

PROPOSED CHARGING LETTER

REGISTERED MAIL - RETURN RECEIPT REQUESTED

Zhongxing Telecommunications Equipment Corporation
ZTE Plaza, Keji Road South
Hi-Tech Industrial Park
Nanshan District, Shenzhen
China

Attention: Zhao Xianming, President

ZTE Kangxun Telecommunications Ltd.
2/3 Floor, Suite A, Zte Communication Mansion Keji (S) Road
Hi-New Shenzhen, 518057
China

Attention: Ye Weimin, Chairman

Dear Dr. Zhao and Mr. Ye:

The Bureau of Industry and Security, U.S. Department of Commerce (“BIS”), has reason to believe that Zhongxing Telecommunications Equipment Corporation, of Shenzhen, China (“ZTE Corporation”) and ZTE Kangxun Telecommunications Ltd. of Hi-New Shenzhen, China (“ZTE Kangxun”) (collectively, “ZTE”) committed 380 violations of the Export Administration Regulations (the “Regulations”),¹ which issued under the authority of the Export Administration Act of 1979, as amended (the “Act”).² Specifically, BIS charges the following violations:

Charge 1 15 C.F.R. § 764.2(d) – Conspiracy

Background, Formation, and Development of the Conspiracy

1. From no later than in or around January 2010, and continuing until in or around April 2016, ZTE Corporation and ZTE Kangxun conspired and acted in concert with others, known and unknown, to bring about or do acts that constitute violations of the Regulations. The purpose of the conspiracy was to evade the long-standing and widely known U.S. embargo against Iran in order to obtain contracts with and related sales from

¹ The Regulations are currently codified in the Code of Federal Regulations at 15 C.F.R. Parts 730-774 (2016). The charged violations occurred in 2010-2016. The Regulations governing the violation at issue are found in the 2010-2016 versions of the Code of Federal Regulations (15 C.F.R. Parts 730-774 (2010-2016)). The 2016 Regulations set forth the procedures that apply to this matter.

² 50 U.S.C. §§ 4601-4623 (Supp. III 2015) (available at <http://uscode.house.gov>). Since August 21, 2001, the Act has been in lapse and the President, through Executive Order 13,222 of August 17, 2001 (3 C.F.R., 2001 Comp. 783 (2002)), as extended most recently by the Notice of August 4, 2016 (81 Fed. Reg. 52,587 (August 8, 2016)), has continued the Regulations in effect under the International Emergency Economic Powers Act (50 U.S.C. § 1701, *et seq.* (2006 and Supp. IV 2010)).

Iranian entities, including entities directly or indirectly affiliated with the Iranian Government, to supply, build, operate, and/or service large-scale telecommunications networks in Iran, the backbone of which would be and were 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.

2. The lynchpin of the conspiracy throughout was the procurement, sale, delivery, and use of U.S.-origin items, without which the Iranian entities would not have entered into large-scale network agreements with ZTE or purchased related items and services as part of those agreements. The deal- and network-critical U.S.-origin items included, for example, routers, microprocessors, servers, databases, and other items listed on the Commerce Control List (“CCL”) and controlled under the Regulations on national security, encryption, regional security, and/or anti-terrorism grounds, as well as items designated EAR99 under the Regulations.³ These items also were subject to the Iranian Transactions and Sanctions Regulations (“ITSR”), 31 C.F.R. Part 560, administered by the Department of the Treasury’s Office of Foreign Assets Control (“OFAC”).⁴
3. During the conspiracy, ZTE employed multiple strategies in an attempt to conceal or obscure the true nature and extent of its role in the transactions and thereby facilitate its evasion of U.S. export controls, of which ZTE had detailed knowledge. A key aspect of the conspiracy was the use of a ZTE affiliate or alter ego, or another Chinese company acting in concert with ZTE, to procure equipment and software, including from well-known U.S. hardware and software technology companies, without disclosing that the items were intended for transshipment or reexport to Iran.
4. The U.S.-origin items procured and transshipped to Iran, either separately or as or for use as components of larger systems, included items controlled under Export Control Classification Numbers (“ECCNs”) 3A001, 3A991, 3A992, 3A999, 4A994, 5A001, 5A002, 5A991, 5A992, 5B991, 5D002, 5D991, 5D992, or 7A994. At all times pertinent hereto, Section 746.7 of the Regulations imposed a BIS license requirement for the export or reexport to Iran of these CCL items, including transshipments through a third country, such as China. Section 742.8 also applied to items controlled under the Regulations on anti-terrorism grounds.
5. In addition, pursuant to Section 746.7 of the Regulations, no person could lawfully export or reexport any item subject to the Regulations, whether an item on the CCL or designated EAR99, if the transaction was prohibited by the ITSR. This additional prohibition under Section 746.7 applied whether or not the Regulations otherwise imposed a license requirement for the transaction. At all times pertinent hereto, the ITSR

³ EAR99 is a designation for items subject to the Regulations but not listed on the CCL. *See* 15 C.F.R. §§ 734.3(c) and 772.1.

