LAUNCH SITE SECURITY IN THE PRC

The U.S. satellite manufacturer is responsible for the physical security of U.S. satellites that are exported to the PRC, and for guarding against the unauthorized or illegal transfer of U.S. technology during technical discussions that occur in the PRC. The U.S. Government oversees this function by assigning a representative of the Defense Technology Security Administration (DTSA), now known as the Technology Security Directorate of the Defense Threat Reduction Agency, to the launch site in the PRC.

This Defense Department "monitor" is responsible for ensuring that the satellite manufacturer properly implements a Technology Transfer Control Plan that is intended to provide and maintain protection against the unauthorized transfer of U.S. technology. Defense Department monitors also are required to attend all meetings of a technical nature that may occur between the satellite manufacturer's employees and representatives of the PRC launch provider leading up to and during the launch.

In the course of their duties, Defense Department monitors are required to report regularly to the U.S. Air Force's Space Command and Technology Security Directorate Headquarters on their activities at the launch site, including any security infractions they have detected. According to the Director of the Defense Technology Security Administration and Defense Department monitor reports, these infractions represent instances that require the monitor's attention, but do not necessarily constitute violations of the export license that should be reported to the State Department. The guidance that is provided to Defense Department monitors provides that, should they encounter a security infraction at a launch site, they should first try to work out the problem with the satellite manufacturer's personnel, including its security guard force. If this effort does not result in resolution of the problem to the satisfaction of the monitor, then the monitor is to call Headquarters and advise a supervisor. The supervisor may then call the company to insist that it remedy the security problem.

Defense Department monitors have reported many minor to severe security infractions at launch sites in the PRC. While the Select Committee's limited review has found no witness to confirm that a transfer to the PRC of controlled U.S.

technology has occurred as a result of ineffective launch site security, given the difficulty of proving that an improper transfer has occurred, it cannot be inferred that no such transfer has taken place. Moreover, the security infractions that have been documented demonstrate the potential for technology transfers to occur. Testimony by the Department of Defense on the potential for a technology transfer to occur as a result of access to a satellite in the PRC provides a perspective for considering these security infractions.

The Defense Department concluded that visual or photographic access to a satellite would allow confirmation of the existence of various attributes of a satellite already in the public domain.

With additional, longer-term unguarded access, the Defense Department estimated that a foreign intelligence collector could gain physical access to the satellite and obtain technical information of value regarding the satellite.

U.S. satellite manufacturers hire a security force to provide physical security for a satellite while it is awaiting launch in the PRC. In recent years, only one security guard company has bid on and received contracts to provide this service in the PRC.

The conduct, professionalism, and abilities of that company's personnel have been sharply criticized both by Defense Department monitors and the satellite companies.

Because of the potential that technology transfers associated with the launch of a U.S. satellite in the PRC can occur, it is critical that the Defense Department monitors, the physical security guards, and the satellite manufacturers provide effective protection of U.S. technology associated with launches in the PRC. The Strom Thurmond National Defense Authorization Act for FY 1999 has addressed several of the criticisms received both from inside and outside the Defense Department regarding its monitoring program. However, the Clinton administration has not yet issued regulations to implement the Act.

PROTECTING SENSITIVE INFORMATION AT PRC LAUNCH SITES

The United States relies on a variety of means to protect controlled military-related technology during PRC launches of U.S. satellites. These include bilateral agreements between the United States and the PRC, export licenses for satellites and related technology, the presence of private security guards at PRC launch sites, and monitoring of launch-related activities and communications by U.S. Defense Department representatives.

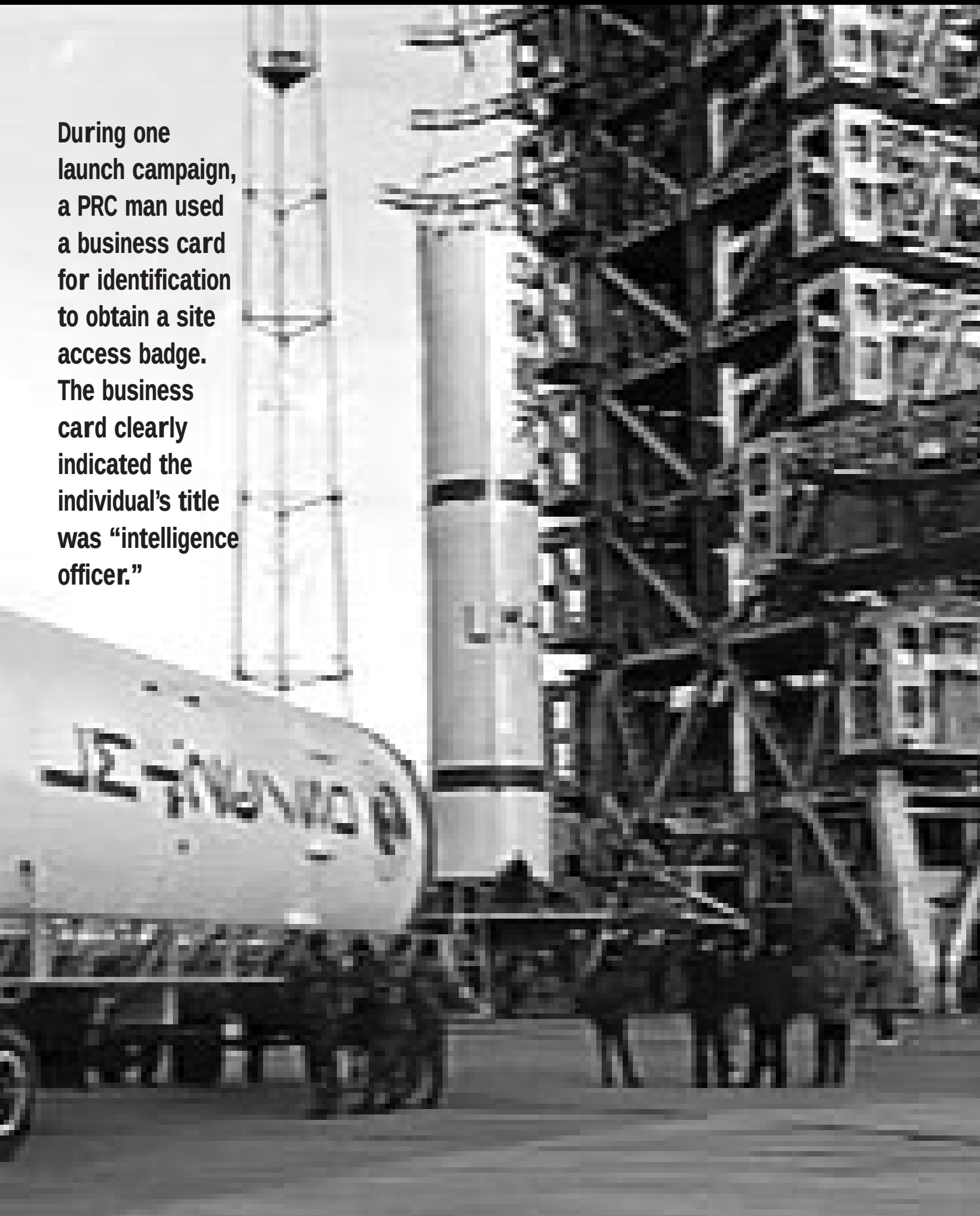
Background

U.S.-PRC Bilateral Agreement

In 1988, prior to authorizing the first launches of U.S. satellites from the PRC, the United States entered into a bilateral agreement with the PRC to prevent unauthorized disclosures of controlled technology. Under that agreement, the PRC agreed to give the United States access to and complete control over the satellite and related information while it is in the PRC for launch. The PRC also agreed not to seek to obtain unauthorized information.[1]

Export Licenses for PRC Launching of U.S. Satellites

Under U.S. law (including the Arms Export Control Act, the International Traffic in Arms Regulations, and regulations issued by the Department of Commerce),[2] a private party wishing to launch a U.S. satellite from the PRC must first obtain an export license to do so. The license limits the access that the PRC can have to the satellite, restricts the information that can be shared with the PRC, and requires that the private



During one launch campaign, a PRC man used a business card for identification to obtain a site access badge. The business card clearly indicated the individual's title was "intelligence officer."

party develop and abide by a plan to protect controlled information from unauthorized disclosure. Private security guards are often hired for this purpose.

Defense Department Monitors

The United States requires that Defense Department representatives must be present at the PRC launch site, and that the expense of these monitors must be borne by the U.S. satellite manufacturer. These Defense Department officials are responsible for overseeing the physical security of the satellite and associated equipment and documents. They are also required to monitor the technical interchange meetings that occur between U.S. and PRC engineers throughout the satellite development and launch campaign.

Each of these mechanisms for protecting sensitive, controlled U.S. information from unauthorized disclosure is discussed in this chapter.

Unauthorized Access Allows Opportunities to Gain Information Concerning U.S. Satellites and Other Controlled Technology

Launch site security is intended to protect controlled military-related technology, including information that could be gleaned from a U.S. satellite and its associated documents, equipment, and technical personnel, against disclosure to the PRC. Protecting controlled information that might be stolen or inadvertently disclosed during the launch or pre-launch period is a demanding and important task.

