United States Department of State

Bureau of Political-Military Affairs
Directorate of Defense Trade Controls

Washington, D.C. 20522-0112

Draft Charging Letter

Mr. Larry Hunter
Executive Vice President, General Counsel and Secretary
The DIRECTV Group
2250 East Imperial Hwy
El Segundo, CA 90245-0956

Mr. Dean Manson
General Counsel
Hughes Network Systems
11717 Exploration Lane
Germantown, MD 20876-2700

Re: Investigation of The DIRECTV Group, Inc. and Hughes Network Systems, Inc. regarding unauthorized exports to China, India, Turkey, South Korea and South Africa.

Dear Mr. Hunter:

(1) The Department of State ("Department") charges The DIRECTV Group ("DTV") and Hughes Network Systems, Inc. ("HNS") (hereinafter "Respondents") with violations of the Arms Export Control Act ("Act") and the International Traffic in Arms Regulations ("ITAR" or "Regulations") in connection with the unauthorized export of technical data, defense services and defense articles to foreign person employees, to include those of proscribed countries, and other matters as set forth herein concerning the Respondents' business activities. Fifty-six (56) violations are alleged at this time. The essential facts constituting the alleged provisions involved are described herein. The Department reserves the right to amend this draft charging letter (See 22 C.F.R. § 128.3 (a)), including through a revision to incorporate additional charges stemming from the same misconduct of the Respondents in these matters. Please be advised that this is a draft charging letter to impose debarment or civil penalties pursuant to 22 C.F.R. § 128.3.

Part I – Relevant Facts

Jurisdictional Requirements

(2) Respondents are corporations organized under the laws of the State of Delaware.

(3) Respondents are and were during the period covered by the offenses set forth herein engaged in the manufacture and export of defense articles and defense services and so registered with the Department of State, Directorate of Defense Trade Controls ("DDTC") in accordance with Section 38 of the Act and § 122.1 of the Regulations.

(4) Respondents are U.S. persons within the meaning of § 120.15 of the ITAR and, as such, are subject to the jurisdiction of the United States, in particular with regard to the Act and the Regulations.

(5) Respondents identified in their voluntary disclosure to this office certain foreign persons within the meaning of § 120.16 of the Regulations who had unauthorized access to ITAR controlled technical data, defense services and defense articles.

(6) The commodities constituting the violations outlined below are designated as controlled under Category XIII (b) and Category VI (a) of the ITAR.[1] The defense services and technical data provided by HNS are covered under Category XIII (k). Further, HNS exported to military end-users modified software and hardware products that were subject to the ITAR as designated in § 120.3 of the ITAR.

(7) Shanghai Hughes Network Systems Co., Ltd, ("Shanghai Hughes"), the Chinese Army, Navy, and Air Force, Chinese Ministry of Public Security, China Electronics System Engineering Corp ("CESEC"), China

[1] Category XIII covers, inter alia, military cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems, including equipment and software for tracking, telemetry and control (TT&C) encryption and decryption, to include ancillary equipment specifically designed or modified.

Launch and Tracking Control General ("CLTC"), Hughes Escorts Communications Ltd. ("HECL"), Hughes Software Systems Limited ("HSS"), ITI Limited ("ITI"), Turk Telekomunikasyon A.S., Mercury Corporation, Korea Telekom, Telkom, Nanoteq and other persons so identified below are all foreign persons within the meaning of § 120.16 of the Regulations.

Background:

(8) In 1998, the Department of State and the Department of Justice (DOJ) initiated separate independent investigations of Hughes Electronics Corporation (now DTV) and Hughes Space and Communications (now Boeing Satellite Systems) concerning violations of the Arms Export Control Act and the International Traffic in Arms Regulations in connection with their misconduct related to the January 1995 failed launch of the Long March 2E rocket carrying the APSTAR II spacecraft, the February 1996 failed launch of the Long March 3B rocket carrying the INTELSAT 708 spacecraft, and other matters concerning their business activities in China.