⁴ The ITSR were formerly known as the Iranian Transaction Regulations or “ITR.” On October 22, 2012, OFAC renamed and reissued the Iranian Transactions Regulations as the Iranian Transactions and Sanctions Regulations. *See* 77 Fed. Reg. 64,664 (Oct. 22, 2012). 31 C.F.R. part 560 remained the same in pertinent part at all times relevant hereto.

prohibited, *inter alia*, the unauthorized exportation, reexportation, sale or supply, directly or indirectly, from the United States to Iran of any goods, technology, or services. This broad prohibition included the exportation, reexportation, sale or supply of any goods, technology, or services from the United States to a third country, such as China, undertaken with knowledge or reason to know that (a) they were intended for supply, transshipment, or reexportation, directly or indirectly, to Iran, or (b) they were intended specifically for use in the production of, for commingling with, or for incorporation into goods, technology, or services to be directly or indirectly supplied, transshipped, or reexported predominantly or exclusively to Iran. 31 C.F.R. § 560.204. Like the Regulations, the ITSR also prohibited a conspiracy to violate any of its prohibitions, as well as any transactions that evaded or were intended to evade, or caused or attempted a violation of, any of its prohibitions. 31 C.F.R. § 560.203.

6. At all times pertinent hereto, a license had to be obtained from BIS for any transaction that involved items that were subject to the Regulations, but not the ITSR, and required a license under Section 746.7 or 742.8 of the Regulations. However, in order to avoid duplication regarding transactions involving items subject to both the Regulations and the ITSR, whether CCL or EAR99 items, Section 746.7 provided that authorization did not need to be obtained from both BIS and OFAC, but instead that authorization by OFAC under the ITSR was considered authorization for purposes of the Regulations as well.
7. No authorization was sought or obtained from BIS, or from OFAC, in connection with any of the transactions or activities described herein. To the contrary, during the course of and in furtherance of the conspiracy and the Iranian network contracts, ZTE, *inter alia*, ordered, bought, sold, concealed, transferred, transported, forwarded, used, financed, and/or serviced items subject to the EAR, or directed and caused such activities to occur, with knowledge that a violation of the Regulations had occurred or was about or intended to occur.
8. Beginning in no later than 2010, ZTE began transshipments and/or reexports to Iran in violation of the U.S. embargo, including to Ertebatat Tamin Shams Novin, subsequently known as Rightel (“Tamin/Rightel”), and to the Telecommunications Company of Iran (“TCI”). Publically available information indicates that Tamin/Rightel was established in or about May 2007, by the Iranian Social Security Investment Company, which is a state-owned fund and investment vehicle for the Iranian social security system, while TCI is majority-owned by a consortium owned or controlled by the Iranian Revolutionary Guard Corps.
9. Tamin/Rightel was awarded Iran’s Third Mobile Network License in 2009, and sought thereafter in 2010 to contract for the development and operation of a Global System for Mobile Communications (GSM)/UMTS Terrestrial Radio Access Network (UTRAN), which would cover numerous sites in Tehran and eight other main Iranian cities.
10. In seeking this network contract, ZTE Corporation’s then-CEO at all times pertinent hereto met with Tamin/Rightel officials on or about July 29, 2010. During the meeting, the then-CEO highlighted ZTE’s connection to the Chinese government and ZTE’s

ability to facilitate Tamin/Rightel's acquisition of financing for the project through Chinese banks.

11. ZTE subsequently finalized and signed a contract with Tamin/Rightel on or about November 22, 2010 for "Project: GSM/UTRAN Network in I.R. [of] Iran," to supply, build, operate, and service Iran's first 2G/3G- and 4G-ready mobile telecommunication network. The contract was signed by not only Tamin/Rightel and ZTE, but also by ZTE's Iranian representative office, ZTE Parsian, and a ZTE-controlled Chinese entity, Beijing 8 Star International Co. Ltd. ("Beijing 8 Star" or "8S"). ZTE agreed to deliver "Geo-Marketing, Engineering, Build, Operate, Maintenance and Transfer solutions," and agreed that it was "liable, responsible and [the] coordinator for the full performance of the whole GSM/UTRAN network under this Contract." ZTE was to supply equipment and parts, either directly or through Beijing 8 Star, while ZTE Parsian would handle local equipment and service logistics. ZTE also agreed to provide 85% of the financing under the contract.
12. While negotiating with Tamin/Rightel, ZTE also was negotiating a similar network contract with TCI, which owned or controlled Iran's fixed line telecommunications infrastructure and was Iran's largest Internet service provider and cellular and data communications operator. By in or about February 2010, ZTE and TCI had come to a "mutual cooperation agreement" concerning the expansion of TCI's existing networks under which ZTE would be the "sole vendor" to "collaborate" with TCI, including with regard to obtaining financing through Chinese banking institutions.
13. On or about December 28, 2010, the contract for TCI's "Network Optimization Project" was finalized by ZTE and TCI. As with the Tamin/Rightel network contract, this contract also was structured as a four-party agreement, with ZTE Parsian and Beijing 8 Star again signing in addition to ZTE and TCI. Under the stated terms of this contract, ZTE was to supply "self-developed equipment," manage the network, and collect payment. Beijing 8 Star was to supply "relevant third-party equipment" and ZTE Parsian to provide services and handle local supply and logistics. The TCI network contract included a surveillance function.
14. As ZTE's Iran business grew during the course of 2010, and as the network contract negotiations with Tamin/Rightel and TCI neared completion in the fourth quarter of the year, ZTE took steps to expand and systematize its efforts to evade the U.S. embargo and avoid detection by the U.S. Government. For example, a ZTE corporate memorandum entitled "Iran's Logistics Implementation," and marked "highly confidential," was emailed among ZTE employees on or about October 27, 2010. The memorandum began by referencing that ZTE had projects underway in each of (at that time) Iran's 30 provinces, listed the U.S. embargo as one of the "main risks" in executing ZTE's Iran contracts, including with regard to "follow-up maintenance of the equipment[.]" and instructed employees that "orders for [recognizable U.S. brand] products shall be placed in batches in the name of other clients[.]"

