



Conclusion: The Way Forward

Our reliance on cyberspace will only continue to grow in the years ahead. Cyberspace and the networks that connect to it now support our economy and provide for our national and homeland defense. This national dependency must be managed with continuous efforts to secure the cyber systems that control our infrastructures.

Securing cyberspace is a complex and evolving challenge. *The National Strategy to Secure Cyberspace* was developed in close collaboration with key sectors of the economy that rely on cyberspace, state and local governments, colleges and universities, and concerned organizations. Town hall meetings were held around the country, and fifty-three clusters of key questions were published to spark public debate.

In addition, a draft version of the *National Strategy to Secure Cyberspace* was shared with the Nation for public comment. The response has been overwhelming.

The public-private partnerships that formed in response to the President's call have developed their own strategies to protect the parts of cyberspace on which they rely. This unique partnership and process was and will continue to be necessary because the majority of the country's cyber resources are controlled by entities outside of government. For the *National Strategy to Secure Cyberspace* to work it must be a plan in which a broad cross section of the country is both invested and committed. Accordingly, the dialogue about how we secure cyberspace will continue.

The *National Strategy to Secure Cyberspace* identifies five national priorities that will help us achieve this ambitious goal. These are: (1) a national cyberspace security response system; (2) a national cyberspace security threat and vulnerability reduction program; (3) a national cyberspace security awareness and training program; (4) securing governments' cyberspace; and, (5) national security and international cyberspace security cooperation. These five priorities will serve to prevent, deter, and protect against attacks. In addition, they also create a process for minimizing the damage and recovering from attacks that do occur.

The *National Strategy to Secure Cyberspace* is, however, only a first step in a long-term effort to secure our information infrastructures. The federal executive branch will use a variety of tools to implement this *Strategy*. The Administration will work with Congress to craft future federal security budgets based on the *Strategy*, providing every department and agency involved in cybersecurity with resources to execute its responsibilities. Each lead department and agency will plan and program to execute the initiatives assigned by the *National Strategy to Secure Cyberspace*.

Within the federal government DHS will play a central role in implementing the *National Strategy to Secure Cyberspace*. In addition to executing its assigned initiatives, the Department would also serve as the primary federal point-of-contact for state and local governments, the private sector, and the American people on issues related to cyberspace security. Working with the White House, the

Department therefore would coordinate and support implementation of non-federal tasks recommended in the *National Strategy to Secure Cyberspace*.

Each department and agency will also be accountable for its performance on cybersecurity efforts. The federal government will employ performance measures—and encourage the same for state and local governments—to evaluate the effectiveness of the cybersecurity programs outlined in this *Strategy*. These performance measures will allow agencies to measure their progress, make resource allocation decisions, and adjust priorities accordingly.

Federal, state, and local governments, as well as organizations and people all across the United States will continue to work to improve cyberspace security. As these strategies and plans are implemented, we will begin to incrementally reduce threats and vulnerabilities.

Cybersecurity and personal privacy need not be opposing goals. Cyberspace security programs must strengthen, not weaken, such protections. The federal government will continue to regularly meet with privacy advocates to discuss cybersecurity and the implementation of this *Strategy*.

For the foreseeable future, two things will be true: America will rely upon cyberspace and the federal government will seek a continuing broad partnership to develop, implement, and refine the *National Strategy to Secure Cyberspace*.