Efforts to protect U.S.-controlled technology during the launch and pre-launch period in the PRC are complicated by several factors.

First, the launch and related pre-launch activities (often called the "launch campaign") in the PRC take place largely on a PLA military base. The Xichang Space Launch Center, from which many U.S.-manufactured satellites are launched, is located within a PLA military installation. Yet the U.S. satellite manufacturer is required to maintain control over certain portions of the facilities and to make them secure during the time a U.S. satellite and its associated documents and equipment are located there.

Associated Press

Efforts to protect U.S.-controlled technology are complicated by the fact that the launches of U.S. satellites take place on PLA military bases.

Second, U.S. satellite manufacturing companies take considerable amounts of controlled equipment and technical data to the military facility in order to assist them in their work to prepare the satellite for launch. All this controlled information is required to be kept under lock and seal when not in use and protected.

Yet PRC workers have legitimate reasons for having access to some of these U.S. materials at various times, making the security function particularly demanding.

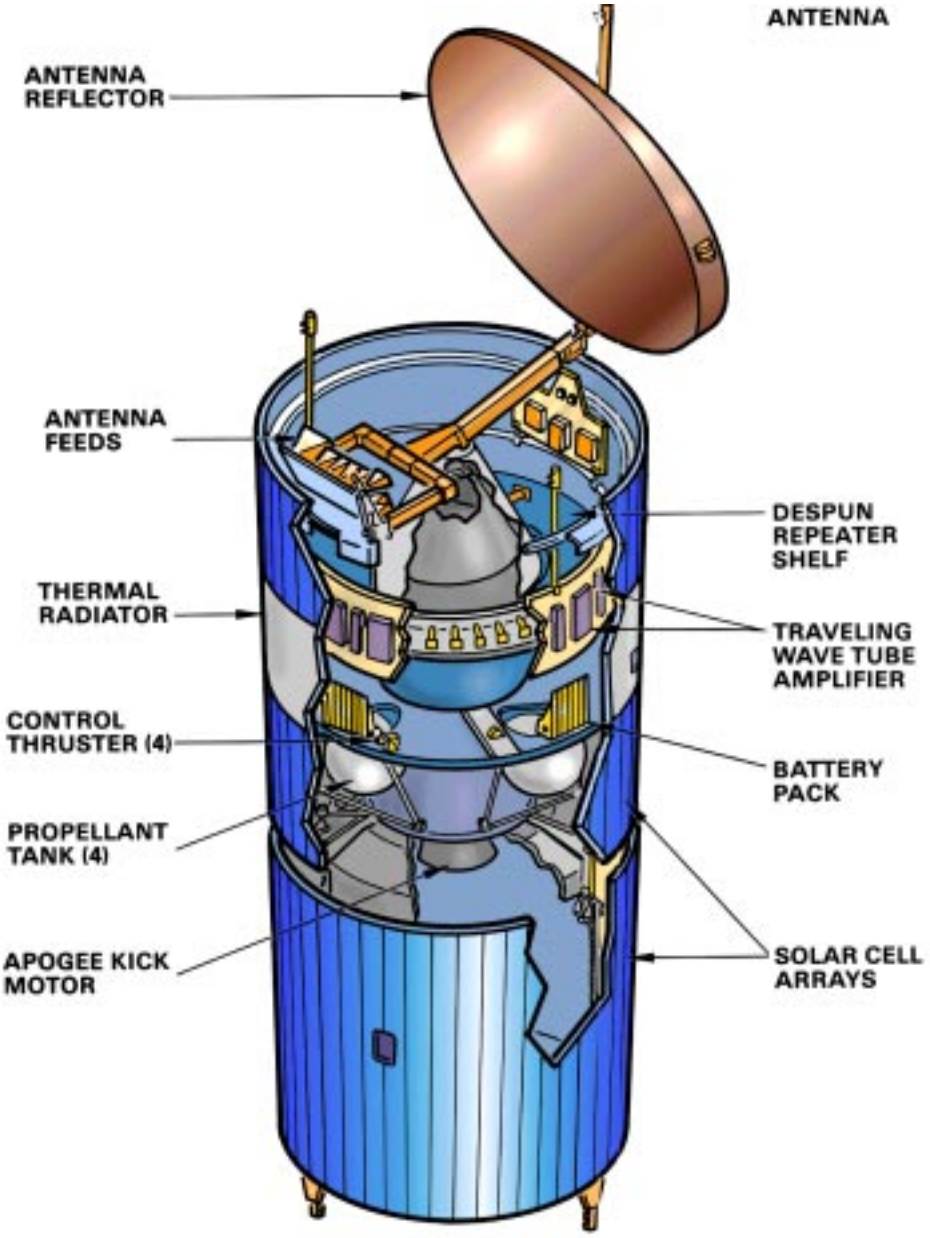
Third, the U.S. engineers and support personnel who accompany the satellite must live and operate far away from home, often under relatively uncomfortable conditions. Some U.S. companies are unaccustomed to doing business in such a demanding security environment.

One satellite manufacturing company security official says that his company takes every possible precaution, but notes that, if the PRC really wanted to monitor everything that went on for the duration of the launch campaign, it probably could easily do so.

Allen Coates

Allen Coates

At the Taiyuan space launch center, underground steam and electrical access tunnels measuring three feet by five feet snake beneath and through buildings where U.S. satellites are prepared for launch.



Access to U.S. communication satellites has undoubtedly permitted the PRC to gain invaluable information about their configuration and design. In as little as two hours, PRC technical personnel can penetrate the interior of a satellite without leaving any traces.

The official also recalls that, during one launch campaign at Xichang when building access badges were being made for local PRC personnel, a PRC man gave the official a business card as identification. The card clearly indicated the PRC man's title was "intelligence officer."[3] The individual was not allowed access to the satellite.

There are indications that the PRC carefully monitors the activities of the U.S. personnel at the launch site. For example, Lockheed-Martin's Director of Security explains that the power facility for the Xichang Space Launch Center is located adjacent to the satellite processing building. At one point when U.S. personnel supplied power to the satellite for testing purposes, a number of PRC personnel emerged from the facility's power building to determine what was happening. This was an indication, in his view, of how closely the PRC was monitoring satellite operations.[4]

Access by the PRC to U.S. communications satellites could permit the PRC to gain information about the configuration and design of Western-manufactured satellites. If the PRC has only visual or photographic access to a U.S. communications satellite — the most common violation of U.S. security guidelines — only information that confirms known capabilities and is already in the public domain may be obtained. If the PRC had unrestricted access to a U.S. communications satellite for at least two hours, the PRC military could gain valuable information that is not otherwise available in the public domain.

The PRC could accomplish even exploitation that penetrated the interior of the satellite, given two hours of time, without leaving any traces.

With this kind of exploitation, the PRC could gain new information about major satellite subsystems, as well as the design and manufacture of each subsystem.

While unmonitored PRC access to a U.S. satellite for more than five or six hours would produce diminishing returns, there is almost nothing about a U.S. satellite that the PRC could not learn from unrestricted access for 24 hours.

Among the reasons the PRC would be interested in exploiting the technology in U.S. communications satellites is to determine the satellite manufacturer's techniques for passive thermal control. Thermal control is critical to satellite life. The PRC would also likely be interested in:

- **Encryption**
- **The materials used in satellites**
- **Engine and propellant data**
- **Electrical design and protection**

Additionally, the PRC could seek to acquire information about the dimensions and part numbers for satellite components or assemblies, as well as dimensional tolerances. Obtaining part numbers could allow the PRC to try to acquire U.S. technology directly from the manufacturer that would improve the performance and provide for longer on-orbit life for PRC satellites.

Launch-related equipment, documents, and personnel accompany the satellite to the PRC military facility for the launch campaign. Technical interchange meetings between U.S. and PRC experts also occur. All of these materials and exchanges relating to controlled technology or information are required to be monitored by the Defense Department.

Unauthorized PRC access to controlled equipment or materials, including blueprints or testing equipment, could benefit the PRC's own military space launch activities.

Unauthorized PRC participation in technical discussions, as well as PRC eavesdropping into technical discussions among U.S. experts, could have similar military benefits to the PRC. For example, the chapters of this Report concerning Loral and Hughes discuss in detail the potential gains to the PRC from technical discussions held in connection with unauthorized failure analyses performed by these companies' experts.

Inadequacy of Current Safeguards

The Select Committee's investigation has identified numerous security lapses in connection with U.S. satellite launches in the PRC that could have provided the opportunity for improper transfers of controlled information.

U.S. policy permitting the launch of U.S. satellites from the PRC rests in large measure on the assumption that companies will comply with legal requirements governing controlled information, and that such information will not be transferred to the PRC during a launch campaign. However, as noted below, reporting available to the Select Committee indicates that there have been lapses in security.

There is also reason to believe that not all lapses in security may have been reported. During the course of the Select Committee's investigation, no witness has been found to confirm that a transfer to the PRC of controlled technology has occurred as a result of ineffective launch site security. However, given the difficulty of proving that an improper transfer has occurred, it cannot be inferred that no such transfer has taken place.