15. ZTE Corporation also created a team of employees dubbed the “YL Front Line,” using “YL” as a coded reference for Iran. The YL Front Line was tasked with finding ways to enable ZTE to further the conspiracy and fulfill the network contracts by procuring, and shipping on to Iran, U.S.-origin equipment and software without the required U.S. Government authorization, which ZTE knew in all likelihood could not be obtained.
16. The initial strategy developed by the YL Front Line centered on using Beijing 8 Star, which had been formed by two ZTE employees in 2009, rather than by ZTE itself. As a front or “carve out” company, Beijing 8 Star would be staffed and controlled by ZTE, but would appear from the outside to be separate and independent. Beijing 8 Star would be used to purchase U.S.-origin equipment and software from suppliers on ZTE’s behalf and then transship the items to Iran.
17. This initial, carve out company scheme was reflected in the structure of ZTE’s network contracts with Tamin/Rightel and TCI. However, given the high value and large volumes of items that ZTE needed to procure and then supply to execute its Iran network contracts, this scheme quickly became problematic, as third-party companies declined to deal or work with Beijing 8 Star because it had no established credit or operational history or business reputation within even China.
18. ZTE thus altered its scheme to adopt what it described as the “partial isolation effect,” under which ZTE Kangxun (rather than Beijing 8 Star) would serve as the purchasing agent, procuring the U.S.-origin items and related items, including ZTE-produced equipment, but would not itself ship the items to Iran. ZTE Corporation would then transship the more sensitive U.S.-controlled items to Iran based on ZTE’s view that its shipments were less likely to be stopped, searched, or detained by customs officials than shipments by Beijing 8 Star. Less sensitive U.S.-origin items and foreign-origin items generally were to be shipped together to Iran by Beijing 8 Star.
19. Subsequently, ZTE changed the scheme again, including under the Tamin/Rightel and TCI network contracts, in response to further problems faced by Beijing 8 Star. As a result, in executing these contracts, the U.S.-origin items typically were shipped by ZTE Corporation itself. Nonetheless, ZTE continued to staff and direct the activities of Beijing 8 Star.
20. ZTE took and directed additional steps to conceal and further the conspiracy. For example, whether shipped by ZTE or by Beijing 8 Star, U.S.-origin items were sandwiched between foreign-origin items to decrease the risk that the U.S.-origin items would be detected if a container was opened by customs officials. The packing lists for items being shipped by ZTE to Iran were not to contain any ZTE markings, the signatory on export documentation for ZTE had to differ from the signatory on documentation for Beijing 8 Star, and such documentation for Beijing 8 Star could only bear the Beijing 8 Star seal. ZTE’s Export Department also was ordered to pay special attention so that “sensitive materials shall be packed in the place not easily [detected], and shall not have any ZTE mark [on the] packing list[.]” Even after the “sensitive” items were packed,

additional checks had to be performed by ZTE's Contract Performance Department, which was ordered to "carefully examine" each shipment a second time.

Fulfillment of the Tamin/Rightel and TCI Contracts and Systemization of the Scheme

