

Opening Statement
The Honorable Adrian Smith, Ranking Member
Subcommittee on Technology and Innovation
Committee on Science and Technology
U.S. House of Representatives

Agency Response to Cyberspace Policy Review

June 16, 2009

Mr. Chairman, thank you for holding this hearing today to review the Administration's efforts to strengthen cybersecurity, as outlined specifically in the White House's recently released *Cyberspace Policy Review*.

While Federal efforts to increase network security date back several years, they were brought to the forefront in early 2008, when President Bush formally established the Comprehensive National Cybersecurity Initiative to deal with widespread and successful cyberattacks on Federal networks. President Obama has committed to fully continue this effort under his administration and emphasized its importance in a recent speech.

It seems this continuity across the Bush and Obama Administrations—as well as the increased attention being given to this issue in Congress—provide indication of a small but important advantage over where we were just a couple of years ago: awareness of this problem and the need for action is now nearly universal. There is broad agreement on the seriousness and magnitude of our cybersecurity vulnerabilities, and the complexity of the technical and policy challenges that must be addressed to overcome them.

However, while there is a consensus on the problem, we are still at the earliest stages of identifying and implementing solutions, and we're working through relatively un-chartered policy territory as we do so. Accordingly, I hope both Congress and the Administration will work to balance the pressure to act quickly and aggressively on cybersecurity with the need for thorough and deliberate consideration of all possible courses of action.

To this end, as we hold these hearings and consider legislative options later this summer, I hope to focus on three broad areas of cybersecurity policy: (1) R&D—Are we investing enough in R&D given its importance as the primary driver of increasing security over the long-term?; (2) DHS-led efforts to secure the dot-gov domain—are we confident that the reported \$30 billion price tag of this initiative is appropriately focused, and is its centerpiece program EINSTEIN going to provide effective and lasting security?; and (3) private sector critical infrastructure—what is the best approach to improving the security of these networks—do new regulations or liability protections make sense, or could they be counterproductive to our security goals?

I hope today's hearing will serve to begin the process of answering these questions. I thank the witnesses for being here and I look forward to a productive discussion.