Secretary of Commerce Wilbur L. Ross, Jr. Announces $1.19 Billion Penalty for Chinese Company's Export Violations to Iran and North Korea

Settlement results in largest civil penalty ever levied in a Commerce Export Control case. Company executives developed elaborate scheme to evade U.S. regulations; Obstructed subsequent investigation

Mar | 07 | 2017

Trade and Investment **Export Administration Regulations (EAR)** **Iranian Transactions and Sanctions Regulations (ITSR)** **Wilbur L. Ross**

Posted at 10:50 AM

FOR IMMEDIATE RELEASE
Tuesday, March 7, 2017

Office of Public Affairs

202-482-4883
publicaffairs@doc.gov

Secretary of Commerce Wilbur L. Ross, Jr. today announced that China's Zhongxing Telecommunications Equipment Corporation and ZTE Kangxun Telecommunications Ltd., known collectively as ZTE, has agreed to a record-high combined civil and criminal penalty of $1.19 billion, pending approval from the courts, after illegally shipping telecommunications equipment to Iran and North Korea in violation of the Export Administration Regulations (EAR) and the Iranian Transactions and Sanctions Regulations (ITSR).

As part of the settlement, ZTE has agreed to pay a penalty of $661 million to Commerce's Bureau of Industry Security (BIS), with $300 million suspended during a seven-year probationary period to deter future violations. This civil penalty is the largest ever imposed by the BIS and, if the criminal plea is approved by a federal judge, the combined $1.19 billion in penalties from Commerce, the Department of Justice, and the Department of Treasury, would be the largest fine and forfeiture ever levied by the U.S. government in an export control case.

"We are putting the world on notice: the games are over," said Secretary Ross. "Those who flout our economic sanctions and export control laws will not go unpunished – they will suffer the harshest of consequences. Under President Trump's leadership, we will be aggressively enforcing strong trade policies with the dual purpose of protecting American national security and protecting American workers."

In addition to these monetary penalties, ZTE also agreed to active audit and compliance requirements designed to prevent and detect future violations and a seven-year suspended denial of export privileges, which could be quickly activated if any aspect of this deal is not met.

“The results of this investigation and the unprecedented penalty reflects ZTE’s egregious scheme to evade U.S. law and systematically mislead investigators,” Secretary Ross said. “This penalty is an example of the extraordinary powers the Department of Commerce will use to vigorously protect the interests of the United States. I am very proud of the outstanding work of the Department’s Bureau of Industry and Security, Office of Export Enforcement and its Office of Chief Counsel.”

As part of the $1.19 billion plea deal, the U.S. District Court for the Northern District of Texas will consider imposing $430,488,798 in combined criminal fines and forfeiture on ZTE as part of a plea agreement with the Department of Justice. ZTE has also agreed to pay the Department of the Treasury’s Office of Foreign Assets Control (OFAC) $100,871,266 pursuant to a settlement agreement.

ZTE’s Scheme

Starting no later than January 2010 and continuing through April 2016, ZTE conspired to evade the long-standing and widely known U.S. embargo against Iran in order to obtain contracts with and related sales from Iranian entities, including entities affiliated with the Iranian Government, to supply, build, operate, and/or service large-scale telecommunications networks in Iran, the backbone of which would be U.S.-origin equipment and software.

As a result of the conspiracy, ZTE was able to obtain hundreds of millions of dollars in contracts with and sales from such Iranian entities. Additionally, ZTE undertook other actions involving 283 shipments of controlled items to North Korea with knowledge that such shipments violated the EAR.

Shipped items included routers, microprocessors, and servers controlled under the EAR for national security, encryption, regional security, and/or anti-terrorism reasons. In addition, ZTE engaged in evasive conduct designed to prevent the U.S. government from detecting its violations.

The Investigation, Sanction, and Subsequent Charges

The BIS Office of Export Enforcement Dallas Field Office, in partnership with the U.S. Attorney’s Office for the Northern District of Texas, The Department of Justice Counterintelligence and Export Control Section, FBI and the Department of Homeland Security’s Homeland Security Investigations, investigated ZTE for five years, beginning in 2012 when allegations of illegal conduct first surfaced in media reports. BIS’s subsequent service of an administrative subpoena on ZTE’s U.S. affiliate, ZTE USA, Inc., led ZTE to slow its unlawful shipments to Iran. BIS later learned that in November 2013, following a meeting of senior managers chaired by its then-CEO, ZTE made plans to resume transshipments to Iran that would continue during the course of the investigation.