21. The ZTE-Tamin/Rightel network contract included annexes setting unit prices and provided that Tamin/Rightel could issue purchase orders without any prior quotation. It also provided that ZTE would prepare equipment pro forma invoices in accordance with a breakdown of the contract prices, subject only to a three working-day comment period, and submit them to Tamin/Rightel for the establishment of letters of credit for payment purposes. The first purchase order issued under this contract no later than on or about December 26, 2010. This extensive purchase order covered good and services totaling approximately \$165 million and included references to payments to be made totaling the same amount for fulfilling the order. ZTE issued a corresponding pro forma invoice dated April 4, 2011.⁵
22. Subsequently, ZTE issued invoices in June 2011, one in its name and the other under Beijing 8 Star's name, totaling approximately \$46.8 million under the Tamin/Rightel network contract.
23. ZTE also made extensive shipments under the TCI network contract, including, for example, one shipment on or about July 23, 2011, that involved a 907-page packing list. The TCI network contract had a stated value of approximately \$130.2 million when signed on December 28, 2010. In July and August 2011, ZTE was paid at least approximately \$26.5 million by TCI, and in March and April 2013, received another approximately \$41.2 million in payments from TCI for shipments that had occurred in 2011-2012.
24. As its Iran business expanded rapidly during 2011, including significantly due to the Tamin/Rightel and TCI network contracts and related sales, ZTE continued to develop revised strategies to evade the Regulations, including through further efforts to systematize its schemes.
25. Using "YL" as code for Iran in an internal document entitled "Proposal for Import and Export Control Risk Avoidance – YL as an Example" and marked "Top Secret Highly Confidential," ZTE analyzed in detail the "serious import and export control risks" associated with its violations of U.S. trade embargoes and related export control laws, including countries such as Iran that the U.S. had designated as "State Sponsor of

⁵ This pro forma invoice's stated amount in Euros was unchanged from the December 2010 purchase order. Due to the currency conversion rates applicable to the two dates, this amount had risen by April 2011 to approximately \$166.3 million. For ease of reference, all monetary amounts associated with this invoice and other documents relating to the November 22, 2010 Tamin/Rightel network contract or to other contracts alleged in this proposed charging letter, including, *inter alia*, purchase orders, commercial invoices, and credit advices, will be set out only in dollar terms based on the Euro-U.S. Dollar conversion rate on the applicable date.

Terrorism.” The analysis continued by discussing the differences between the “partial isolation” or “semi-detached” model—which ZTE summarized as a model under which the “trading relationship on the surface between exporter and importer involves non-controlled commodities”—and a “completely detached business” model—under which additional layers of intermediary companies would be created or used such that a “trading relationship does not exist at all on the surface between exporter and importer.” The analysis also noted that ZTE had entered into many agreements with Iranian clients, which “had all entered the project execution phase,” and then warned:

[The] Semi-Detached Model is the cooperation model used on these agreements, and the contract(s) were signed by four parties, YL Client, ZTE, ZTE YL, and 8S. However, in the actual execution process, our company did not strictly follow the requirements of the Semi-Detached Model Instead, ZTE directly assumed the rights and obligations of 8S, and ZTE exported controlled-commodities directly to YL. Such [an] operating model would directly expose our company to the import and export control risks, which will easily lead to the U.S. Government’s notice and investigation and it’ll go against our company’s preliminary argument and defense.

Since the above mentioned risks exist in our company’s current operating model in YL, our company urgently needs to choose a proper Detached Model and strictly follow the [selected] model during operation, severing contacts with the YL Client, and to the best of [our] ability, preventing our company from being identified as having trade activities with YL; thus effectively avoiding the import and export control risks.

26. Furthermore, in or around late August and early September 2011, a ZTE document entitled “Report Regarding Comprehensive Reorganization and Standardization of the Company Export Control Related Matters” which had been drafted by ZTE Corporation’s Legal Department, was ratified and signed by four high-ranking ZTE Corporation executives, including ZTE Corporation’s CEO, who ratified and signed on or about September 2, 2011. The ratified report described the risks of violating U.S. export control laws in connection with exporting U.S.-origin items to embargoed destinations, including because ZTE had “many technologies and components that came from suppliers in the U.S., [and] therefore, when our export or re-export involves technologies and products of the U.S., they are all monitored and restricted by the U.S. Government” and require that export or reexport licenses be sought and obtained from the U.S. Government. The report specifically discussed the risks of large civil penalties against ZTE, prison sentences for high-level managers, and placement “on the Blacklist and be[ing] banned from purchasing U.S. products directly or indirectly for a period of time,” and even included specific examples of Chinese companies that had been placed on the “Blacklist” and a Chinese corporate executive who had been sentenced to a long jail term in the U.S. for violating U.S. export control laws.
27. The ratified report also identified and described specific legal constraints on doing business in Iran, the risk of detection the company had already faced through inquiries

from U.S. companies, and a possible strategy for dealing with the growing U.S. export control risks associated with ZTE's rapid expansion of its dealings with U.S.-embargoed destinations. The report then laid out a ZTE "response plan" to, *inter alia*, further standardize the operation of its Iran projects and manage potential risks, including the creation of a number of cross-department project teams or committees with regard to its embargoed projects. The plan specifically named more than 70 individual ZTE employees, from a total of more than 20 different departments, as members of various committees and described the role and responsibilities of each. The plan also established an award of 400,000 Renminbi ("RMB"), or approximately \$64,000, to encourage team members to successfully complete project assignments.