(9) On March 4, 2003, the Department signed a Consent Agreement imposing a $32,000,000 (thirty-two million dollar) fine on Hughes Electronics Corporation ("HEC") and Boeing Satellite Systems, Inc., ("BSS") in a civil settlement of charges against them for violations of the AECA and the ITAR.[2]

(10) The Order implementing the terms and conditions of the Consent Agreement called for HEC to pay $20,000,000 (twenty million dollars) cash penalty. HEC was also to apply an additional $2,000,000 (two million dollars) to offset costs associated with remedial compliance measures required by the Consent Agreement.

(11) The Consent Agreement required HEC to appoint a Special Compliance Official ("SCO") who would be responsible for oversight of HEC's ITAR regulated activities particularly in China and the countries of the former Soviet Union. This SCO was tasked with "ensuring that HEC (now DTV) performs its responsibilities in a timely and satisfactory manner

[2] BSS is not a party to this current matter.

as required by the Consent Agreement." Further, the SCO was to be kept fully informed by DTV's General Counsel and Director of Export Compliance, and actively engaged in overseeing all activities related to compliance with the Regulations, and the Act, as well as the terms and conditions of the Consent Agreement.

(12) In the Consent Agreement, HEC (now DTV) acknowledged and accepted, among other things, that the definition of "defense services" in the Regulations is well established and clearly understood by them as setting out responsibilities and requirements which are binding as a matter of law and regulation on them.[3]

(13) On May 10, 2004, DTV submitted an initial notification of possible violations of the ITAR with respect to its wholly owned subsidiary, HNS. DTV advised this office that concerns were first raised in December 2003 when DTV became aware of potential improper dealings with military organizations in India. As a result of these concerns DTV began an investigation into this matter and ultimately, in January 2004, developed sufficient information to provide a preliminary disclosure about possible ITAR violations with respect to India.

(14) On May 14, 2004, DDTC informed DTV that DDTC had imposed a policy of denial to all applications for licenses or other requests for written approvals submitted by, or on behalf of, or otherwise directly or indirectly involving HNS, based on their violation of the terms of the Consent Agreement.

(15) On June 9, 2004, DTV submitted to DDTC its voluntary disclosure pertaining to unauthorized exports of technical data and defense services to foreign persons in China, India, Turkey and South Korea. DTV additional reports dated July 1, 2004, July 15, 2004, August 31, 2004, and October 29, 2004 supplemented the initial disclosure and advised of additional unauthorized exports to South Africa and Taiwan.[4]

---

[3] March 4, 2003 Consent Agreement between the Department and HEC (paragraph 3).

[4] On October 29, 2004, DTV submitted another supplemental report concerning exports of defense services to Taiwan which will be addressed in the remedial compliance measures imposed in a Consent Agreement to this matter.

(16) HNS manufactures and exports commercial telecommunications products, including Very Small Aperture Terminals ("VSATs") and related ground-segment equipment, for use in satellite-based telecommunications networks. The products and related technology are generally controlled by the Department of Commerce under the Export Administration Regulations ("EAR"). However, HNS's internal investigation concluded that HNS had engaged in numerous unauthorized exports of defense articles, technical data and defense services to foreign military organizations in China, India, Turkey, South Korea, and South Africa by providing defense services or modifying the standard HNS products specifically for these customers.

(17) The primary VSAT systems that are subject of this matter are: TES systems, which are two-way VSAT systems designed primarily for voice transmissions; Personal Earth Stations ("PES"), which are two-way systems designed primarily for data transmissions; Hybrid Earth Stations ("HES"), which combine TES and PES systems to provide a wider range of voice and data capabilities; and DirecPC/Enterprise Edition ("DPC/EE"), which are one-way, receive only remotes for receptions of Internet Protocol ("IP") services via satellite.

(18) The TES, PES and HES systems have no encryption capability. However, HNS added a "Test Port" feature in the early 1990s to its commercial TES Channel Units (CUs). The Test Port feature enables a user to connect its own external encryption equipment to the TES product. When an external encryption device is attached via the Test Port, the digitized voice data is routed from the CU for transmission over a satellite network in encrypted form.