On March 7, 2016, the Department of Commerce sanctioned ZTE by adding it to the Entity List, which created a license requirement to export, reexport, or transfer (in-country) to ZTE any items subject to the EAR. The principal basis for the addition were two ZTE corporate documents titled “Report Regarding Comprehensive Reorganization and Standardization of the Company Export Control Matters,” which indicated that ZTE reexported controlled items to sanctioned countries contrary to U.S. law and “Proposal for Import and Export Control Risk Avoidance,” which described how ZTE planned and organized a scheme to establish, control and use a series of “detached” (i.e., shell) companies to illicitly reexport controlled items to Iran in violation of U.S. export control laws.

During the course of the investigation, ZTE made knowingly false and misleading representations and statements to BIS or other U.S. law enforcement agencies, including that the company had previously stopped shipments to Iran as of March 2012, and was no longer violating U.S. export control laws. ZTE also engaged in an elaborate scheme to prevent disclosure to and affirmatively mislead the U.S. Government, by deleting and concealing documents and information from the outside counsel and forensic accounting firm that ZTE had retained with regard to the investigation.

This scheme included forming and operating a 13-member "Contract Data Induction Team" within ZTE between January and March 2016, that destroyed, removed, or sanitized all materials concerning transactions or other activities relating to ZTE's Iran business that post-dated March 2012; deleted on a nightly basis all of the team's emails to conceal the team's activities; and required each of the team members to sign a non-disclosure agreement covering the ZTE transactions and activities the team was tasked with hiding. Under the non-disclosure agreement, team members would be subject to a penalty of 1 million Renminbi (or approximately $150,000) payable to ZTE if it determined a disclosure occurred.

"Despite ZTE's repeated attempts to thwart the investigation, the dogged determination of investigators uncovered damning evidence of an orchestrated, systematic scheme to violate U.S. export controls by supplying equipment to sanctioned destinations," said Douglas Hassebrock, Director of the Bureau of Industry and Security's Office of Export Enforcement which spearheaded the investigation.

Organizations and Groups
Leadership
Related content

Mar | 15 | 2016

Commerce and Treasury Announce Significant Amendments to the Cuba Sanctions Regulations Ahead of President Obama's Historic Trip to Cuba

Trade and Investment **Cuba** **Cuban Assets Control Regulations (CACR)** **Export Administration Regulations (EAR)**

Today, the Department of the Treasury's Office of Foreign Assets Control (OFAC) and the Department of Commerce's Bureau of Industry and Security (BIS) announced significant...

/*Fix video embed transcript line height which was set to 0, squishing transcript to one line.*/ .file.view-mode-embedded_video { line-height: inherit; }

Source URL: https://www.commerce.gov/news/press-releases/2017/03/secretary-commerce-wilbur-l-ross-jr-announces-119-billion-penalty

Links:
[1] https://www.commerce.gov/news/press-releases/2017/03/secretary-commerce-wilbur-l-ross-jr-announces-119-billion-penalty
[2] https://www.commerce.gov/categories/trade-and-investment
[3] https://www.commerce.gov/tags/export-administration-regulations-ear
[4] https://www.commerce.gov/tags/iranian-transactions-and-sanctions-regulations-itsr
[5] https://www.commerce.gov/tags/wilbur-l-ross
[6] https://www.commerce.gov/doc/os/office-public-affairs
[7] mailto:publicaffairs@doc.gov

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Tuesday, March 7, 2017

ZTE Corporation Agrees to Plead Guilty and Pay Over $430.4 Million for Violating U.S. Sanctions by Sending U.S.-Origin Items to Iran

Combined Penalty of $1.19 Billion with Department of Commerce and Department of Treasury Actions Shows All of Government Approach to Sanctions Enforcement

ZTE Corporation has agreed to enter a guilty plea and to pay a $430,488,798 penalty to the U.S. for conspiring to violate the International Emergency Economic Powers Act (IEEPA) by illegally shipping U.S.-origin items to Iran, obstructing justice and making a material false statement. ZTE simultaneously reached settlement agreements with the U.S. Department of Commerce's Bureau of Industry and Security (BIS) and the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC). In total ZTE has agreed to pay the U.S. Government $892,360,064. The BIS has suspended an additional $300,000,000, which ZTE will pay if it violates its settlement agreement with the BIS.

Attorney General of the United States Jeff Sessions, Acting Assistant Attorney General for National Security Mary B. McCord, U.S. Attorney John R. Parker for the Northern District of Texas and FBI Assistant Director Bill Priestap for the Counterintelligence Division made the announcement today.

