NBR THE NATIONAL BUREAU of ASIAN RESEARCH

MEDIA ADVISORY

FOR IMMEDIATE RELEASE
Washington, D.C.
July 22, 2015

Contact: Rachel Wagley
Assistant Director, External Relations
Phone: (202) 347-9767
Email: media@nbr.org

OPM HACK AN OPPORTUNITY TO REVISIT KEY CYBER REFORMS

On July 9, 2015, the United States Office of Personnel Management (OPM) announced that the recent cyberattack on the agency compromised the personal information of at least 21.5 million people. 19.7 million of those affected are federal background investigation applicants, including nearly every person who has applied for a background check since 2000. In the wake of the announcement, OPM director Katherine Archuleta stepped down. Members of Congress on both sides of the aisle expressed alarm that OPM officials had failed to take the necessary steps to protect classified data against cyberattacks.

This cyberattack has cued much debate in policy and media circles as to what these necessary steps actually are. The Commission on the Theft of American Intellectual Property (the IP Commission) set out to identify and recommend many of these steps to the federal government in 2013. Heeding one of the IP Commission's key recommendations, Congress passed into law in December 2014 new sanctions authority that would enable the president to deny the privilege of the U.S. banking system to foreign persons that commit cyberespionage. But many leading experts argue that this is not enough. As American law and law enforcement operations lose pace with hacking technology and the speed of the Internet, the Commission's recommendations grow even more relevant.

At the time of the attack, OPM was not tracking servers or devices that had network access and did not support authentication methods one would expect when accessing online banking or a workplace system. Nearly a quarter of OPM's computer systems were operating without valid safety authorizations, even though the agency had recently experienced similar attacks. These deficiencies, in addition to the many other concerns identified in a November 2014 OPM Office of the Inspector General audit report, establish that the agency was not utilizing adequate, up-to-date vulnerability mitigation measures that would better deter opportunistic hackers.

Such measures, however, are only the first defense, especially against targeted hackers with specific missions who are not easily deterred by a strong network defense. The IP Commission encourages legislators to discuss legal reforms that consider deterrence countermeasures to keep these hackers out. Effective deterrence operations could change targeted hackers' cost-benefit analysis. Meanwhile, the IP Commission recommends that the Department of Homeland Security, the Department of Defense, and law enforcement agencies be given the legal authority to use deterrence systems that "operate at network speed against unauthorized intrusions into national security and critical infrastructure networks."

The IP Commission concludes that the government should equip corporations and individuals with the legal rights they need to protect their networks and prevent data exploitation in an environment where law enforcement is extremely limited. The IP Commission endorses an open, two-way communications flow between the government and the private sector that gives corporations the legal protections they need to share information about cyber threats.

The severity of the OPM cyberattack—the latest in a string of breaches that the agency could have done more to avoid—demonstrates the long overdue need to fundamentally reform how the United States prioritizes and legislates on cybersecurity. Establishing diplomatic tools and international cyber codes of conduct are useful long-term exercises. But in order to curb cyber theft, the United States must act to immediately protect its systems and grant both government agencies and the private sector the tools and flexibility they need to deter entry to their networks.

About The Commission on the Theft of American Intellectual Property

The Commission on the Theft of American Intellectual Property was an independent and bipartisan initiative of leading Americans from the private sector, public service in national security and foreign affairs, academe, and politics chaired by Admiral Dennis Blair, former U.S. Director of National Intelligence, and Governor Jon Huntsman, Jr., former U.S. Ambassador to China. The IP Commission outlines detailed policy recommendations to protect the United States against cyber theft.

About The National Bureau of Asian Research

The National Bureau of Asian Research (NBR) conducts advanced independent research on strategic, political, economic, globalization, health, and energy issues affecting U.S. relations with Asia. Drawing upon an extensive network of the world's leading specialists and leveraging the latest technology, NBR bridges the academic, business, and policy arenas. NBR's executive team created and managed the IP Commission.

###