(19) In March 1994 HNS submitted a Commodity Jurisdiction request ("CJ") to DDTC. HNS stated, "HNS has determined that the absence of any cryptographic capabilities in the TES eliminated the possibility of control under Category XIII of the ITAR. The TES has no hardware or software with the ability to maintain secrecy of information, which is the basis for control under any of the provisions in Category XIII." HNS further added, "the TES's data stream interface does not include any cryptographic hardware or software, it merely allows the customer to connect its own encryption device to the Channel Unit ("CU"). Whether or not a particular

customer chooses to install its own cryptographic device and use the Channel Unit's data stream interface is entirely a matter of individual customer discretion."

(20) On June 8, 1994, this office issued our finding to CJ 098-94 submitted by HNS stating, "the Department of State had determined that the TES, when the data stream access feature (or interface) is removed or disabled, is subject to the licensing jurisdiction of the Department of Commerce. However, the TES data stream access feature, or data stream interface, or the TES when it incorporates the data stream interface is subject to the licensing jurisdiction of the Department of State." The modifications and defense services provided by HNS, without State Department approval, to its customers to enable them to use third party encryption equipment with HNS TES, violated the ITAR.

(21) HNS standard statement of work ("SOW") for VSAT commercial systems ensures that HNS contracts offer all necessary types of services to sell, install and test the TES with the customer's system, while at the same time providing HNS and the customers with flexibility to permit HNS to perform activities necessary to enable HNS' equipment to operate with the end-user's applications. The contracts entered with military entities identified below used this standard SOW terminology as to providing "services" to its customers.

(22) As detailed below, HNS exported to military end-users in China, India, South Korea, Turkey and South Africa without State Department authorization, defense services and technical data related to the interfacing of HNS' VSAT systems with defense articles covered by USML. HNS's provision of the technical data and defense services provided the foreign recipients with a new capability to enhance secure satellite communications. Further, in the course of the transactions with China and India, HNS made unauthorized proposals to export defense articles and defense services to proscribed countries.

Part II – Unauthorized Exports to Proscribed Countries

China:

(23) Between 1993 and 2003, HNS entered into a series of contracts for the sale of VSAT networks, additional remote units and spare parts for end-use by China's Army, Air Force, Navy and China Satellite Launch and Tracking Control General ("CLTC"). HNS also sold VSAT networks to the Chinese Ministry of Public Security.

(24) HNS conducted operations in China through its wholly owned subsidiary, Hughes Network Systems (Beijing) Co. Ltd. ("HNS China"), and through a partially owned joint venture, Shanghai Hughes Network Systems Co. Ltd. ("Shanghai Hughes"). HNS and its Chinese affiliates provided unauthorized defense services and product modifications to these Chinese end-users in connection with the integration of HNS' equipment with the Chinese end-users' applications, including their external encryption equipment, without State Department approval.

(25) The primary purchaser of HNS' equipment for end-use by the Chinese Army, Air Force, Navy and Ministry of Public Security was China Electronics System Engineering Corp. ("CESEC"). CESEC is operated by the Communications Department of the Chinese military's General Staff Department and served as a procurement agency for the Chinese military and the Ministry of Public Security in these transactions.

(26) Some of the reported end uses for these systems are (a) the transmission of weather data to remote locations and e-learning courses to personnel; (b) transmission of air traffic control data between remote radar tracking stations and air force bases throughout China; (c) provision of telephone connectivity among remote tracking stations in order to facilitate the tracking and monitoring of satellite launch vehicles; and (d) provision of voice and data communications between various police outposts throughout China.

(27) Between 1997 and 2002, HNS provided technical services and support to the Chinese customers identified above in an effort to resolve a series of technical problems associated with the customer's use of external

encryption equipment with HNS' TES systems. In some cases, HNS modified components of its TES CUs to address these encryption interface problems.

(28) The Chinese Army, the Air Force, CLTC and the Ministry of Public Security sought to use HNS' equipment in connection with their own external encryption devices in order to transmit secure communications over the VSAT networks. HNS stated that they did not have specific information regarding the manufacturers or models of the encryption equipment used by the Chinese military customers. However, HNS understood that the encryption boxes were supplied internally by agencies of the Chinese military.

