The White House

Office of the Press Secretary

For Immediate Release

January 16, 2015

FACT SHEET: U.S.-United Kingdom Cybersecurity Cooperation

The United States and the United Kingdom agree that the cyber threat is one of the most serious economic and national security challenges that our nations face. Every day foreign governments, criminals, and hackers are attempting to probe, intrude into, and attack government and private sector systems in both of our countries. President Obama and Prime Minister Cameron have both made clear that domestic cybersecurity requires cooperation between governments and the private sector. Both leaders additionally recognized that the inherently international nature of cyber threats requires that governments around the world work together to confront those threats.

During their bilateral meetings in Washington, D.C. this week, President Obama and Prime Minister Cameron agreed to further strengthen and deepen the already extensive cybersecurity cooperation between the United States and the United Kingdom. Both leaders agreed to bolster efforts to enhance the cybersecurity of critical infrastructure in both countries, strengthen threat information sharing and intelligence cooperation on cyber issues, and support new educational exchanges between U.S. and British cybersecurity scholars and researchers.

Improving Critical Infrastructure Cybersecurity

The United States and United Kingdom are committed to our ongoing efforts to improve the cybersecurity of our critical infrastructure and respond to cyber incidents. Both governments have agreed to bolster our efforts to increase threat information sharing and conduct joint cybersecurity and network defense exercises to enhance our combined ability to respond to malicious cyber activity. Our initial joint exercise will focus on the financial sector, with a program running over the coming year. Further, we will work with industry to promote and align our cybersecurity best practices and standards, to include the U.S. Cybersecurity Framework and the United Kingdom's Cyber Essentials scheme.

Strengthening Cooperation on Cyber Defense

The United States and the United Kingdom work closely on a range of cybersecurity and cyber defense matters. For example, the U.S. Computer Emergency Readiness Team (US-CERT) and CERT-UK collaborate on computer network defense and sharing information to address cyber threats and manage cyber incidents. To deepen this collaboration in other areas, the United Kingdom's Government Communications Headquarters (GCHQ) and Security Service (MI5) are working with their U.S. partners – the National Security Agency and the Federal Bureau of Investigation – to further strengthen U.S.-UK collaboration on cybersecurity by establishing a joint cyber cell, with an operating presence in each country. The cell, which will allow staff from each agency to be co-located, will focus on specific cyber defense topics and enable cyber threat information and data to be shared at pace and at greater scale.

Supporting Academic Research on Cybersecurity Issues

The governments of both the United States and the United Kingdom have agreed to provide funding to support a new Fulbright Cyber Security Award. This program will provide an opportunity for some of the brightest scholars in both countries to conduct cybersecurity research for up to six months. The first cohort is expected to start in the 2016-17 academic year, and the U.S.-UK Fulbright Commission will seek applications for this cohort later this year.

In addition, the Massachusetts Institute of Technology's Computer Science & Artificial Intelligence Laboratory (located in Cambridge, MA) has invited the University of Cambridge in the United Kingdom to take part in a "Cambridge vs. Cambridge" cybersecurity contest. This competition is intended to be the first of many international university cybersecurity competitions. The aim is to enhance cybersecurity research at the highest academic level within both countries to bolster our cyber defenses.