Revisions to and Renewal of the Scheme During the U.S. Government's Investigation

28. ZTE continued its Iran dealings in furtherance of the conspiracy for the remainder of 2011 and into 2012, albeit without implementing or fully implementing the "completely detached business" model in connection with at least the Tamin/Rightel and TCI network contracts. Despite the various schemes and extensive efforts ZTE had used to conceal its expanding Iran business, a news media report about some of its Iranian dealings published in March 2012, and BIS's service of an administrative subpoena on its U.S. affiliate, ZTE USA, Inc., led ZTE to slow its unlawful shipments to Iran. Those shipments continued into May 2012, at which time ZTE suspended them, while continuing to provide ongoing services and support through ZTE Parsian.
29. Shortly thereafter, during the summer of 2012, ZTE required all employees involved in Iranian sales to sign a non-disclosure agreement ("NDA") relating to ZTE's operations in Iran. Any employee in breach of the NDA would face a penalty of 1 million RMB (or approximately \$150,000), payable to ZTE.
30. Subsequently, in the summer of 2013, ZTE executives, including a team of in-house attorneys, traveled to Iran to assess the state of ZTE's Iranian projects and to determine whether ZTE should resume its shipments to Iran. Upon its return from Iran in or around August 2013, the ZTE legal team, including the Executive Vice-President who headed ZTE's Legal Department, was not in favor of resuming shipments to Iran.
31. Despite the views of ZTE's legal team, in November 2013, following a meeting of senior managers chaired by its then-CEO, ZTE made plans to resume transshipments to Iran. The head of the ZTE Parsian office in Iran was directed to find an established third party with a history of selling to Iran that would agree to sign contracts with Iranian entities directly, enter into a separate contract with ZTE, and then act as shipper to Iran at a reasonable price to ZTE. A committee of ZTE employees was formed to find a willing third party. This strategy was designed to enable ZTE to have a low profile in the transactions while resuming its shipments to Iran in violation of U.S. export control laws, including of the U.S.-origin goods without which the ZTE equipment could not function as called for under their Iranian network contracts. ZTE would in effect begin using a strategy closer to the "Detached Model" discussed in its "Proposal for Import and Export

Control Risk Avoidance,” described in Paragraph 25, *supra*. Under that model, ZTE would insulate itself, at least on paper, from dealings with embargoed destinations by using other Chinese entities as go-betweens with ZTE’s Iranian customers.

32. ZTE solicited and selected an established Chinese company, Chinese Company A (“CCA”), based in Yixing, China, to serve as its intermediary in furtherance of the conspiracy. On or about November 20, 2013, a Power of Attorney was signed by ZTE’s then-Chairman that authorized a senior ZTE manager in Beijing to sign contract agreements with CCA.
33. Soon after, on or about December 2, 2013, ZTE Corporation and CCA signed a “Telecommunication Equipment Framework Agreement (System Equipment),” purportedly for domestic Chinese sales. CCA then signed a separate agreement with TCI in or around February 2014, to supply equipment in three Iranian provinces to further the network project described in Paragraphs 12-13, *supra*. The February 2014 agreement was valued at approximately \$95.2 million and provided that it would be fulfilled pursuant to three purchase orders. The agreement specifically identified each of the purchase orders by its amount (in Euros) and listed the Iranian provinces that would be covered by the supplies provided under each of the purchase orders. The contract also specified that a letter of credit would be issued for each purchase order “in accordance with pro forma invoices issued by the supplier.”
34. CCA then entered into a contract with Tamin/Rightel in March 2014, to supply GSM/UTRAN network equipment to further the network project described in Paragraph 11, *supra*. This contract, valued at approximately \$94.3 million, included annexes setting unit prices and provided that Tamin/Rightel could issue purchase orders without any prior quotation. It also provides that Tamin/Rightel had to open an irrevocable letter of credit in ZTE’s favor upon ZTE’s submission of a pro forma invoice in accordance with a breakdown of the contract prices, subject only to a three working-day comment period. As part of this March 2014 contract, spare parts would be provided to Tamin/Rightel in Iran for a period of ten years.
35. Using CCA to implement its revised scheme, ZTE resumed shipments to Iran for the Tamin/Rightel and TCI projects in furtherance of the conspiracy no later than in or around July 2014. ZTE aggressively pursued completion of these contracts. By in or around October 2014, ZTE had delivered its first batch of equipment to Tamin/Rightel and anticipated that the remaining equipment would be delivered within a month.
36. Furthermore, ZTE’s founder and then-Chairman met with Iranian Government officials and Tamin/Rightel’s CEO on or about November 25, 2014, in order to further rebuild Tamin/Rightel’s strategic cooperation with them, increase ZTE’s Iranian market share, and highlight ZTE’s experience in operating and maintaining the Tamin/Rightel network. Similarly, on or about March 2, 2015, ZTE met with the CEO of TCI.
37. ZTE continued to make or direct shipments to Iran under the Tamin/Rightel and TCI contracts in knowing violation of the U.S. embargo through at least January 2016.

