

## FACT SHEET: The Administration's Cybersecurity Accomplishments

*"From now on, our digital infrastructure – the networks and computers we depend on every day – will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority." – President Obama, May 29, 2009*

The Administration has made significant progress in cybersecurity, ensuring that Americans, our businesses, and our government are building better protections against cyber threats. Departments and agencies have implemented numerous programs to enhance their risk management with regard to their systems. They have also put processes in place to engage with their suppliers and their private-sector stakeholders. In addition to those activities, we have completed or will shortly complete all of the 10 near-term actions from the [Cyberspace Policy Review](#), and we continue to implement the [Comprehensive National Cybersecurity Initiative](#). At the same time, the Administration is taking significant steps to institutionalize the need for strong cybersecurity and to operationalize the policies that we have developed to better protect our Nation against cyber threats.

### Near-Term Actions from the Cyberspace Policy Review

1. Appoint a cybersecurity policy official responsible for coordinating the Nation's cybersecurity policies and activities; establish a strong NSC directorate, under the direction of the cybersecurity policy official dual-hatted to the NSC and the NEC, to coordinate interagency development of cybersecurity-related strategy and policy.
  - Complete. Howard A. Schmidt has been [appointed](#) as the Cybersecurity Coordinator.
2. Prepare for the President's approval an updated national strategy to secure the information and communications infrastructure. This strategy should include continued evaluation of CNCI activities and, where appropriate, build on its successes.
  - Complete. The direction and needs highlighted in the Cyberspace Policy Review and previous national cybersecurity strategy are still relevant, and we have updated that strategy on targeted cyber issues, such as identity management and international engagement.
3. Designate cybersecurity as one of the President's key management priorities and establish performance metrics.
  - Complete. All senior executives and senior leadership have been informed that cybersecurity is one of the President's [key management priorities](#) for the Federal Government. We have established metrics through the CyberStats program, and

we have also worked with the Office of Management and Budget (OMB) to update the [Federal Information Security Management Act \(FISMA\) metrics](#) by which departments and agencies are graded on their cybersecurity. Together, we are shifting the Federal Government's approach to cybersecurity from a static, paper-based certification and accreditation to a dynamic, relevant process based upon continuous monitoring and risk assessment.

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

- Complete. Our second Director for Privacy and Civil Liberties official joined us from the Federal Trade Commission in December 2010.

5. Convene appropriate interagency mechanisms to 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.

- Complete. We have developed a formal interagency process as we continue to address policy and legal issues. As part of that process, we identified additional authorities that the executive branch needs to fulfill its mission, and we have requested those authorities as part of our [legislative package](#).

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

- Complete. We have created the [National Initiative for Cybersecurity Education \(NICE\)](#) with the dual goals of a cyber-savvy citizenry and a cyber-capable workforce, including raising awareness for consumers, enhancing cybersecurity education, and improving the structure, preparation, and training of the cybersecurity workforce. After the 2010 National Cyber Security Awareness Month, DHS launched a year-round national awareness campaign, which has held events around the country.

7. Develop U.S. Government positions for an international cybersecurity policy framework and strengthen our international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity.

- Complete. We have finished and will soon release the International Strategy for Cyberspace, which provides a unified foundation for the nation's international engagement on cyberspace issues.

8. Prepare a cybersecurity incident response plan; initiate a dialog to enhance public-private partnerships with an eye toward streamlining, aligning, and providing resources to optimize their contribution and engagement.

- Complete. The National Cyber Incident Response Plan (NCIRP) was developed and tested during a national cyber exercise, [Cyber Storm III](#). It is now in the final stages of being updated, based upon our experience using the plan in different cyber exercises.

9. In collaboration with other EOP entities, 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; provide the research community access to event data to facilitate developing tools, testing theories, and identifying workable solutions.

- Complete. The White House Office of Science and Technology Policy has finalized a Cyber Research and Development Framework. Public release of the plan is expected to occur in May 2011.

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

- Complete. The [National Strategy for Trusted Identities in Cyberspace \(NSTIC\)](#) was released on April 15, 2011. The Department of Commerce will stand up a [program office](#) to coordinate the federal government and private sector in implementing this effort.