Advisory

MARCH 2016

Chinese National Pleads Guilty to Conspiracy to Commit Cyber Theft of Export-Controlled Technology

On March 23, 2016, U.S. law enforcement authorities announced that Su Bin, a citizen of the People's Republic of China and a resident of Canada, pleaded guilty to conspiracy to violate the Arms Export Control Act, the Computer Fraud and Abuse Act, and the International Traffic in Arms Regulations ("ITAR"). The investigation and prosecution of Su Bin should remind industry – and particularly defense contractors – of the imperative to have robust cyber controls to protect proprietary and controlled information.

Su Bin was charged by indictment for his role in a conspiracy to steal technical data, including data pertaining to U.S. military aircraft, including the C-17 strategic transport and F-22 and F-35 fighter jets. Su Bin's plea agreement was publicly filed on March 22, 2016 in the U.S. District Court of the Central District of California in connection with his plea of guilty. Under the terms of the plea agreement, Su Bin admitted to conspiring with two other persons in China from October 2008 to March 2014 to gain unauthorized access to protected computer networks in the United States, including computers belonging to a Fortune 50 defense contractor, to obtain sensitive military information for the purpose of exporting that information to China. Su Bin's plea agreement makes clear that the information he and his co-conspirators targeted and improperly obtained included U.S. Munitions List data.

The plea agreement's factual statement describes an elaborate scheme where Su Bin communicated with his co-conspirators and identified individuals (including company executives), companies, and technologies for his confederates to hack from China. Su Bin's co-conspirators would then gain unauthorized access to electronic information residing on computers of U.S. companies and email Su Bin directory files and folder listings. Su Bin then directed his co-conspirators to particular files and folders from which to expropriate data. Su Bin translated the pilfered data from English to Chinese and emailed reports about the stolen information and technology to parties that were not identified in the publicly filed documents.

Su Bin will face a maximum sentence of five years' imprisonment and $250,000 in fines when he is sentenced on July 13, 2016.

This prosecution should serve to remind U.S. companies to be on guard against cyber intrusions and hacking activity. National security and sensitive data should be vigilantly monitored and protected.

If you have any questions about this Advisory, please contact:

JAMES GLASSER
203.498.4313
jglasser@wiggin.com

DAVID HALL
215.988.8325
dhall@wiggin.com

MATTHEW NETTLETON
203.498.4401
mnettleton@wiggin.com