Security lapses reported by the Defense Department at a number of launches in the PRC include the following:[5]

- **A PRC national set up all secured and unsecured fax, voice and data communications for a U.S. satellite manufacturing company at the PRC launch site**
- **Doors, windows or equipment unsealed or unattended**
- **Unsecured windows — in one instance a window may have been unsecured for 21 days**

Allen Coates

- **Multiple instances of equipment left unattended**
- **Doors discovered with seals ripped off**
- **Controlled documents missing or unattended**
- **A laptop computer containing digital pictures of the satellite left unattended in a hotel room**
- **Notebooks containing controlled information left unattended in areas where the PRC had access**
- **Filing cabinets containing controlled documents left open or without proper seals**
- **Documents improperly removed from cabinets**
- **Controlled equipment improperly discarded in trash**
- **Multiple examples of documents shipped without proper locks/seals**

Allen Coates

Hand-carried containers often lacked seals or security locks *(left and above)*. In some instances technical data was improperly displayed on the outside of cases.

- **Satellite test data left in cabinets without seals**
- **Satellite diagrams and other sensitive documents left out in the open**
- **Schematic of satellite bus equipment module and related documents left out**
- **Test valve document left out**
- **X-ray position diagrams found in improper location**
- **Notes left on blackboards**
- **Improper access by PRC workers**
- **PRC workers spent long periods of time (an hour or more) in areas where they were not supposed to be present**
- **No access list of PRC personnel provided to monitor**
- **PRC workers in controlled areas without proper escorts or badges**
- **PRC technicians worked unsupervised in the area of the satellite**
- **PRC personnel had improper access to fairing doors that provided visual/physical access to the satellite**
- **Unauthorized photographs were taken of the satellite**
- **Controlled information not properly inventoried**
- **Telephones used without proper security procedures**
- **Improper practices with security cameras**
- **Security cameras mis-positioned, giving the PRC potential access to the satellite container without detection**
- **Failure to man proper location when security camera inoperable**

Allen Coates

Allen Coates

Buildings in Xichang where American satellites are prepared for launch pose security risks. Large windows offer numerous points of entry, as do underground steam pipe tunnels accessed through nearby manhole covers.

Once the U.S. satellite is mated to the PRC rocket, a fairing encloses the equipment to protect it during launch. PRC personnel had improper access to fairing doors that provided both visual and physical access to U.S. satellite technology.

- **Lax attitudes toward security exhibited by U.S. personnel, including failures to record or investigate potential violations**
- **Blueprints of Vandenberg Air Force Base facilities exposed in the presence of PRC personnel**
- **Unauthorized discussions with PRC personnel**

Defense Technology Security Administration Director Tarbell confirms that Defense Department monitors have provided reports that there had been circumstances of short-duration, unescorted PRC access to U.S. communications satellites in the PRC.[6] However, Tarbell says that he is not aware of any evidence that this access resulted in a technology transfer that would significantly affect national security.[7]

A Defense Department monitor wrote the following comments in his final report during a 1998 PRC launch campaign:

> *This assignment for DTSA [the Defense Technology Security Administration] has proven to be exceptionally taxing and difficult. We are trained, given the necessary tools/skills and expected to protect U.S. technology from improper disclosure/compromise.*
>
> *Our responsibilities as monitors become transparent when aerospace companies (some not all) are given a Commerce License. It is viewed by industry as a license to steal and the monitors are a necessary evil to pacify management and our government.*
>
> *There is a general consensus within the public sector that, if restrictive measures and significant penalties are not levied against industries (specifically aerospace) by the Commerce Department (or higher), our technology will be compromised to such a staggering level and that our highest level of technology advancements will be available to our international competitors before it comes off the research and development floor.*
>
> *We as a nation cannot allow or afford to have industry police itself when it comes to national security . . .*
>
> *History is filled with unnecessary shortcuts in safeguard/security procedures resulting in the loss of American lives and federal grand jury investigations into illegal transfer of our technology by major corporations in an effort to increase their profit . . .*[8]

In an October 27, 1992 memorandum, Sumner Benson, Director of the Defense Technology Security Administration Technology Policy Directorate, expressed the following concerns regarding the security situation relating to the launch in the PRC of the FREJA satellite:

U.S. Defense Department monitors are required at PRC launches of American satellites. According to one monitor, a U.S. Commerce Department license to launch in the PRC "is viewed by industry as a license to steal," and the monitors are seen as "a necessary evil to pacify management and our government."

During the subject launch campaign, PRC personnel had unmonitored access to the FREJA satellite after it had been mated with the PRC LM2C launch vehicle [Long March 2C rocket]. Because PRC access was unmonitored, the [Defense Department] technology security monitors cannot state with certainty that no technology was transferred.

During a three day period from 26-28 September 1992, the [Defense Department] representatives noted PRC activity in the Vehicle Equipment Bay (VEB), located in the lower section of the FREJA clean room at the top of the LM2C [Long March 2C] booster.

Neither the [Defense Department] representatives nor the Swedish Space Corporation (SSC) representatives [the purchaser of the satellite] had been informed about this activity, and it had not been included in Combined Operations Procedures. The PRC were apparently working on their navigation and guidance equipment, but access to the lower side of the FREJA satellite was possible from the VEB.

When the [Defense Department] representative became aware of and attempted to monitor this activity, he was prevented from doing so by the PRC launch site commander.

Through a series of meetings with PRC representatives of the launch site, the launch site parent organization (CLTC) and PRC Defense Department (COSTIND), the [U.S. Defense Department] representative determined that the PRC:

> *Did not believe that unilateral work on their equipment was combined operations activity and therefore advanced notification and monitoring was not required;*
>
> *Felt that the [Defense Department] monitor was overzealous in wanting to monitor the PRC activity in the VEB;*

Did not feel monitoring was necessary because they [the PRC] could be trusted not to try to acquire any technology even when they had access to the satellite; and finally,

Felt that they [the PRC] had not violated the Technology Safeguards Agreement. [9]

Allen Coates

A Defense Department monitor deliberately attempted to break into a PRC satellite processing building, such as the one shown above, to determine whether he would be detected. The monitor was able to penetrate the facility and approach the security supervisor undetected until tapping him on the shoulder.

In another instance, a Defense Department monitor indicated that he deliberately attempted to break into the satellite processing building in the PRC to determine whether he would be detected. The monitor was able to penetrate the facility and approach the security supervisor undetected until tapping him on the shoulder.[10]

Safeguarding U.S.-Built Satellites and U.S. Rocket Technology at PRC Launches

Country-to-Country Agreements

In 1988, and again in 1993, the United States entered into agreements with the PRC for the purpose of precluding the unauthorized transfer of sensitive technology associated with the export of U.S.-manufactured satellites for launches in the PRC.

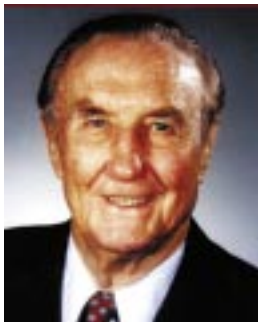
The agreements specify that at no time will there be unmonitored or unescorted access by PRC nationals to any of the equipment or associated technical data.[11] Additionally, only "form, fit and function data" [12] that describe mechanical and electrical mating requirements for attaching the satellite to the rocket are authorized for release to PRC nationals.[13] The agreements further indicate that the U.S. Government shall oversee and monitor implementation of Technology Transfer Control Plans, which are required to be developed by the satellite manufacturer. The PRC is required to permit and facilitate that monitoring.

Access to all satellite equipment and technical data is required to be controlled on a 24-hour basis by U.S. persons who have received training in security procedures from the U.S. Government. These U.S. persons must exercise this control throughout launch preparations, satellite transportation, mating/demating, test and checkout, satellite launch, and required return of equipment to the United States.[14]

Export Licenses

With the passage of the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999, all satellites and related items have been transferred to the United States Munitions List, and their export is controlled by the State Department under the Arms Export Control Act.[15]

Prior to this Act, the Department of Commerce had jurisdiction for licensing the export of some commercial satellites from 1993 through 1996, and over export licenses for all commercial satellites from 1996 through 1998.[16]



The FY99 National Defense Authorization Act is named for U.S. Senator Strom Thurmond (R-SC). It provides that U.S. business interests must not be placed above national security interests.

During the period 1993 through 1996, the Department of Commerce issued three export licenses for commercial communications satellites to be launched in the PRC that did not require the presence of Defense Department monitors, and did not require the U.S. exporter to reimburse the Defense Department for the expenses of providing monitoring in the PRC.[17]

Although the U.S. licenses routinely stipulate the presence of a Defense Department monitor, this requirement has not always been well-received by the satellite manufacturer.

For example, in one instance, a satellite manufacturing company demonstrated a negative attitude toward the presence of a Defense Department monitor as required under a license issued by the Department of Commerce. The Defense Department monitor explained that he had a disagreement with a program manager and the company site security supervisor over the manner in which a computer board would be shipped. The security site supervisor told the monitor that his company had a Department of Commerce license for that particular satellite launch and, therefore, the Defense Department monitor was in the PRC as a courtesy.[18]

Licenses issued by the Department of State include detailed provisos concerning technology transfer and security. For example, one license issued to Hughes stipulated:

> *Hughes must develop a plan(s) to comply with the applicable provisos of this [license]. These plans must address the technology safeguards implementation, security support, tranportation, debris recovery and other issues.* [19]

The Defense Department's Responsibilities for Safeguarding U.S. Technology at Launches

The Defense Department provides oversight in safeguarding technology at launch sites in the PRC. The Defense Department does this in part by overseeing implementation of Technology Transfer Control Plans and Security Plans prepared by the U.S. satellite manufacturers as required under export licenses.