(29) HNS and HNS China engineers participated in a series of tests using HNS' equipment together with the encryption boxes used by the Chinese Army, Air Force and Ministry of Public Security. Between January and December 1998, representatives of the Chinese customers brought their encryption boxes to the test facility at HNS' China's Beijing office on seven occasions to conduct those tests with HNS' equipment. On other occasions, HNS' engineers traveled to the customers' facilities to conduct the tests on-site. These tests involved HNS' engineers observing and analyzing the timing of data transmissions over the interface between HNS' equipment and the customer's encryption device. HNS' engineers provided the Chinese customers with the technical specifications related to the Channel Unit.

(30) HNS' engineers, to address this technical problem, modified the channel unit (CU3), i.e., HNS modified the software code embedded in the programmable read only memory chip on the CU3's auxiliary data card (the "modified ADC"). HNS' engineers provided to the Chinese customers two different versions of the modified chips for testing. It was subsequently determined that the transmission problem was caused by incorrect interface settings in the customers encryption boxes.

(31) In December 1998, HNS' engineers provided the Chinese customers with two technical documents setting forth a comparison of the CU2 and CU3 encryption interfaces and an analysis of the encryption error condition traces. HNS emphasized findings to the customer that point

towards a performance problem within the customer's encryption equipment.

(32) In July 2002, HNS and HNS China engineers assisted the Chinese Air Force in resolving technical problems with the encryption interface that arose in connection with a software upgrade for the single channel version of the TES product. An HNS engineer recommended a possible channel unit configuration to resolve this problem.

(33) An HNS engineer traveled to China on three occasions between July 2002 and September 2002, to conduct an on-site analysis of a transmission problem between the hub and remote locations involving the Chinese Air Force. With the assistance of the HNS engineering team in Germantown, Maryland, they developed and implemented a software solution specifically for this customer to eliminate the system failure of transmission data to remotes connected to air traffic radar stations, thereby freeing up additional bandwidth for use by other components of the network.

India:

(34) On December 22, 2002, HNS entered into a contract for the sale of a TES network to ITI Limited, an Indian telecommunications service provider and equipment integrator, for end-use by the Indian Army. HNS and its Indian affiliates provided software modifications and technical support to the integration of HNS equipment with external encryption equipment provided by ITI without authorization from the Department.

(35) Hughes Escorts Communications, Ltd. ("HECL") based in India, is a joint venture between HNS and Escorts Ltd that provides VSAT satellite communications solutions and services to commercial and government end-users in India.

(36) On May 19, 2000, the Government of India Ministry of Defense ("GOI/MOD") issued a Request for Proposals ("RFP") seeking bids for the establishment of a transportable VSAT network for use by the Indian Army. The RFP required that the VSAT interface with external encryption units to be produced under a separate RFP.

(37) In August 2000, HECL submitted a proposal to the GOI/MOD, which included designs for defense articles, including vehicle-based transportable remote terminals protected from nuclear, biological or chemical weapons fallout.

(38) The GOI/MOD eventually awarded this contract to ITI. ITI subsequently entered into a subcontract with HNS in December 2002, for the purchase of TES network management equipment, remote terminals, spare parts and related services. As the prime contractor, ITI was responsible for integrating HNS' TES equipment with external encryption devices and delivering both products to the Indian Army.

(39) Between June and December 2002, HNS engineers participated in technical discussions and email exchanges with HNS and HECL engineers in India regarding this project, and conducted some of the tests and analyses of HNS equipment in Germantown, Maryland, to ensure that the TES equipment could function effectively with ITI's external encryption devices for the transmission of encrypted communications of the Indian Army's network.

(40) As a result of these tests, two problems arose with regard to the interface between the TES equipment and the encryption boxes. To address these issues a team of HNS and HECL engineers in India and HNS engineers in Maryland developed a software solution that permitted the TES equipment to conform to the requirements of the encryption box.

Part III - Unauthorized Exports to Turkey, South Korea, and South Africa

Turkey:

(41) In November 1996, HNS entered into a contract with Turk Telekom to provide TES communications network for end-use by the Turkish MOD. The system sold to the Turkish MOD was used for transmitting voice communications among the troops deployed throughout the country and also to transmit data communications for official military use.

