tools in a network environment; replicating complex, heterogeneous networks; enabling multiple, independent, simultaneous experiments on the same infrastructure; and applying the scientific method for rigorous cybertesting. Managed by the Defense Advanced Research Projects Agency (DARPA), the NCR is expected to reach an initial operating capability sometime in the spring of 2011.[19]

Partially in response to cyber attacks from China in 2009, the North American Electric Reliability Corporation has revised cyber security standards for the control systems of the U.S. electric power grid. The revision was part of a multi-stage process to develop "good housekeeping" requirements designed to provide a foundation of security practices that will secure critical infrastructure from cyber security threats. Entities found in violation of the standards can be subjected to stiff fines.

In an effort to better deal with the threat, DHS announced in 2009 a plan to more than double the size of its workforce in the National Cybersecurity Division, from 111 to 260 employees. The division analyzes and responds to computer attacks on the government and companies that provide critical services such as electricity and phone transmission. Although we're unable to confirm whether this increase actually took place, we applaud the intent.

OMB announced late last year a new strategy for acquisition of major IT systems. This resulted from a government-wide review that identified a need for government and industry to communicate and collaborate more effectively, as well as sharpen the governance and accountability processes for monitoring major IT acquisitions. Part of the review included an announced freeze on programs that were behind schedule or over budget.

In December, the State Department announced creation of a new cybersecurity coordinator position to aid in efforts to defend against theft of classified material.

The Obama administration recently released a "Privacy Bill of Rights" to protect consumers using the internet and providing guidelines for companies' handling of user data. Demonstrating a bit of ambiguity on the subject, the administration has also requested changes to existing laws that would make it easier for the FBI to acquire information on individuals' e-mail and browser activities. The request specifically asks that the FBI be granted authority to add "electronic communications transactional records" to the list of items investigators may demand from internet providers without prior approval by a judge. These records include e-mail dates and times, addresses of e-mail correspondents, and browser histories. Not included is the content of e-mail messages. Privacy rights advocates have predictably responded. As reported in the Washington Post, "...the move is another example of an administration retreating from campaign pledges to enhance civil liberties in relation to national security. The proposal is 'incredibly bold, given the amount of electronic data the government is already getting,' said Michelle Richardson, American Civil Liberties Union legislative counsel."[20]

---

[19] "Defense Researchers Developing National Cyber Test Range," story by Henry Kenyon in *Signal Connections,* 15 April 2009, available at http://www.afcea.org/signal/articles/templates/200904SIGNALConnections.asp?articleid=1919

[20] "White House proposal would ease FBI access to records of Internet activity" Ellen Nakashima, *The Washington Post*, 29 July 2010, available at http://www.washingtonpost.com/wdyn/content/article/2010/07/28/AR2010072806141.html

Jim Ed Crouch, NSCI
Larry K. McKee, Jr., NSCI
Gen (Ret) Ron Keys, RK Solution Enterprises
January 18, 2011

The administration is busy establishing security standards for cloud computing services and expects to finalize them for release within the next six months. The government hopes to ultimately transition to cloud computing in an effort to save on costs, space, and labor. However, issues regarding security must be resolved before cloud computing can be widely accepted.

In November, DHS announced the opening of a 24-hour watch-and-warning center dedicated to cyber-related activities. Known as the Multi-State Information Sharing and Analysis Center (MS-ISAC) Cyber Security Operations Center, the facility will provide enhance situational awareness at the state and local level for the National Cybersecurity and Communications Integration Center—the DHS-led integrated cyber-incident response hub—and allow the federal government to provide critical cyber risk, vulnerability, and mitigation data to state and local governments.[21]

Last fall, the White House announced standup of a subcommittee to deal with privacy and internet policy issues. The subcommittee, which is composed of representatives from more than a dozen departments, agencies, and federal offices, will work to develop principles and strategy that are consistent with legislative, regulatory, and international internet policies. The group is also charged with working with private stakeholders in promoting innovation and economic expansion, while also balancing the rights of individuals to privacy.

In an effort to better share information on real-world cyber attacks, the Homeland Security Department has implemented a program inviting comments from a variety of cyber stakeholders on forms redesigned to capture lessons learned from cyber incidents. The DHS program facilitates the dissemination of data regarding attacks targeted against entities representing industry, academia, and non-profits.

Last fall, the National Institute of Standards and Technology (NIST) issued its first Guidelines for Smart Grid Cyber Security. As reported by Space War, these include "high-level security requirements, a framework for assessing risks, an evaluation of privacy issues at personal residences, and additional information for businesses and organizations to use as they craft strategies to protect the modernizing power grid from attacks, malicious code, cascading errors and other threats.... The guidelines are the second major output of NIST-coordinated efforts to identify and develop standards needed to convert the nation's aging electric grid into an advanced, digital infrastructure with two-way capabilities for communicating information, controlling equipment, and distributing energy."[22]

[21] "DHS Opens New 24-Hour Cybersecurity Facility," The New New Internet, 19 November 2010, available at http://www.thenewnewinternet.com/2010/11/19/dhs-opens-new-24-hour-cybersecurity-facility/
[22] "NIST Finalizes Initial Set Of Smart Grid Cyber Security Guidelines," *Space War*, 16 September 2010