The Defense Department also is responsible for monitoring all technical interchange meetings between U.S. and PRC personnel.[20] These meetings can occur as early as two years prior to a launch and continue during the launch campaign, as well as after a launch. Provisos in the U.S. export license for the PRC indicate the limits of the technical data that may be exchanged in these meetings. A Defense Department monitor is required to attend technical interchange meetings when PRC nationals are in attendance in order to assure that only data permissible under the license is exchanged.

Deficiencies Observed in the Current System

U.S.-PRC Technical Discussions Occur Prior to The Issuance of Export Licenses

When a U.S. satellite manufacturer applies for an export license for the satellite and related technical data, the Department of State or the Department of Commerce notifies the Defense Department that monitors will be needed to oversee the launch and the technical interchange meetings. However, technical discussions are conducted over the telephone or through informal personal discussions and marketing meetings prior to the license being issued.

This illustrates the fact that U.S. satellite manufacturers are on the honor system, to a large extent, in ensuring that no licensable technical data is exchanged in the absence of a Defense Department monitor.[21]

Although Defense Technology Security Administration Director David Tarbell agrees that "anything is possible," he believes it is not likely that a technology transfer would occur during early contractual discussions of this type. Tarbell says that conversations in these early stages would relate to the type of satellite the buyer wants, not how the satellite would be launched.[22]

Technology Transfer Control Plans and Security Plans Vary Throughout the Space Industry

The current U.S. Government export control system requires industry to formulate a variety of required plans, including Technology Transfer Control Plans and

Security Plans. These plans are provided to the Defense Department for review and approval. However, the plans vary from company to company, despite the fact that the launch facilities are the same, and the processing procedures of each company are similar.

Tarbell comments that, although standardization of the plans would be desirable, some degree of flexibility should be allowed, and any standardization should not rise to the level of rulemaking.[23]

Temporary Assignments of Defense Department Monitors Disrupt Continuity of Launch Site Security

Because the Defense Department did not have the resources to allow its permanent staff to participate as monitors on a regular basis, the Defense Technology Security Administration decided that the monitors for communications satellite launch campaigns in the PRC and U.S.-PRC technical interchange meetings should be drawn from the Air Force Space Command.[24] According to one former Defense Department official, an individual often is chosen to be a monitor by Space Command because he or she is between jobs or may be expendable.[25]

The duration and living conditions of these assignments make them even more unappealing. In addition, these assignments are unpopular with commanding officers because they do not enhance the Space Command mission, and because participation by their personnel could be construed as indicating that they have excess resources at their disposal.

The lack of a permanent corps of Defense Department monitors with relevant technical experience has drawn criticism from the space industry.[26]

An aggravating circumstance is the frequent rotation of monitors throughout the launch campaign. During the five-to-eight week duration of one PRC launch, for example, as many as five monitors were rotated in and out of the site.[27] Additional monitors may have participated in technical interchange meetings that occurred prior to the launch.[28]

Dept. of Defense

The Air Force Space Command provides monitors for each satellite in the PRC because the Defense Department decided it did not have the resources to allow its permanent staff to participate as monitors on a regular basis. According to one former Defense Department official, monitors are often chosen by the Space Command because they are between jobs or are expendable. Actual launch site security personnel do not work for the Defense Department, but are contracted from private firms by the company exporting the satellite.

Frequent rotation results in a lack of continuity and consistency in monitoring decisions during the technical interchange meetings and the launch. The information discussed during a technical interchange meeting is often based on the information discussed during a preceding meeting.

Thus, a new monitor coming into a meeting without having attended the previous meeting is not aware of what particular information the previous monitor may have either prohibited or allowed the participants to discuss. Additionally, as one former Defense Department monitor opined, "The knowledge base that's required from one technical meeting to the other sets the precedents for the next one." [29]

The same is true at the launch site. A series of Defense Department monitors coming and going disrupts continuity. According to one security official, ". . . to have three different DTSA [Defense Department] representatives is very difficult from a security perspective because . . . they each have their own areas of specialty, they each have their own background and limited experience." [30]

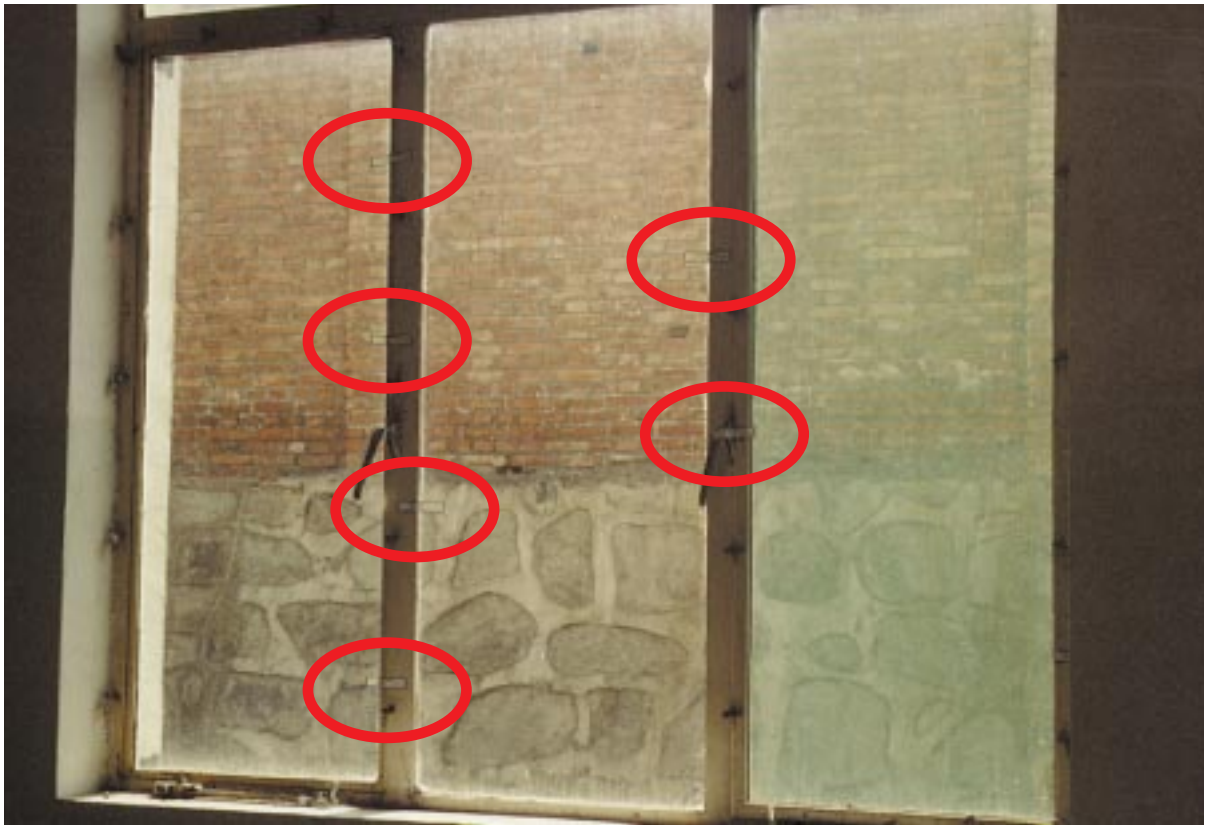
For example, while the first Defense Department monitor assigned to the launch when the satellite arrives in the PRC is responsible for ensuring that the facility is secure, in one instance a replacement monitor toured the facility and made a series of changes to the physical security plan that had been found to be satisfactory by the previous monitor.[31]

An Inadequate Number of Defense Department Monitors Is Assigned to PRC Launches

While the number of Defense Department monitors assigned to a launch site has varied over the years, it has been standard practice to assign only one or two monitors at a time to launches in the PRC.