38. ZTE took a number of steps designed to reduce the risk of detection of its renewed and continuing shipments to Iran. Whereas ZTE previously had routinely used “YL” as code for Iran, it now substituted the country of Qatar as code for Iran. Still unsure how the media had learned in March 2012, of some of its dealings with Iran, ZTE also implemented procedures to silo the information within the company. For example, by 2014, ZTE’s sale system omitted the names of its customers when those customers were Iranian; all other customers’ names remained in the system. ZTE also omitted its logo from items or documentation sent to Iran, including shipping boxes and correspondence.
39. By January 2016, however, ZTE had become increasingly concerned that the U.S. Government’s criminal/administrative investigation was progressing. In an effort to further the conspiracy and prevent detection by the U.S. Government, ZTE Corporation’s then-CEO met with a group of four ZTE Corporation executives in or around January 2016. At that meeting, a senior executive was tasked with ensuring that the forensic accounting firm that ZTE had hired, at its outside counsel’s request, in connection with the U.S. Government’s investigation was prevented from discovering ZTE’s resumption of shipments to Iran during the U.S. Government’s investigation.
40. As a result, a 13-member team dubbed the “Contract Data Induction Team” was formed. The team members were ordered to delete from ZTE databases any references to shipments of U.S.-origin items to Iran. These deletions were designed to conceal ZTE’s post-March 2012 sales to Iran from the forensic accounting firm and, thus, its outside counsel and the U.S. Government. ZTE knew that the results of forensic accounting firm’s work were to be, and did in fact become, the basis of statements and presentations made to U.S. law enforcement through ZTE’s outside counsel. Once the deletions were made, ZTE gave the forensic auditor access to a falsified version of its database that made no mention of exports to Iran after 2012. ZTE had, in fact, continued shipments to Iran in violation of the Regulations and U.S. export control laws into at least in or around January 2016.
41. Moreover, emails from all Contract Data Induction Team members were auto-deleted on a daily basis until in or around March 2016, in order to conceal their cover up efforts. Furthermore, ZTE obtained a NDA from each member of the Contract Data Induction Team. Any team member in breach of the NDA would face a penalty of 1 million RMB (or approximately \$150,000), payable to ZTE.
42. As alleged in Paragraph 7, *supra*, none of the transactions and activities alleged herein were authorized by BIS or OFAC.
43. In so doing, ZTE Corporation and ZTE Kangxun violated Section 764.2(d) of the Regulations, for which they are jointly and severally liable.

Charges 2 - 284: 15 C.F.R. § 764.2(e) – Acting with Knowledge of a Violation in Connection with Unlicensed Shipments of Telecommunications Items to North Korea via China

44. BIS re-alleges and incorporates herein the allegations set forth in Paragraphs 1- 43, *supra*.
45. On 283 occasions between on or about February 10, 2010, and on or about June 25, 2015, ZTE ordered, bought, stored, used, sold, transferred, and/or forwarded telecommunications equipment subject to the Regulations, with knowledge that a violation of the Regulations had occurred or was about or was intended to occur in connection with these items.
46. ZTE procured parts and components subject to the Regulations, classified under Export Control Classification Numbers 3A001, 3A991, 4A994, 5A002, 5A991, 5A992, and controlled for national security, encryption, or anti-terrorism reasons, as well as items designated as EAR99. ZTE incorporated these parts and components into telecommunications items that ZTE transferred and/or forwarded from its facilities in China to employees or agents of the Korea Posts and Telecommunications Co., a North Korea state-owned entity, knowing that the items would be driven to North Korea without the required U.S. Government authorization.
47. Pursuant to Section 746.4 of the Regulations, a BIS license was required at all times pertinent hereto to export or reexport any item subject to the Regulations to North Korea. ZTE knew of the long-standing and well-known U.S. embargo against North Korea, including that U.S. Government authorization was required to ship the items to North Korea. For example, in its “Report Regarding Comprehensive Reorganization and Standardization of the Company Export Control Related Matters,” alleged in further detail in Paragraph 26, *supra*, ZTE specifically discussed that under “U.S. export control laws, our company must apply for reexport licenses when exporting controlled items to these five major embargoed countries—Iran, Sudan, North Korea[,], Syria, and Cuba.” The report, which had been ratified and signed by ZTE’s CEO and three other high-ranking executives, also specifically discussed the fact that violations of U.S. law in connection with North Korea transactions (or transactions involving any of the other U.S.-embargoed destinations) would subject ZTE to “large” civil penalties, its “high-level managers [could] face prison sentences in a criminal case,” and ZTE could be “placed on the Blacklist” and “banned from purchasing U.S. products directly or indirectly for a period of time.” The report also noted that ZTE faced additional legal risks because high-level company managers “are also [on] the board of directors of our subsidiary company in the U.S.”
48. ZTE also knew that items to be used in the project were U.S.-origin and subject to the Regulations because, *inter alia*, its U.S. subsidiary, ZTE USA, Inc., signed a Framework Agreement for Chipset Procurement with a major U.S.-based supplier, in January 2011. This agreement modified an existing long-term supply contract with that supplier, which specified that the products and certain technical information provided under the supply

contract were subject to U.S. export control laws.

