REMARKS OF U.S. ATTORNEY GEOFFREY S. BERMAN ON THE APT10 INDICTMENT

Today, we announce charges against two Chinese hackers --ZOO HWAH and JONG SHE-LONG--for their involvement in the massive theft of intellectual property and confidential business information from U.S. and foreign companies, and from U.S. government agencies.

The extent and types of data stolen by the defendants is *shocking* and *outrageous*. As alleged, the defendants were members of a hacking group that operated in China called APT10, which stands for Advanced Persistent Threat 10.

As alleged, these defendants engaged in their hacking campaign in association with the Chinese Ministry of State Security.

Over the past 12 years, APT10 has mounted a series of sophisticated computer intrusion campaigns that targeted more than 45 commercial and defense companies in the U.S. as well as managed service providers and their clients around the globe.

How did they do it? As the Indictment alleges, the defendants used spear phishing to install malware that stole the usernames and passwords of employees of victim companies in order to gain entry to their systems. Then, once on the victim's systems, the defendants --using methods to prevent detection-- transferred valuable information and data to computer servers they controlled.

A more recent phase of the conspiracy targeted "managed service providers" or "MSPs". By compromising the computer systems of an MSP, the defendants gained a foothold to more easily compromise the computer networks of the MSP's numerous *clients* on a global scale. As charged, the defendants compromised the data of MSP clients located in at least 12 countries – Brazil, Canada, France, Finland, Germany, India, Japan, Sweden, Switzerland, the United Arab Emirates, the United Kingdom, and the United States.

The defendants' hacking campaigns also targeted U.S. government agencies – including the laboratories of NASA and the U.S. Department of Energy, and the U.S. Navy. Members of APT10 stole confidential personal information, including social security numbers and dates of birth for over 100,000 of our Navy personnel.

It is galling that American companies and government agencies spent years of research and countless dollars to develop their intellectual property, while the defendants simply stole it and got it for free. As a nation, we cannot, and will not, allow such brazen thievery to go unchecked.

I have a message for these defendants, the other members of APT10 as well as their associates in the Chinese Ministry of State Security – the U.S. Government will work relentlessly to identify you and bring you to justice. You cannot remain anonymous even if you are half a world away.

While these defendants remain at large, they are now fugitives from the American justice system, which has a long memory. We look forward to the day when we will have them in a courtroom in the Southern District of New York, and hold them accountable.

I want to thank the FBI, represented here by Director Wray, the Defense Criminal Investigative Service, represented here by [], and the Naval Criminal Investigative Service, represented here by []. Their work in this case has been extraordinary

and serves as an example of what can be accomplished by collaboration among U.S. law enforcement agencies. We are very lucky to have them as partners.

I also would like to thank the prosecutors in my Office who investigated and prosecuted this case: AUSA Sagar Ravi, as well as the supervisors of our Complex Frauds and Cybercrime Unit, Timothy Howard and Daniel Noble.