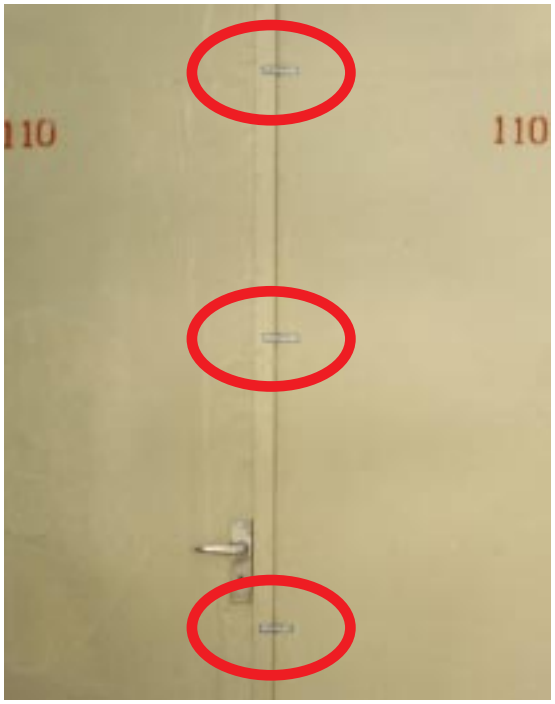
However, a July 1993 order of the Secretary of the Air Force directed that:

> *Air Force Space Command will identify **two to five** qualified technology safeguard monitors for each satellite program, depending on the program's scope, complexity and duration.*
>
> *Further, for each launch campaign (typically five to eight weeks), Space Command will **ensure that two to four monitors are present at the launch site at all times.***
>
> *To accomplish this, Space Command will assign one lead monitor to remain at the foreign launch base for the duration of the mission, and will typically form two teams of two monitors each to accompany the lead monitor. Each team of two will be at the foreign launch site for about five weeks, (nominally), plus a week of travel time for each team (counting both legs of the trip).*[32] [Emphasis added]



Allen Coates

Allen Coates



Allen Coates

Paper seals were used to secure doors at PRC satellite preparation facilities. These were later replaced with peel-away "void" seals. When it was very cold, the seals could be taken off and replaced, leaving no evidence of a security breach.

Some company representatives believe that one Defense Department monitor is adequate during the course of a normal launch campaign to cover technical interchange meetings and to monitor technology at the site. This, they say, is largely because most of the technical discussions have already occurred during the years leading up to the launch. One company's security manager says meetings with the PRC at a launch never would occur without the presence of the Defense Department monitor.[33] In the event of a launch failure, however, more monitors may be necessary.

The sole Defense Department monitor at the Intelsat 708 failure had difficulty working alone to oversee interactions between the PRC, Loral employees, and the private security force to ensure that no technology would be transferred as a result of the failure. The monitor recalls that:

> *Following the destruction of the Long March 3B, Loral upper management completely took over the operation of satellite piece recovery and ignored my advice to delay piece recovery until the area became safe and a meeting between PRC, Loral and myself could control the situation.*
>
> *As a result, at least two technicians returned from the crash site complaining of bulging eyes and severe headache requiring a 5-minute oxygen treatment.*
>
> *I believe we were lucky we recovered 63.5 percent of the vehicle [rocket] along with the [satellite's] encryption-decryption equipment.*[34]

This same monitor says he was not able to keep the Loral program manager from traveling to the crash site unaccompanied before the site was declared safe.[35]

Uneven Prior Technical Experience Of the Defense Department Monitors

Without a permanently assigned corps of Defense Department monitors, matching the experience of the monitor to the necessary tasks is difficult. Program officers, instead of engineers, have been used as monitors.[36]

Some company personnel noted that the Defense Department monitors have different backgrounds, and their technical expertise, therefore, varies.[37] By and large, the security managers interviewed by the Select Committee believed that the Defense Department monitors had the necessary technical expertise to keep pace with discussions between the company engineers and the PRC.[38]

The space industry has indicated that the Defense Department should maintain an adequate staff of trained professionals in monitoring technology transfer at foreign launches, with the end result being more uniformity overall.[39]

The Defense Department monitors participate in a three-day training course to prepare for assignments. The training is conducted by Air Force Space Command and includes such topics as the International Traffic in Arms Regulations, Export Administration Regulations, Memorandums of Agreement, Licensing Provisos, Technology Transfer Control Plans, Security Plans, Daily Logs, Incident Reports and Trip Reports.[40] Training also includes formal briefings by the Defense Department, and continues on an ad hoc basis with regard to particular licenses.[41] As launch numbers have increased, there have been more training sessions that incorporate lessons learned during past launches to prepare monitors for future assignments.[42]

Inadequate Headquarters Review of Monitor Reports

The July 1993 order of the Secretary of the Air Force directed that the lead Defense Department monitor for each launch campaign must maintain a complete daily log of events during that campaign. This daily log must include records of each meeting between the U.S. satellite manufacturer and the foreign launch provider, and it must summarize all decisions affecting technology security.[43]

The monitors are instructed to fax their daily logs to both Space Command and the Defense Technology Security Administration (now the Technology Security Directorate).[44] Because the fax machines often are not reliable at PRC launch sites, Space Command also faxes the monitor logs to the Defense Technology Security Administration to ensure that they are received.[45]

The lead Defense Department monitor is required to report the satellite processing status and plans, along with any safeguarding problems and recommendations, to the

Defense Technology Security Administration (now the Technology Security Directorate), and also to Space Command at least once a week during a launch campaign.[46]

Space Command is responsible for the receipt and storage of reports that the Defense Department monitors prepare and send while they are on assignment at a launch site abroad.[47]

The Director of the Defense Technology Security Administration, David Tarbell, says he is not aware whether Defense Department monitors' reports are first received at his agency and reviewed, or whether they are sent directly to Space Command prior to being warehoused there.[48]

Although Space Command schedules the monitors and is considered to be a flow-through point for reports from the monitors, Space Command's interaction with the monitors is administrative, not substantive, and similar to that of a program manager. Yet, Space Command receives daily activity logs from Defense Department monitors that contain information concerning security incidents and infractions at the launch site.[49]

Tarbell stressed that it is the Defense Department monitor's responsibility to assure that serious incidents are brought directly to Headquarters' attention.[50] Less significant security infractions are reported to both Space Command and the Defense Technology Security Administration via the monitor's daily logs.

Actual entries from Defense Department monitors' logs appear at the end of this chapter.

According to Defense Technology Security Administration officials, only two security matters reported by Defense Department monitors have been raised to the attention of the Director in the past 13 months.[51]

Lack of Headquarters' Support

Some Defense Department monitors have reported difficulties in contacting Defense Technology Security Administration management in the United States while they are on a PRC launch campaign.

One Defense Department monitor noted in his daily log, during a PRC launch operation in 1998: ". . . Attempted to contact the DTSA office in Washington, however, all personnel were TDY [away on temporary duty]." [52]

Another Defense Department monitor also attempted to contact the Defense Technology Security Administration in Washington on another date, and also was told all personnel were away on temporary assignments.[53]

The Defense Department monitor assigned to the Loral-Intelsat 708 launch in the PRC reports that he attempted unsuccessfully to resolve repetitive security infractions during that launch. He indicated that he then attempted to contact Space Command in Colorado, and wrote several memoranda to his superiors at the Defense Technology Security Administration.[54] That official then had to telephone Loral directly to have the deficiencies reviewed and corrected.[55] Following the phone call, the Defense Department monitor acknowledged security had "greatly improved." [56]

The Loral site security supervisor for the Intelsat 708 launch indicates that the Defense Technology Security Administration did not support the monitor in attendance at that launch. The monitor reportedly had no security plans provided to him by the agency beforehand, and had to make on-the-spot decisions concerning the release of documents.[57]

Lack of Intermediate Sanction Authority

One Defense Department monitor explains that several types of security violations can occur during a launch campaign or a technical interchange meeting.[58] Most incidents fall into the category of infractions that do not rise to the level of a license violation, but may include such things as controlled documents being left out in the open, unescorted visitors, and broken security seals on doors or windows.

Tarbell characterized infractions as instances that run the gamut "from very, very minor things to things that require DTSA's attention, but don't rise to the level of an export control violation that we should report to the State Department." [59] Tarbell says that Defense Technology Security Administration guidance to monitors encourages them to try to resolve problems on site and, if that is not effective, to contact the agency immediately so that it can resolve the situation with the company.[60]

Loral Space & Communications Ltd.

CONSOLIDATED STATEMENTS OF CASH FLOWS

(In thousands, except per share data)

	Year ended December 31, 1997	Nine months ended December 31, 1996	Year ended March 31, 1996
Operating activities:			
Net income (loss)	$ 40,004	$ 8,677	$ (13,785)
Gain on the sale of K&F stock	(78,591)		
Equity in net loss of affiliates	47,273	4,709	8,628
Minority interest	4,834		
Deferred taxes	419	(926)	3,838
Accretion on GTL CPEOs	(1,739)		
Depreciation and amortization	62,764	1,051	
Changes in operating assets and liabilities, net of acquisitions:			
Contracts in process and inventories	(152,794)		
Deposits	(107,670)		
Other assets	(26,615)	(9,252)	
Accounts payable	68,574	(1,832)	
Customer advances	(57,778)		
Accrued expenses	(36,602)	(4,506)	
Taxes payable	24,873		
Long-term liabilities	(17,200)	(1,124)	
Cash used in operating activities	(230,248)	(3,003)	(1,319)
Investing activities:			
Acquisition of businesses, net of cash acquired	(545,642)		
Proceeds from the sale of K&F stock, net of expenses	79,591		
Investment in affiliates	(237,895)	(6,425)	(105,231)
Other assets	(63,482)		(9,800)
Proceeds from the sale of property, plant and equipment		5,003	
Capital expenditures	(255,340)	(540)	
Cash used in investing activities	(1,022,772)	(1,962)	(115,031)
Financing activities:			
Borrowings under revolving credit facility, net	32,812		
Proceeds from issuance of term loan	275,000		
Proceeds from convertible preferred equivalent obligations		583,292	
Proceeds from exercise of stock options and issuances to employee savings plan	7,338		
Contribution from minority partner	9,100		
Preferred dividends	(25,435)		
Proceeds from the Distribution		612,274	
Transaction expenses related to the Distribution		(12,386)	
Advances from Loral Corporation prior to the Distribution		2,425	116,362
Cash provided by financing activities	298,815	1,185,705	116,362
(Decrease) increase in cash and cash equivalents	(954,205)	1,180,740	12
Cash and cash equivalents—beginning of period	1,180,752	12	
Cash and cash equivalents—end of period	$ 226,547	$1,180,752	$ 12
Non-cash transactions:			
Mandatory exchange of Convertible Preferred Equivalent Obligations	$ 583,292		
Issuance of Series C Preferred Stock to acquire equity interest in SS/L	$ 149,600		
Issuance of Loral common stock to acquire equity interest in SS/L and Globalstar partnership interests	$ 148,387	$ 100,313	
Deferred purchase price to acquire Globalstar partnership interests	$ 24,787		
Assets transferred from Loral Corporation at the Distribution		$ 31,383	
Liabilities assumed from Loral Corporation at the Distribution		$ 27,313	
Transfer of GTL common stock to acquire equity interest in SS/L		$ 5,158	
Supplemental information:			
Interest paid	$ 40,866		
Taxes paid	$ 8,901	$ 1,528	

