FACT SHEET
Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure

In February 2009, President Obama directed the National Security Council (NSC) and Homeland Security Council to conduct a 60-day review of the plans, programs, and activities underway throughout government that address our communications and information infrastructure (i.e., "cyberspace"), in order to develop a strategic framework to ensure that the U.S. government's initiatives in this area are appropriately integrated, resourced, and coordinated.

Threats to the information and communications infrastructure pose one of the most serious economic and national security challenges of the 21st Century for the United States and our allies. In this environment, the status quo is no longer acceptable, and a national dialogue on cybersecurity must begin today. The U.S. Government cannot succeed in securing cyberspace in isolation, but it also cannot entirely delegate or abrogate its role in securing the Nation from a cyber incident or accident. Ensuring that cyberspace is sufficiently resilient and trustworthy to support U.S. goals of economic growth, civil liberties and privacy protections, national security, and the continued advancement of global democratic institutions requires working with individuals, academia, industry, and governments. We must make cybersecurity a national priority and lead from the White House.

The review team's report to the President contains five main chapters, outlined below, and includes a near-term action plan for U.S. Government activities to strengthen cybersecurity.

(U) ***Chapter I: Leading from the Top*** **–** Makes the case for strengthening cybersecurity leadership for the United States through 1) the establishment of a Presidential cybersecurity policy official and supporting structures, 2) reviewing laws and policies, and 3) strengthening cybersecurity leadership and accountability at federal, state, local, and tribal levels.

(U) ***Chapter II: Building Capacity for a Digital Nation*** **–** Advocates a national dialogue on cybersecurity to increase public awareness of the threats and risks and how to reduce them. Outlines the need for increased education efforts at all levels to ensure a technologically advanced workforce in cybersecurity and related areas, similar to the United States' focus on mathematics and science education in the 1960s. Identifies the need to expand and improve the federal information technology workforce and for the Federal government to facilitate programs and information sharing on cybersecurity threats, vulnerabilities, and effective practices across all levels of government and industry.

(U) ***Chapter III: Sharing Responsibility for Cybersecurity*** – Discusses the need for improving and expanding partnerships between the Federal government and both the private sector and key U.S. allies.

(U) ***Chapter IV: Creating Effective Information Sharing and Incident Response*** – The United States needs a comprehensive framework to facilitate coordinated responses by government, the private sector, and allies to a significant cyber incident. This chapter explores elements of such a framework and suggests enhancements to information sharing mechanisms to improve incident response capabilities.

(U) ***Chapter V: Encouraging Innovation*** – The chapter addresses ways for the United States to harness the benefits of innovation to address cybersecurity concerns, including work with the private sector to define performance and security objectives for future infrastructure, linking research and development to infrastructure development and expanding coordination of government, industry, and academic research efforts. It also addresses supply chain security and national security / emergency preparedness telecommunications efforts.

Expected attendees at today's East Room event:

Secretary Steven Chu, Department of Energy
Secretary Janet Napolitano, Department of Homeland Security
General James Jones, National Security Advisor
Deputy Secretary William Lynn, Department of Defense
Deputy Secretary Neal Wolin, Department of Treasury
Lawrence Summers, Director of the National Economic Council
Lynne Osmus, Acting Administrator of the Federal Aviation Administration
Jon Wellinghoff, Chairman of the **Federal Energy Regulatory Commission**
Michael Copps, Acting Chairman of the Federal Communications Commission
Jon Leibowitz, Chair of the Federal Trade Commission
James Cartwright, Vice Chairman of the Joint Chiefs of Staff
Robert Mueller, Director of the Federal Bureau of Investigation
John P. Holdren, Director of the Office of Science and Technology
John Kimmons, Lieutenant-general, Director of National Intelligence Office
John O. Brennan, Assistant to the President for Homeland Security and Counterterrorism
Maryland Governor Martin O'Malley, Chair of National Governors Association, Homeland Security Committee
Congressman Bart Gordon
Congressman Peter King
William Pelgrin, Chair of the Multi-State Information Sharing and Analysis Center

Heather Hogsett, National Governors Association, Director, Public Safety and Homeland Security Office of Federal Relations