"ZTE Corporation not only violated export controls that keep sensitive American technology out of the hands of hostile regimes like Iran's – they lied to federal investigators and even deceived their own counsel and internal investigators about their illegal acts," said Attorney General Sessions. "This plea agreement holds them accountable, and makes clear that our government will use every tool we have to punish companies who would violate our laws, obstruct justice and jeopardize our national security. I am grateful to the Justice Department's National Security Division, the U.S. Attorney's Office for the Northern District of Texas and the FBI for their outstanding work on this investigation."

"ZTE engaged in an elaborate scheme to acquire U.S.-origin items, send the items to Iran and mask its involvement in those exports. The plea agreement, which is pending before the Court, alleges that the highest levels of management within the company approved the scheme. ZTE then repeatedly lied to and misled federal investigators, its own attorneys and internal investigators. Its actions were egregious and warranted a significant penalty," said Acting Assistant Attorney General McCord. "The enforcement of U.S. export control and sanctions laws is a major component of the National Security Division's commitment to protecting the national security of the United States. Companies that violate these laws – including foreign companies – will be investigated and held to answer for their actions."

"ZTE Corporation not only violated our export control laws but, once caught, shockingly resumed illegal shipments to Iran during the course of our investigation," said U.S. Attorney Parker. "ZTE Corporation then went to great lengths to devise elaborate, corporate-wide schemes to hide its illegal conduct, including lying to its own lawyers."

"The plea agreement in this case shows ZTE repeatedly violated export controls and illegally shipped U.S. technology to Iran," said Assistant Director Priestap. "The company also took extensive measures to hide what it was doing from U.S. authorities. This case is an excellent example of cooperation among multiple U.S. agencies to uncover illegal technology transfers and make those responsible pay for their actions."

The plea agreement, which is contingent on the court's approval, also requires ZTE to submit to a three-year period of corporate probation, during which time an independent corporate compliance monitor will review and report on ZTE's export compliance program. ZTE is also required to cooperate fully with the Department of Justice (DOJ) regarding any criminal investigation by U.S. law enforcement authorities. The plea agreement ends a five-year joint investigation into ZTE's export practices, which was handled by the DOJ's National Security Division, the U.S. Attorney's Office for the Northern District of Texas, the FBI, the BIS and the Department of Homeland Security, U.S. Immigration and Customs Enforcement's Homeland Security Investigations.

A criminal information was filed today in federal court in the Northern District of Texas charging ZTE with one count of knowingly and willfully conspiring to violate the IEEPA, one count of obstruction of justice and one count of making a material false statement. ZTE waived the requirement of being charged by way of federal indictment, agreed to the filing of the information and has accepted responsibility for its criminal conduct by entering into a plea agreement with the government. The plea agreement, which is contingent on the court's approval, requires that ZTE pay a fine in the amount of $286,992,532 and a criminal forfeiture in the amount of $143,496,266. The criminal fine represents the largest criminal fine in connection with an IEEPA prosecution.

Summary of the Criminal Conduct

According to documents filed today, for a period of almost six years, ZTE obtained U.S.-origin items – including controlled dual-use goods on the Department of Commerce's Commerce Control List (CCL) – incorporated some of those items into ZTE equipment and shipped the ZTE equipment and U.S.-origin items to customers in Iran. ZTE engaged in this conduct knowing that such shipments to Iran were illegal. ZTE further lied to federal investigators during the course of the investigation when it insisted, through outside and in-house counsel, that the company had stopped sending U.S.-origin items to Iran. In fact, while the investigation was ongoing, ZTE resumed its business with Iran and shipped millions of dollars' worth of U.S. items there.

ZTE also created an elaborate scheme to hide the data related to these transactions from a forensic accounting firm hired by defense counsel to conduct a review of ZTE's transactions with sanctioned countries. It did so knowing that the information provided to the forensic accounting firm would be reported to the U.S. government by outside counsel. Outside counsel was not aware of this scheme and indeed was wholly unaware that ZTE had resumed business with Iran. After ZTE informed its counsel of the scheme, counsel reported – with permission from ZTE – the conduct to the U.S. government.

The Iran Business

According to court documents, between January 2010 and January 2016, ZTE, either directly or indirectly through a third company, shipped approximately $32,000,000 of U.S.-origin items to Iran without obtaining the proper export licenses from the U.S. government. In early 2010, ZTE began bidding on two different Iranian projects. The projects involved installing cellular and landline network infrastructure. Each contract was worth hundreds of millions of U.S. Dollars and required U.S. components for the final products.

In December 2010, ZTE finalized the contracts with Iranian customers. The contracts were signed by four parties: the Iranian customer, ZTE, Beijing 8 Star and ZTE Parsian. Court documents explain that ZTE identified Beijing 8 Star (8S) as a possible vehicle for hiding its illegal shipments of U.S. items to Iran. It intended to use 8S to export U.S.-origin items from China to ZTE customers in Iran. As part of this plan, ZTE supplied 8S with necessary capital and took over control of the company.