Because satellite manufacturers are interested in keeping launch costs low and pushing schedules, they often view security as an obstruction to their mission. One Loral program manager told a Defense Department monitor that "security is ninth on my list of priorities."

Tarbell says that he believes that his agency has a significant sanction available — the ability to stop a launch. In addition, Tarbell also indicates that he believes that the Defense Technology Security Administration has additional enforcement powers by virtue of its relationship to the licensing process and the Arms Export Control Act.

However, there appear to be no intermediate sanctions available to discourage relatively common, repetitive security infractions.

Conflicting Industry Priorities

Tarbell acknowledges that the satellite manufacturer's program management staff is interested in pushing the schedule, making sure costs are low, finishing the project, and limiting risk to the project. This forces the satellite firm to make judgments that push as hard as possible against the barriers of security and technology transfer. This is why, in Tarbell's view, Defense Department monitors are necessary.[61]

One Loral site security manager indicates that industry project managers consider security to be an obstruction to the completion of their mission. It is an extra cost and poses additional obstacles to them.[62] One Loral program manager repeatedly stated to a monitor that "Security was ninth on my list of priorities." [63]

A former security manager for Loral says that he argued against having the program manager being placed in charge of satellite security during the Intelsat 708 launch in the PRC, because a program manager's main objective of launching the satellite will take precedence over security.[64] He was overruled twice, even after several reports were received during the launch campaign that the Defense Department monitor was having problems with the program manager's lax attitude toward security issues.[65]

During the Loral-Intelsat 708 launch campaign, complaints were made that the program manager invited PRC nationals into the satellite processing building and allowed them to be photographed standing in front of the satellite.[66] The PRC nationals were alleged to be employees of the local hotel, as well as members of the PRC technical team.[67] Comments were made that the program manager's Chinese heritage invoked his sense of pity concerning the quality of life of the PRC nationals near the launch site, and motivated him to invite the visitors for a photo session.[68] No record of this incident appears in Defense Technology Security Administration files.

Although U.S. laws and regulations require 24-hour security of satellites in the PRC, the private security guards hired by satellite companies were found sleeping on the job, under the influence of alcohol, and routinely leaving the launch site to meet with prostitutes while on duty.

Satellite Manufacturers, Not the Defense Department, Supervise Site Security Personnel

At the launch site, the security force reports to the U.S. satellite manufacturer's representatives (because the security personnel's contractual obligations run to the company that pays them, not to the U.S. Government). Therefore, the security force cannot be considered to constitute an independent security function.[69] Yet some industry officials insist that the program manager should be responsible for the entire launch campaign, including security.[70]

Reliance on Private Contractor Security Is Inadequate

United States commercial satellite manufacturers routinely contract with a private security firm to provide security, including protection against technology transfers, at PRC launch sites. Since few, if any, other security firms currently provide this specialized service, Pinkerton Aerospace Division has been used almost exclusively by U.S. satellite firms launching in the PRC. Of the ten security firms identified in a recent business journal, for example, only Pinkerton currently offers foreign launch site security services.[71] Another firm, Launch Security Services International, provided such services prior to going out of business in 1996.[72]

Both the Defense Department monitors and industry representatives have complained about the quality of work and the conduct of some members of the contractor security forces.[73]

Allen Coates

Procedures called for television security cameras to be disconnected or turned away from satellite processing activity *(below).* Infractions of these procedures occurred on a regular basis.

One Defense Department monitor experienced a range of problems with the private security guard force on a PRC launch, including:

- **Sleeping on the job**
- **Reporting to work under the influence of alcohol**
- **Poor reporting on daily logs and at shift changes**
- **Racial and gender slurs towards PRC nationals in the local village**
- **Routine bus trips into the town to meet prostitutes**
- **Overall lack of respect for management**

The Defense Department monitor indicates that the solicitation of prostitutes became so intense that he was approached by a PRC foreign affairs officer who was assigned to the launch to report that one of the guards had been seen soliciting prostitution in front of the local police department.[74]

One security guard even reported for duty carrying a sleeping bag.[75]

Another Defense Department monitor describes a situation during a launch campaign in the PRC in which the contractor security guards moved a table out of the line of sight of a video surveillance camera, in order to use it as a bed.

Since the table on which the security guard was sleeping also obstructed entry and exit to the room, the Defense Department monitor called the guard on the telephone to request that the table be moved away from the door, and back into the position where it had previously been located.

The guard reportedly responded that he was "not in the furniture moving business." [76] In response, the Defense Department monitor had to leave his duties and walk to the remote building to confront the guard and ensure that the table was moved.

Insufficient Numbers of Security Guards at PRC Launch Sites

Each U.S. satellite manufacturer is permitted to develop its own security plans for launches in the PRC, with subsequent approval by the Defense Department. As a result, the number of security guards at PRC launch sites varies.

One U.S. satellite company security official indicates he believes that attempting to

take less than ten contract security guards to a launch in the PRC is "rolling the dice" in terms of the ability to provide effective safeguards. Taking less than nine is, in his view, "crazy." Most satellite manufacturers take 12 or 13 security officers to a PRC launch.[77]

However, one Loral site security supervisor says he was asked by the program manager to try to reduce costs and investigate the possibility of reducing the number of contractor security staff, since the program manager had observed that security guards often were idle. The supervisor agreed to require only nine security officers — even though he had never been to the PRC launch site, and even though he was aware that 12 security guards had been used at the same facility for the previous Loral launch. The Loral site security supervisor says that he experienced no problems maintaining proper security with only nine officers.[78]

Some satellite manufacturers attempt to augment the contractor security force by using their own technical staff to provide escorts for nationals during a launch campaign. During launches in the PRC, this has resulted in periods when PRC visitors were unescorted and unattended, because the technicians were called away or not attentive to their escort duties.[79]

Correcting Security Deficiencies

In recent months, an effort has been underway to standardize security practices among U.S. companies launching satellites in the PRC. Security managers from Hughes and Loral have been trying to form a working group with the Defense Department "to try to standardize . . . some of our practices." [80]

Tarbell notes that U.S. satellite companies have expressed great interest in working with the Defense Department to achieve some standardization in their approaches to site security.[81]

Additionally, some companies hold "lessons learned" sessions after a launch occurs to incorporate circumstances and responses encountered during a launch, including site security, into future launch operations.

Following the failure of the Intelsat 708 launch, for example, the security manager reviewed the Defense Department's reports and findings and made changes to the

company's security system. He concluded that Loral needed "a much more intensive educational program to inform everybody that there will be a very stringent document control system with bright red covers and locked safes and daily inventories.[82] Additionally, the Loral security manager requested that a representative from the Defense Department speak to company management to discuss how the company could improve its security procedures.

The 1999 Defense Authorization Act

The Strom Thurmond National Defense Authorization Act for Fiscal Year 1999 provides that U.S. business interests must not be placed above U.S. national security interests, and that the export or transfer of advanced communication satellites and related technologies from U.S. sources to foreign recipients should not increase the risks to the national security.

Further, the Act states that the United States should not export missile equipment or technology to the PRC that would improve its missile or space launch capabilities, and should pursue policies that protect and enhance the U.S. space launch industry.

In furtherance of these interests, the Act calls for mandatory Defense Department monitors and reimbursement of related costs by the U.S. satellite manufacturer, in any case in which a license is approved for the export of a satellite for launch in a foreign country. The stated purpose is to prevent the unauthorized transfer of technology, including technical assistance and technical data.[83]

The Secretary of Defense is also directed by the Act to establish a program for recruiting, training and maintaining a staff dedicated to monitoring launches of satellites in foreign countries. The Act calls for mandatory Technology Transfer Control Plans approved by the Defense Department, and Encryption Technology Transfer Control Plans approved by the National Security Agency.[84]

The Technology Security Directorate within the Defense Department's Defense Threat Reduction Agency is developing plans for implementation of the Act. Tarbell indicated that the plans are undergoing funding review within the Defense Department. Tarbell also indicated that the Technology Security Directorate is reviewing the range of satellite-related activities in which it should be involved.[85]

Excerpts from Defense Department Monitors' Reports of Security Breaches at PRC Launches of U.S. Satellites

Loral-Mabuhay (1995): Report of DTSA Defense Department Monitor Major P. Smith

8-6-95

1. Meeting with PRC in a conference room **with drawings for the TEMPO program still on the white board**.
2. Discussed issue with Nick Yen, who promised that the conference room will be "clean" for future meetings.

