Department of Justice
Office of Public Affairs
FOR IMMEDIATE RELEASE
Monday, May 19, 2014

U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage

First Time Criminal Charges Are Filed Against Known State Actors for Hacking

A grand jury in the Western District of Pennsylvania (WDPA) indicted five Chinese military hackers for computer hacking, economic espionage and other offenses directed at six American victims in the U.S. nuclear power, metals and solar products industries.

The indictment alleges that the defendants conspired to hack into American entities, to maintain unauthorized access to their computers and to steal information from those entities that would be useful to their competitors in China, including state-owned enterprises (SOEs). In some cases, it alleges, the conspirators stole trade secrets that would have been particularly beneficial to Chinese companies at the time they were stolen. In other cases, it alleges, the conspirators also stole sensitive, internal communications that would provide a competitor, or an adversary in litigation, with insight into the strategy and vulnerabilities of the American entity.

"This is a case alleging economic espionage by members of the Chinese military and represents the first ever charges against a state actor for this type of hacking," U.S. Attorney General Eric Holder said. "The range of trade secrets and other sensitive business information stolen in this case is significant and demands an aggressive response. Success in the global market place should be based solely on a company's ability to innovate and compete, not on a sponsor government's ability to spy and steal business secrets. This Administration will not tolerate actions by any nation that seeks to illegally sabotage American companies and undermine the integrity of fair competition in the operation of the free market."

"For too long, the Chinese government has blatantly sought to use cyber espionage to obtain economic advantage for its state-owned industries," said FBI Director James B. Comey. "The indictment announced today is an important step. But there are many more victims, and there is much more to be done. With our unique criminal and national security authorities, we will continue to use all legal tools at our disposal to counter cyber espionage from all sources."

"State actors engaged in cyber espionage for economic advantage are not immune from the law just because they hack under the shadow of their country's flag," said John Carlin, Assistant Attorney General for National Security. "Cyber theft is real theft and we will hold state sponsored cyber thieves accountable as we would any other transnational criminal organization that steals our goods and breaks our laws."

"This 21st century burglary has to stop," said David Hickton, U.S. Attorney for the Western District of Pennsylvania. "This prosecution vindicates hard working men and women in Western Pennsylvania and around the world who play by the rules and deserve a fair shot and a level playing field."