West Texas Cyber Security Consortium

Cyber Security

President Obama has declared that the “cyber threat is one of the most serious economic and national security challenges we face as a nation” and that “America's economic prosperity in the 21st century will depend on cybersecurity.” As a result, the President directed a top-to-bottom review of the Federal Government's efforts to defend our information and communications infrastructure, which resulted in a report titled the Cyberspace Policy Review. To implement the results of this review, the President has appointed Howard Schmidt to serve at the U.S. Cybersecurity Coordinator and created the Cybersecurity Office within the National Security Staff, which works closely with the Federal Chief Information Officer Steven VanRoekel, the Federal Chief Technology Officer Todd Park, and the National Economic Council.

President Obama has declared that the “cyber threat is one of the most serious economic and national security challenges we face as a nation” and that “America's economic prosperity in the 21st century will depend on cybersecurity.”

As a result, the President directed a top-to-bottom review of the Federal Government's efforts to defend our information and communications infrastructure, which resulted in a report titled the Cyberspace Policy Review. To implement the results of this review, the President has appointed Howard Schmidt to serve at the U.S. Cybersecurity Coordinator and created the Cybersecurity Office within the National Security Staff, which works closely with the Federal Chief Information Officer Steven VanRoekel, the Federal Chief Technology Officer Todd Park, and the National Economic Council.

Why This is Important

Cyberspace touches nearly every part of our daily lives. It's the broadband networks beneath us and the wireless signals around us, the local networks in our schools and hospitals and businesses, and the massive grids that power our nation. It's the classified military and intelligence networks that keep us safe, and the World Wide Web that has made us more interconnected than at any time in human history. We must secure our cyberspace to ensure that we can continue to grow the nation’s economy and protect our way of life.

What We Must Do

Our Nation’s cybersecurity strategy is twofold: **(1) improve our resilience to cyber incidents** and **(2) reduce the cyber threat.**

Improving our cyber resilience includes: hardening our digital infrastructure to be more resistant to penetration and disruption; improving our ability to defend against sophisticated and agile cyber threats; and recovering quickly from cyber incidents—whether caused by malicious activity, accident, or natural disaster.

Where possible, we must also reduce cyber threats.   We seek to reduce threats by working with allies on international norms of acceptable behavior in cyberspace, strengthening law enforcement capabilities against cybercrime, and deterring potential adversaries from taking advantage of our remaining vulnerabilities.

Underlying all of these efforts is the need to acquire the best possible information about the state of our networks and the capabilities and intentions of our cyber adversaries. We must also make critical cybersecurity information available to and usable by everyone who needs it, including network operators and defenders, law enforcement and intelligence agencies, and emergency management officials in the Federal, State, local, and tribal governments, private industry, and allied governments.

As we take all these actions to secure our networks, we will do so in a manner that preserves and enhances our personal privacy and enables the exercise of our civil liberties and fundamental freedoms. In the 21st Century, our digital networks are essential to our way of life around the world and are an engine for freedom. We will lead by example in order to demonstrate that increased security, enhanced user privacy and keeping the Internet open and innovative go hand-in-hand.

Near Term Actions

The President’s Cyberspace Policy Review identifies 10 near term actions to support our cybersecurity strategy:

1. Appoint a cybersecurity policy official responsible for coordinating the Nation’s cybersecurity policies and activities.
2. Prepare for the President’s approval an updated national strategy to secure the information and communications infrastructure.
3. Designate cybersecurity as one of the President’s key management priorities and establish performance metrics
4. Designate a privacy and civil liberties official to the NSC cybersecurity directorate.
5. Conduct interagency-cleared legal analyses of priority cybersecurity-related issues.
6. Initiate a national awareness and education campaign to promote cybersecurity.
7. Develop an international cybersecurity policy framework and strengthen our international partnerships.
8. Prepare a cybersecurity incident response plan and initiate a dialog to enhance public-private partnerships.

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

http://www.whitehouse.gov/issues/foreign-policy/cybersecurity