Loral-Intelsat 708 (1996): Reports of Defense Department Monitor Captain S. Prichard

1-5-96

1. **Security Plan, Debris Recovery Plan, and a document detailing the responsibilities of the contractor security, escort, badging, logging, and detex procedures were not available for immediate reference prior to satellite arrival**. **When received, they were not signed, nor contained sufficient detail.**

1-5-96

1. **International Traffic in Arms Regulations-sensitive equipment not locked or sealed on aircraft when it arrived**.
2. **Security cordon around aircraft not established**.
3. **Container opened on ground** to obtain tie-downs and chains.
4. Ground security was unaware that sensitive material was aboard flight.
5. **Sensitive documentation packed in cardboard boxes on regular pallets** wrapped in plastic film.
6. **Monitor was only physical security deterring PRC entry for entire afternoon**.

1-7-96

1. **Inadequate locks and seals**.
2. Medical doctor is a PRC national and allowed to spend considerable amount of time in processing building.

1-14-96

1. **Open box containing International Traffic in Arms Regulations documents arriving on board aircraft**.
2. **International Traffic in Arms Regulations classified documents contained within a notebook discovered in the corner of the Satellite**

Excerpts from Defense Department Monitors' Reports of Security Breaches at PRC Launches of U.S. Satellites (continued)

Processing Building 2 airlock, an area used by PRC workers.

1-15-96
1. **Unescorted PRC technician in telephone wiring room. A technician escorting him finally returned after two minutes**.

1-16-96
1. **23 PRC nationals in satellite area without escorts**. Security was understaffed, and technicians were supposed to be escorts but were busy doing other tasks.
2. **Unsecured windows**.
3. **Badges not returned. Security has no idea who is in the building**.
4. "A serious attitude and a significant increase in security knowledge is needed."

2-4-96
1. **Broken door seals**.

2-6-96
1. **Crash doors left open**, security unaware.
2. **Incidents reported to security are only logged, and not investigated**.
3. **Events are not always logged because only one page is filled**.

2-14-96
1. **"Security is ninth on my list of priorities."** (Emphasis added)

2-16-96
1. Following destruction of LM-3B [Long March 3B], upper management [of Loral] completely took over the operation of satellite recovery without coordinating appropriately with monitor.

Loral-Apstar 2R (1997): Reports by Defense Department Monitor Captain S. Davis

9-25-97
1. Discussed Asia Pacific Telecommunications (APT) access to satellite with E. Acosta (Palo Alto). Acosta stated that APT observed [satellite] testing in Palo Alto. **Monitor stated that his interpretation of the country to country Memorandum of Agreement (MOA) precluded that. Air Force Space Command concurred with monitor.**

10-1-97
1. **Found a laptop computer with digital pictures of the satellite left improperly controlled in the small hotel [in PRC].**

Excerpts from Defense Department Monitors' Reports of Security Breaches at PRC Launches of U.S. Satellites (continued)

10-7-97

1. Satellite Processing Building 3 Officer Gallagher (Pinkerton) notified monitor that a **PRC representative was covertly drawing pictures of the satellite**.

   Discussed with Nick Yen [Loral], explained that drawings of the satellite were considered controlled technical data that required prior approval.

   [Defense Department] Monitor asked Nick Yen to remind Director Lee that individuals seeking technical data not specifically authorized is a violation of the country to country agreement.

   The artist was identified as Wong Zwei Chan of CALT.

   Chan provided a sketch to the monitor. Upon review, Officer Gallagher was not convinced that it was the same drawing. The provided drawing did not contain sufficient detail to represent a technology transfer.

2. **The security camera** of the satellite container on the pad was initially provided by a single closed circuit TV camera. Monitor deemed this **inadequate as the top of the container could be removed undetected**.

   Instructed Loral either to establish closed circuit TV coverage of the top of the container, or to seal the container with security tape. Loral chose security tape.

10-8-97

1. **Nick Yen released technical data prior to U.S. Government review. The documents released contained test data from the umbilical check and updated ICD [interface control documentation] information.**

10-9-97

1. **Nick Yen told PRC that when they accessed the fairing doors**, Loral required a report the next day on what actions took place. Monitor stated that **U.S. monitor needed to be present too**. Monitor had discussion with K. Patterson [Loral] re: policies for fairing access to satellite.

   Monitor offered Nick Yen two solutions:

   (1) ensure that PRC notify U.S. Government prior to access and wait for [Defense Department] oversight prior to opening fairing;

   (2) Monitor offered to inspect fairing access doors and if [PRC] visual/physical access is not possible, closed circuit TV would suffice as U.S. monitoring.

   Loral opted for inspection. **Inspection concluded PRC access was possible, and that very little time would be needed**.

Excerpts from Defense Department Monitors' Reports of Security Breaches at PRC Launches of U.S. Satellites (continued)

2. At 1615 hrs, **monitor observed PRC accessing fairing doors**. Monitor notified Nick Yen, who immediately called the PRC.

3. Nick Yen explained [to PRC] that fairing access required U.S. Government oversight.

10-10-97

1. **PRC again accessed payload fairing** without prior coordination. Monitor again briefed Nick Yen who again called the PRC.

2. Nick Yen called for a U.S.-only caucus, and indicated that **he would not allow his personnel to support the monitoring as it presented a safety hazard**.

3. B. Campbell [Loral] concurred that, based on previous experience at this launch facility, the pad is hazardous even when the launch vehicle is not fueled because the PRC pressurize their launch vehicle tanks with unpurged fuel and oxidizer.

4. Monitor advised Nick Yen that he did not have the authority to waive the requirement, and would consult Major Smith (DTSA).

5. Major Smith allowed for a **safety override of U.S. monitoring requirements**.

6. Monitor advised Nick Yen that the following requirements applied to **PRC access to payload fairing:**

   (1) PRC will call the security desk prior to accessing the payload fairing and provide reason for access and expected duration;

   (2) maximum of two PRC nationals may work in the area of the open payload fairing door;

   (3) no photographic equipment allowed;

   (4) PRC may only physically enter the fairing door to the shoulder level (if further access is required U.S. Government monitor must be present);

   (5) if the PRC violates any of these rules the security officer will call U.S. Government monitor, Nick Yen, and K. Patterson immediately; and

   (6) security officer will log all fairing access.

7. Monitor discovered a **Loral subcontractor stored a computer with digital pictures of the satellite in an unsecured room in Launch Complex 2**.

Excerpts from Defense Department Monitors' Reports of Security Breaches at PRC Launches of U.S. Satellites (continued)

8. APT representative and Yang Hua Wang of China Launch and Tracking Control General **took unauthorized photographs of [satellite].**

Hughes-Aussat B-1 (1992): Reports of Defense Department Monitor A. D. Coates

1-22-92

1. Confusion begins because Hughes is unprepared for launch causing them to arrange **multiple technical meetings [with PRC] unnecessarily and without prior notification to monitor**.

1-23-92

1. **Containers holding security equipment with only combination locks, no seals**.
2. **Security videos do not provide coverage of access fairing doors**.

1-24-92

1. Four items scheduled to be shipped without containers and uncovered.
2. Building not secure one week prior to satellite arrival.
3. Advance sea shipment inventory incorrect and **containers not locked and sealed as requested**.
4. No joint operational plans, or intent to create one.

1-28-92

1. **No Hughes management to direct PRC nationals.** [Hughes management] who are at Big Hotel one hour away appear to divorce themselves of responsibility of launch site when there. Security staff assumes ad hoc role to cover for them.
2. Continued **ad hoc decisions by Hughes without review by monitor**.
3. Lack of written procedures.

1-29-92

1. Items on 747 arrived unlocked. Had to board plane and lock before unloading.
2. Badging not addressed until day of 747 arrival.

1-30-92

1. **Documents removed from file cabinet in high bay without controls**.
2. **Satellite test data filing cabinet not sealed**.

Excerpts from Defense Department Monitors' Reports of Security Breaches at PRC Launches of U.S. Satellites (continued)

3. On board 747, data sheets attached to safe-and-arm pyro box, satellite **test data filing cabinet not sealed / located on open pallet**, containers listed as ground support equipment attached to forklift.

1-31-92

1. Test documentation not listed on inventory.
2. **No access list of PRC nationals** provided to monitor for Hughes-controlled area.
3. Hughes inventory of toxic vapor detectors reveals two keep [remain] missing.
4. **No list of documents Hughes exchanged with PRC.**
5. No trash disposal procedure.

2-1-92

1. **Inventory sheet visible on container**.

2-3-92

1. **Hughes may have given "milspec numbers" to PRC**.