(42) Pursuant to Turkish MOD requirements, HNS modified its TES terminal by adding protective cases to its standard terminal equipment. Further, in 1997, HNS conducted tests at their Germantown facility with Turkish MOD's encryption equipment to determine the ability of HNS' equipment to interface with such external equipment. HNS also performed tests and upgraded software that operates the HNS equipment for the Turkish MOD to address issues presented during the implementation and operation of the TES network. HNS also provided a number of training sessions to the MOD personnel at the Germantown facility and in Turkey with respect to the use and operation of the TES network system and provided the MOD with technical specifications and assembly instructions for the TES remote terminal equipment.

South Korea:

(43) In 2001, HNS sold a TES unit to the South Korean Navy to enable voice transmissions for ship-to-ship and ship-to-shore communications. In August 2001, HNS entered into a contract with Mercury Corporation (Mercury), a South Korean company involved in integrating access devices, data communication, transmission equipment and networking. Telekom is the leading telecommunications service provider in South Korea. HNS provided to the South Korean Navy, Mercury and Telekom unauthorized technical assistance, defense services, software modifications and performed certain installation, testing and configuration services at naval bases in South Korea, including certain testing and trouble shooting activities on board naval vessels.

(44) In 1999, HNS provided TES system equipment to the South Korean Navy to evaluate during a pilot phase. During this pilot phase HNS engineers visited South Korea on three occasions. An HNS engineer provided advice to the Korea Telecom engineer on how to configure the TES software to achieve the desired transmission rate for the encryption system.

(45) In the latter part of 2001, HNS engineers on two occasions performed testing and provided modifications for TES equipment onboard a South Korean Naval vessel to shorten the time to complete a call utilizing the TES equipment.

(46) In May 2002, the South Korean Navy found a problem with the audio conference function of the TES system in those cases when external encryption equipment was used during a conference call. As a result, in October 2002, a Mercury engineer visited the HNS facility in Germantown for two weeks and worked with HNS' engineers to test telephones and switches and wrote a release note describing the new feature added to the TES software specifically for the South Korean Navy.

South Africa:

(47) On November 22, 2000, HNS exported without State Department authorization four Modified ADCs to the Embassy of the Republic of South Africa, Washington, D.C. The ADC serves as an interface port for connecting external equipment, such as encryption devices, to the TES remote terminals. The South African Embassy subsequently exported the Modified ADCs to South Africa's Department of Foreign Affairs (DOFA) for testing and evaluation.

(48) DOFA subsequently contracted with two South African companies, Telkom SA Ltd (Telkom) and Nanoteq, to provide telecommunications services and integration services in connection with the TES system, as well as to provide external encryption devices for use with HNS' TES system.

(49) Between August 2000 and February 2002, HNS engineers engaged in numerous technical discussions with representatives of Telkom and Nanoteq to resolve problems during the integration and testing of HNS' equipment with Nanoteq's encryption devices. During these discussions HNS engineers provided Telkom and Nanoteq unauthorized technical data regarding the specifications and functionality of HNS' products, and defense services involving technical assistance regarding the use of the Modified ADCs for interfacing the TES equipment with Nanoteq's external encryption equipment.

Part IV - License and Reporting Requirements

(50) § 126.1 (a) of the Regulations provides that it is the policy of the United States to deny, among other things, licenses and other approvals, for defense articles or defense services, including technical data, destined for or originating in certain countries, including China and India.[5]

(51) § 126.1 (e) of the Regulations provides that no sale or transfer and no proposal to sell or transfer any defense service or technical data may be made to any country referred to in this section and that any person who knows or has reason to know of any actual transfer of such services must immediately inform the Directorate of Defense Trade Controls.

(52) § 127.1 (a) (1) of the Regulations provides that it is unlawful to export or attempt to export from the United States any defense article or technical data or to furnish any defense service for which a license or written approval is required without first obtaining the required license or written approval from the Directorate of Defense Trade Controls.

(53) § 127.1 (a) (3) of the Regulations provides that it is unlawful to conspire to export, import, reexport or cause to be exported, imported or reexported, any defense article or to furnish any defense service for which a license or written approval is required without first obtaining the required license or written approval from the Directorate of Defense Trade Controls.