49. In so doing, ZTE Corporation and ZTE Kangxun committed 283 violations of Section 764.2(e) of the Regulations, for which they are jointly and severally liable.

Charges 285 - 380: 15 C.F.R. § 764.2(h) – Evasion

50. BIS re-alleges and incorporates herein the allegations set forth in Paragraphs 1- 49, *supra*.

51. Between in or around 2014 and on or about April 6, 2016, ZTE engaged in conduct prohibited by, or failed to engage in conduct required by, the Regulations, with intent to evade the Regulations. ZTE made knowingly false and misleading representations and statements to BIS or other U.S. law enforcement agencies during the course of an investigation or other action subject to the Regulations, and failed to correct those representations and statements, which were continuing in effect, as required by the Regulations. ZTE also destroyed, deleted, or concealed documents and information material to the U.S. Government's parallel criminal/administrative investigation of ZTE, and altered or failed to retain other documents relating to transactions and activities subject to Regulations.

52. This course of evasive conduct was designed, *inter alia*, to prevent BIS and other U.S. law enforcement agencies from detecting ZTE's continuing conspiracy to violate the U.S. trade embargo against Iran and related provisions of the Regulations, and to reduce ZTE's exposure for its extensive, long-running violations of U.S. law.

53. At all times pertinent hereto, the Regulations prohibited any person from making any false or misleading representation, statement, or certification, or falsifying or concealing any material fact, either directly to BIS or an official of any other United States agency, or indirectly through any other person, "[i]n the course of an investigation or other action subject to the EAR" or "[f]or the purpose of or in connection with effecting an export, reexport or other activity subject to the EAR." 15 C.F.R. § 764.2(g)(1). All such representations, statements, and certifications were "deemed to be continuing in effect." 15 C.F.R. § 764.2(g)(2). Moreover, any person who had either directly or through another indirectly made a false or misleading representation, statement, or certification was required to notify "BIS and any other relevant agency, in writing," of the actual material facts and circumstances. *See id.*

54. In addition, Part 762 of the Regulations imposed detailed recordkeeping requirements relating to all transactions subject to the Regulations, with a retention period of a minimum of five years. *See* 15 C.F.R. §§ 762.1-762.5. Furthermore, no records formally or informally requested by BIS or another U.S. Government agency could be destroyed or disposed of without the written authorization of BIS and other agencies involved, including documents that had been retained longer than the minimum retention period. *See* 15 C.F.R. §§ 762.6-762.7.

55. During a series of meetings between on or about August 26, 2014, and at least on or about January 8, 2016, ZTE represented and stated to BIS special agents and/or to other federal law enforcement agents and agency officials, that the company had previously stopped shipments to Iran as of March 2012, and was no longer violating U.S. export control laws. In doing so, ZTE acted through outside counsel who was representing ZTE in connection with the U.S. Government's investigation. ZTE's outside counsel was unaware that the representations and statements that ZTE had given to counsel for communication to the U.S. Government were false and misleading. In addition, and in advance of counsel's meetings with the U.S. Government, senior executives or managers at ZTE had reviewed the representations and statements made by defense counsel on the company's behalf and approved them knowing that they were false and misleading.
56. Contrary to this series of representations and statements, ZTE had, in fact, continued to violate the U.S. embargo against Iran and related provision of the Regulations during 2014-2016.
57. ZTE also took other evasive steps, as alleged in further detail in Paragraphs 28-38, *supra*, in connection with its Iran transactions, including using "Qatar" as code for "Iran" in documents relating to Iranian transactions, omitting the names of customers from its sales system when those customers were Iranian, and removing or avoiding the use of its logo from or on items, boxes, or documents sent to Iran. ZTE also failed to retain, or produce documents relating to various Iran transactions, including, *inter alia*, purchase orders, pro forma invoices, (commercial) invoices, credit advices or other account or financial records, bills of lading, waybills, and/or correspondence relating to the Tamin/Rightel and TCI contracts and related allegations detailed in Paragraphs 28-38, *supra*.
58. In addition to these repeated, continuing false and misleading representations and statements, ZTE sought to falsify and conceal facts that were material, and in fact central, to the U.S. Government's investigation. As set forth in further detail in Paragraphs 39-41, *supra*, ZTE 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 relating to any transactions or other activities relating to ZTE's Iran business that post-dated March 2012; deleting on a nightly basis all of the team's emails to conceal the team's activities; and requiring each of the team members to sign a non-disclosure agreement prohibiting any disclosure relating to the ZTE transactions and activities that the team was tasked with hiding, subject to a penalty of 1 million RMB (or approximately \$150,000) payable to ZTE if it determined that a disclosure occurred.
59. ZTE's evasive course of conduct also was designed to enable ZTE to evade the Regulations in connection with its addition to BIS's Entity List, Supplement No. 4 to Part 744 of the Regulations, on March 8, 2016, by which BIS imposed a comprehensive