2-5-92

1. Inventory sheets on containers visible.

2-6-92

1. **Filing cabinet left open**.
2. **Notes kept un-erased on blackboard**.
3. **Controlled documents cannot be located**.

2-7-92

1. Inventory sheets visible on containers.
2. Aussat satellite test equipment status papers on top of equipment.

2-8-92

1. **Satellite diagram left out in Satellite Processing Building 2**.
2. Misuse of telephone.
3. **Sensitive documents left out**.

2-9-92

1. Inventory sheet face up pushed under a typewriter to get it out of the way.
2. No seal between fueling rooms. (Second violation)

Excerpts from Defense Department Monitors' Reports of Security Breaches at PRC Launches of U.S. Satellites (continued)

3. **X-ray position diagram found**.
4. Inventory sheet exposed.
5. Hughes employee **personal notebook** found under briefcase **containing controlled material not inventoried and hand-carried. Worst case so far**. Requested inventory after.

2-10-92

1. Hughes employee asked to write a response, and Hughes [employee] disputes he is required to do so. **Hughes management unwilling to review security plan for requirements**.
2. Hughes holds **discussions with PRC without notifying monitor of contacts beforehand**.
3. **International Traffic in Arms Regulation-controlled material found in building even after monitor told none there**.
4. **No seals on two doors**.
5. **Hughes does not notify monitor of shipment, but notifies PRC.**
6. Inventory lists left exposed.

2-11-92

1. Hughes asks monitor to show them their own security plans. **No one at Hughes reads their own requirements**.
2. **Hughes indicates during security briefing that monitor's requirements are his own whims**.

2-14-92

1. **Schematic** of satellite bus equipment module and related documents **left out.**

2-15-92

1. Three inventory sheets left visible.

2-16-92

1. Invoice sheet left exposed.
2. **Satellite Processing Building 3 large doors had security seal ripped off**, seal partially removed from emergency exit door.

2-17-92

1. Test valve document left on satellite stand.

Excerpts from Defense Department Monitors' Reports of Security Breaches at PRC Launches of U.S. Satellites (continued)

3-15-92 1. **Camera 4 goes down. Security not aware [that they are supposed] to man tower when camera goes down**.

Hughes-Aussat B-2 (1993): Reports by Defense Department Monitors Captain R.J. Byrd, J. Kuriazisl, and S. Long

10-31-92 1. Hughes security guards had expired visas.

1-20-93 1. In the case where U.S. Government representatives might be seriously injured while in Xichang, Hughes made arrangements to quickly fly injured personnel to Hong Kong; alternately [alternatively], a U.S. Marine Corps aircraft could be flown in to transport U.S. Government personnel. It is noted that an injured person would not receive treatment for at least 24 hours from HAC [Hughes] or U.S. Marine Corps aircraft evacuation.

1-20-93 1. Flip-Rite cart not covered on satellite while aboard a chartered FedEx Boeing 747 flying from Los Angeles, CA, to Xichang, China.

2. Hughes security agreed to cover the Flip Rite prior to removal from the Boeing 747.

Hughes-Optus B3 (1994): Report of Defense Department Monitors Kline and Villhard

7-8-94 1. **Window left open for an undetermined period of time. May have been as long as 21 days.**

7-10-94 1. **Trucks left unattended by U.S. citizens. Third time equipment was discovered left unattended during this campaign**.

7-12-94 1. **Non-essential PRC [personnel] allowed in controlled area** because, by making them stand not three feet from technicians, the technicians felt they had to wait outside.

2. **Sea containers stored outside Satellite Processing Building 2 were locked but not sealed** because the security supervisor did not want to seal containers they needed continuous access to.

7-22-94 1. **Found Apstar controlled document file cabinet left open**. Did not see documents logged out.

Excerpts from Defense Department Monitors' Reports of Security Breaches at PRC Launches of U.S. Satellites (continued)

7-25-94 1. PRC working in building and not logging out.

8-29-94 1. **Controlled documents not signed back in. Person it was signed out to said he could not find it**. (Simon Peng)

Lockheed Martin-Chinastar (1998): Reports of Defense Department Monitors Captain H. N. Rollins and J. Chandler

3-25-98 1. **Satellite in Antonov aircraft overnight without U.S. security guards. Russian plane, Russian guards, Russian seal while plane stops in Russia for overnight rest.**

3-31-98 1. Concerned over relationship between Lockheed Martin, China Orient, and China Academy of Launch Vehicle Technology (CALT) because China Orient has lived and worked with Lockheed Martin in East Windsor, NJ for a year and monitor believes [there has been] a transfer of a significant amount to training technical support / data, hardware, software, etc., in contradiction to DTSA handbook.

4-5-98 1. Security found discarded equipment in trash, which is controlled.

3-23-98 to 4-17-98 1. "Lockheed Martin obtained the export license for this satellite contract through the [Commerce Department], not the [Department of State]. I believe this gave them too much discretion in sharing satellite technology with the PRC. For example, PRC engineers were present in the satellite factory in East Windsor, NJ, for the two years prior to shipment. They were present as customer representative for China Orient Telecommunications. **They witnessed all phases of assembly and test**. Beyond how the Chinastar satellite was built and performed, they had the opportunity to learn why it was built this way and the opportunity to infer any inherent weakness or vulnerability in its design." (Emphasis added)

4-27-98 1. Emergency exhaust fan in fueling room inoperable.

2. Emergency shower outside of fueling room inoperable.

Excerpts from Defense Department Monitors' Reports of Security Breaches at PRC Launches of U.S. Satellites (continued)

Motorola-Iridium (1993): Report of Defense Department Monitor Lieutenant M.L. Shaffer

11-30-93 to 12-3-93

1. "A briefing about **thermal issues** was given by Motorola in which information concerning a 'thermal maneuver' was presented. This was a perfect example of the Motorola 'it was given to the Russians so it can be given to the PRC' mentality . . . it was not pertinent information and should not have been discussed. Monitors should watch for items that are given to the PRC that reference either U.S. or Russian hardware or services." (Emphasis added)
2. During Technical Interchange Meeting, **blueprint of facilities of Vandenberg Air Force Base** was pulled out of a briefcase by a Motorola person (in the presence of China Academy of Launch Vehicle Technology (CALT), China Great Wall Industry Corporation, and Taiyuan Satellite Launch Center personnel).

Motorola-Iridium (1995): Report of Defense Department Monitors Lieutenant M.L. Shaffer and Captain E. McCarty

5-26-95

1. With DTSA approval Dan Letson (Motorola) had been monitoring CALT [China Academy of Launch Vehicle Technology] tests for about three weeks without a U.S. Government representative.

8-21-95 to 8-25-95

1. "An interesting note: During the last trip to the [PRC] Taiyuan Satellite Launch Center (21-25 August) there was a **technical thermal conversation going on. The monitor stepped out of the room for a minute and as soon as he did, 'without missing a beat,' one of the PRC engineers said to Motorola thermal engineer,** Bob Allen, 'I noticed that your solar arrays have no push springs on them for deployment. I was wondering how you deploy them on orbit?' To which Bob replied, 'I don't think I'm allowed to tell you that.' That (I was told) was the end of the conversation, which goes to show that we monitors may be more necessary for dissuading the PRC than the contractors." (Emphasis added)
2. **Motorola used the phrase in a TIM [Technical Interchange Meeting], "We have not been happy with the thermal design from the beginning." Major Smith (monitor) was concerned that the discussion would lead to the Americans redesigning the thermal**

Excerpts from Defense Department Monitors' Reports of Security Breaches at PRC Launches of U.S. Satellites (continued)

control system for CALT [China Academy of Launch Vehicle Technology]**.** (Emphasis added)

9-7-95 1. The launch tower lacks essential safety equipment such as an escape shoot and fire alarms.

Motorola-Iridium (1998): Report of Defense Department Monitors Major George R. Gunning

2-22-98
1. **Pinkerton had not read the Security Plan. They were not aware of what data and hardware was sensitive**.
2. Taiyuan Satellite Launch Center [PRC] provided walkie-talkies to Pinkerton guards. The radios lost their charge before the convoy even got started, thereby providing ineffective communications among guards.

2-24-98
1. I observed only one significant problem, **Motorola does not have a document control procedure**.

3-6-98
1. **PRC workers in area where they "had no business."** Work supposed to be completed in five minutes, and **PRC took 1.5 hours**. (Emphasis added)

3-23-98
1. Some Motorola [employees] consider the PRC their "good friends." Team leaders from Motorola develop a sense of trust that could lead to inadvertent transfer of technology.
2. **Unannounced access to controlled area**.

3-28-98
1. **Lack of vigilance** on the [part of] Motorola to protect U.S. technology. On several occasions had to remind MSC [Motorola Satellite Communications] to observe security practices such as **document control, being aware of what is said and transmitted over communications lines** and denying usual access [to] controlled areas.
2. **Motorola has been bringing in a PRC national to set up secure and unsecured fax, voice and data transmissions. "In my point of view this is a huge hole in security." "Given Motorola's lack of security training I would not be surprised to discover that unapproved technical data is being exchanged and intercepted by the PRC."** (Emphasis added)
3. PRC requested copies of Motorola procedure documents. I denied the request. "But if I had not been present they would see no problem in handing them over."