Under the terms of the Iran contracts, ZTE agreed to supply the "self-developed equipment," collect payments for the projects and manage the whole network. ZTE Parsian was to provide locally purchased materials and all services. 8S was responsible for "relevant third-party equipment," which primarily meant parts that would be subject to U.S. export laws. ZTE intended for 8S to be an "isolation company," that is, ZTE intended for 8S (rather than ZTE) to purchase the embargoed equipment from suppliers and provide that equipment under the contract in an effort to distance ZTE from U.S. export-controlled products and insulate ZTE from U.S. export violations. However, 8S had no purchasing or shipping history and no real business reputation.

Ultimately, although 8S was a party to the contracts, ZTE itself purchased and shipped the embargoed goods under the contract. In its shipping containers, it packaged the U.S. items with its own self-manufactured items to hide the U.S.-origin goods. ZTE did not include the U.S. items on the customs declaration forms, though it did include the U.S.-origin items on the packing lists included inside of the shipments.

In early 2011, when ZTE determined that the use of 8S was insufficient to hide ZTE's connection to the illegal export of U.S.-origin goods to Iran, senior management of ZTE ordered that a company-level export control project team study, handle and respond to the company's export control risks. In September 2011, four senior managers signed an Executive Memo, which proposed that the company identify and establish new "isolation companies" that would be responsible for supplying U.S. component parts necessary for projects in embargoed countries. The isolation companies would conceal ZTE's role in the transshipment scheme and would insulate ZTE from export control risks.

In March 2012, Reuters published an article regarding ZTE's sale of equipment to Iran. In response, ZTE made a decision to temporarily cease sending new U.S. equipment to Iran. By November 2013, however, ZTE had resumed its business with Iran. Beginning in July 2014, ZTE began shipping U.S.-origin equipment to Iran once again without the necessary licenses.

Instead of using 8S, however, ZTE identified a new isolation company. ZTE signed a contract with the new isolation company, which in turn signed contracts with the two Iranian customers. According to the new scheme, ZTE purchased and manufactured all relevant equipment – both U.S.-origin and ZTE-manufactured – and prepared them for pick-up at its warehouse by the new isolation company. The new isolation company then shipped all items to the Iranian customers. Shipments to Iran continued from January 2014 through January 2016.

The Obstruction and False Statement

According to court documents, despite its knowledge of an ongoing grand jury investigation into its Iran exports, ZTE took several steps to conceal relevant information from the U.S. government. It further took affirmative steps to mislead the U.S. government. In the summer of 2012, ZTE asked each of the employees who were involved in the Iran sales to sign nondisclosure agreements in which the employees agreed to keep confidential all information related to the company's U.S. exports to Iran.

During meetings throughout late 2014, late 2015 and early 2016, outside counsel for ZTE, unaware that the statements ZTE had given to counsel for communication to the government were false, represented to the DOJ and federal law enforcement agents that ZTE had stopped doing business with Iran and therefore was no longer violating U.S. export laws. Similarly, on July 8, 2015, in-house counsel for ZTE accompanied outside counsel in a meeting with the DOJ and federal law enforcement agents and reported that ZTE was abiding by U.S. laws. That statement was also false.

ZTE also hid data related to its resumed illegal sales to Iran from a forensic accounting firm hired by defense counsel to conduct an internal investigation into the company's Iran sales. ZTE knew the forensic accounting firm was reviewing its systems and knew that the analysis was being reported to the DOJ and U.S. law enforcement. To avoid detection of its 2013-2016 resumed illegal sales to Iran, ZTE formed the "contract data induction team" ("CDIT"). The CDIT was comprised of approximately 13 people whose job it was to "sanitize the databases" of all information related to the 2013-2016 Iran business. The team identified and removed from the databases all data related to those sales. ZTE also established an auto-delete function for the email accounts of those 13 individuals on the CDIT, so their emails were deleted every night – a departure from its normal practices – to ensure there were no communications related to the hiding of the data.

The case is being prosecuted by Deputy Chief Elizabeth Cannon of the National Security Division's Counterintelligence and Export Control Sections and Assistant U.S. Attorney Mark Penley of the Northern District of Texas.

ZTE Information
ZTE Plea Agreement Supplement
ZTE Plea Agreement

ZTE Factual Resume

17-252

National Security Division (NSD)
USAO - Texas, Northern

Topic:
Counterintelligence and Export Control

Updated March 7, 2017