Issued 12/14/18

Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing

The cyberattack on the Marriott hotel chain that collected personal details of roughly 500 million guests was part of a Chinese intelligence-gathering effort that also hacked health insurers and the security clearance files of millions more Americans, according to two people briefed on the investigation. The hackers, they said, are suspected of working on behalf of the Ministry of State Security, the country's Communist-controlled civilian spy agency. The discovery comes as the Trump administration is planning actions targeting China's trade, cyber and economic policies, perhaps within days. Those moves include indictments against Chinese hackers working for the intelligence services and the military, according to four government officials who spoke on the condition of anonymity. The Trump administration also plans to declassify intelligence reports to reveal Chinese efforts dating to at least 2014 to build a database containing names of executives and American government officials with security clearances. Other options include an executive order intended to make it harder for Chinese companies to obtain critical components for telecommunications equipment, a senior American official with knowledge of the plans said. The hacking of Marriott's Starwood chain, which was discovered only in September and revealed late last month, is not expected to be part of the coming indictments. But two of the government officials said that it has added urgency to the administration's crackdown, given that Marriott is the top hotel provider for American government and military personnel. It also is a prime example of what has vexed the Trump administration as China has reverted over the past 18 months to the kind of intrusions into American companies and government agencies that President Barack Obama thought he had ended in 2015 in an agreement with

Mr. Xi. From the first revelation that the Marriott chain's computer systems had been breached, there was widespread suspicion in both Washington and among cybersecurity firms that the hacking was not a matter of commercial espionage, but part of a much broader spy campaign to amass Americans' personal data. While American intelligence agencies have not reached a final assessment of who performed the hacking, a range of firms brought in to assess the damage quickly saw computer code and patterns familiar to operations by Chinese actors. The Marriott database contains not only credit card information but passport data. Lisa Monaco, a former homeland security adviser under Mr. Obama, noted last week at a conference that passport information would be particularly valuable in tracking who is crossing borders and what they look like, among other key data. But officials on Tuesday said it was only part of an aggressive operation whose centerpiece was the 2014 hacking into the Office of Personnel Management. At the time, the government bureau loosely guarded the detailed forms that Americans fill out to get security clearances — forms that contain financial data; information about spouses, children and past romantic relationships; and any meetings with foreigners. Such information is exactly what the Chinese use to root out spies, recruit intelligence agents and build a rich repository of Americans' personal data for future targeting. With those details and more that were stolen from insurers like Anthem, the Marriott data adds another critical element to the intelligence profile: travel habits. James A. Lewis, a cybersecurity expert at the Center for Strategic Studies in Washington, said the Chinese have collected "huge pots of data" to feed a Ministry of State Security database seeking to identify American spies — and the Chinese people talking to them. "Big data is the new wave for counterintelligence," Mr. Lewis said.