license requirement relating to ZTE pursuant to Section 744.11 of the Regulations and Supplement No. 4. As of that Entity List listing, a BIS license was required in connection with any transaction in which items subject to the Regulations were proposed for export, reexport, or transfer (in-country) to ZTE, or with regard to any other transaction in which ZTE was to act as a purchaser, intermediate consignee, ultimate consignee, or end user of items subject to the Regulations. Any such license application was subject to a license review policy of a presumption of denial. The effect of ZTE's Entity List listing was modified through the issuance of a temporary general license on March 24, 2016, that restored ZTE to the *status quo ante* that existed just prior to the listing. Thus, for example, an export to ZTE that would not have required a license or was authorized by a license exception as of March 7, 2016, could occur per the temporary general license without application of the license requirement or license review policy imposed as part of the listing. As a result of its evasive conduct, ZTE was able, for example, to renew its receipt of exports, reexports, and/or transfers (in country) of items subject to the Regulations that would not have been permitted under the terms of ZTE's addition to the Entity List on March 8, 2016.

60. ZTE did not notify BIS (or the other agencies) of the false and misleading nature of its prior representations and statements until doing so, via outside counsel, on or about April 6, 2016.
61. In so doing with intent to evade the Regulations, ZTE Corporation and ZTE Kangxun committed 96 violations of Section 764.2(h) of the Regulations, for which they are jointly and severally liable.

* * * * *

Accordingly, ZTE Corporation and ZTE Kangxun are hereby notified that an administrative proceeding is instituted against them pursuant to Section 13(c) of the Act and Part 766 of the Regulations for the purpose of obtaining an order imposing administrative sanctions, including any or all of the following:

- The maximum civil penalty allowed by law of up to the greater of \$289,238 per violation,⁶ or twice the value of the transaction that is the basis of the violation;⁷
- Denial of export privileges;
- Exclusion from practice before BIS; and/or

⁶ See 15 C.F.R. § 6.4(b)(4). This amount is subject to annual increases pursuant to the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015, Sec. 701 of Public Law 114-74, enacted on November 2, 2015.

⁷ See International Emergency Economic Powers Enhancement Act of 2007, Pub. L. No. 110-96, 121 Stat. 1011 (2007).

- Any other liability, sanction, or penalty available under the law.

If ZTE Corporation or ZTE Kangxun fails to answer the charges contained in this letter within 30 days after being served with notice of issuance of this letter, that failure will be treated as a default. *See* 15 C.F.R. §§ 766.6 and 766.7. If ZTE Corporation or ZTE Kangxun defaults, the Administrative Law Judge may find the charges alleged in this letter are true without a hearing or further notice to ZTE Corporation and ZTE Kangxun. The Under Secretary of Commerce for Industry and Security may then impose up to the maximum penalty for the charges in this letter.

ZTE Corporation and ZTE Kangxun are further notified that they are entitled to an agency hearing on the record if they file a written demand for one with its answer. *See* 15 C.F.R. § 766.6. ZTE Corporation and ZTE Kangxun are also entitled to be represented by counsel or other authorized representative who has power of attorney to represent them. *See* 15 C.F.R. §§ 766.3(a) and 766.4.

The Regulations provide for settlement without a hearing. *See* 15 C.F.R. § 766.18. Should ZTE Corporation and ZTE Kangxun have a proposal to settle this case, ZTE Corporation and ZTE Kangxun or their representative should transmit it to the attorney representing BIS named below.

ZTE Corporation and ZTE Kangxun are further notified that under the Small Business Regulatory Enforcement Flexibility Act, ZTE Corporation and ZTE Kangxun may be eligible for assistance from the Office of the National Ombudsman of the Small Business Administration in this matter. To determine eligibility and get more information, please see: <http://www.sba.gov/ombudsman/>.

The U.S. Coast Guard is providing administrative law judge services in connection with the matters set forth in this letter. Accordingly, ZTE Corporation's and ZTE Kangxun's answers must be filed in accordance with the instructions in Section 766.5(a) of the Regulations with:

U.S. Coast Guard ALJ Docketing Center
40 S. Gay Street
Baltimore, Maryland 21202-4022

In addition, a copy of ZTE Corporation and ZTE Kangxun's answer must be served on BIS at the following address:

Chief Counsel for Industry and Security
Attention: Adrienne Frazier, Esq. and Brian Volsky, Esq.
Room H-3839
United States Department of Commerce
14th Street and Constitution Avenue, N.W.
Washington, D.C. 20230

Adrienne Frazier and Brian Volsky are the attorneys representing BIS in this case; any communications that ZTE Corporation and ZTE Kangxun may wish to have concerning this matter should occur through them. They may be contacted by telephone at (202) 482-5301.

Sincerely,

Douglas R. Hassebrock
Director
Office of Export Enforcement