(54) § 127.1 (b) of the Regulations provides that any person who is granted a license or other approval is responsible for the acts of employees, agents, and all authorized persons to whom possession of the licensed defense article or technical data has been entrusted regarding the operation, use, possession, transportation, and handling of such defense article or technical data.

---

[5] On May 13, 1998, the President imposed sanctions described in Section 102 (b) (2) of the Arms Export Control Act ("AECA"), which terminated authority to export to India or conduct sales of defense articles, defense services, or design and construction services under the AECA. This policy stayed in effect until June 20, 2003, when it was rescinded.

(55) § 127.1 (d) of the Regulations provides that no person may willfully cause, or aid, abet, counsel, demand, induce, procure or permit the commission of any act prohibited by, or the omission of any act required by 22 U.S.C. § 2778, 22 U.S.C. § 2779, or any regulation, license, approval, or order issued thereunder.

(56) § 127.2 of the Regulations provides that it is unlawful to use any export document containing a false statement or misrepresenting or omitting a material fact for the purpose of exporting any defense article or technical data or the furnishing of any defense service for which a license or approval is required.

Part VI – Charges

Unauthorized Exports of Technical Data and Defense Services to Proscribed Countries

Charges 1-19

(57) The Respondents violated 22 C.F.R. § 126.1 (e) of the Regulations when it failed to inform DDTC of the unauthorized provision of defense services and technical data in connection with the integration and product modification of HNS' equipment, including the integration of HNS equipment with external third party encryption equipment the Respondents had made, or knew or had reason to know of, to India and China, countries proscribed under § 126.1 (a).

Charges 20-38

(58) The Respondents violated 22 C.F.R. § 127.1 (a) (1) of the Regulations when, without the required license or other approval from DDTC, they provided a defense service and technical data related to VSATs in connection with the integration and product modification of HNS' equipment, including the integration of HNS equipment with external third party encryption equipment to a country proscribed under § 126.1 (a).

Charges 39-41

(59) The Respondents violated 22 C.F.R. § 127.1 (d) of the Regulations when it willfully caused, or aided and abetted, the commission of an act prohibited by 22 U.S.C. 2778, 22 U.S.C. 2779, or any regulation, license, approval or order issued thereunder, by providing defense services and technical data to countries proscribed under § 126.1 (a).

Unauthorized Exports of Defense Articles, Technical Data and Defense Services to Non-Proscribed Countries

Charges 42-52

(60) The Respondents violated 22 C.F.R. § 127.1 (a) (1) of the Regulations when it disclosed without State Department authorization, controlled technical data and provided defense services to South Korea, Turkey and South Africa.

Charges 53-56

(61) The Respondent violated 22 C.F.R. § 127.1 (a) (1) when it exported without State Department authorization four modified Auxiliary Data Cards, defense articles, to the South African Embassy and also provided a defense service and technical assistance to Telkom and Nanoteq.

Part VII - Administrative Proceedings

(62) Pursuant to 22 C.F.R. § 128 administrative proceedings are instituted against the Respondents for the purpose of obtaining an Order imposing civil administrative sanctions that may include the imposition of debarment or civil penalties. The Assistant Secretary for Political Military Affairs shall determine the appropriate period of debarment, which shall generally be for a period of three years in accordance with § 127.7 of the Regulations, but in any event will continue until an application for reinstatement is submitted and approved. Civil penalties, not to exceed $500,000 per violation, may be imposed in accordance with § 127.10 of the Regulations.

(63) A Respondent has certain rights in such proceedings as described in §128, a copy of which is enclosed. Furthermore, pursuant to § 128.11 cases may be settled through consent agreements, including after service of a Draft Charging Letter. Please be advised that the U.S. Government is free to pursue civil, administrative and criminal enforcement for violations of the Arms Export Control Act and the International Traffic in Arms Regulations. The Department of State's decision to pursue one type of enforcement action does not preclude it or any other department or agency of the U.S. Government from pursuing another type of enforcement.

Sincerely,

David C. Trimble
Director
Defense Trade Controls Compliance