

June 16, 2008

Mr. Matthew S. Borman
Acting Assistant Secretary for Export Administration
U.S. Department of Commerce
Bureau of Industry and Security
Regulatory Policy Division
14th Street and Constitution Ave., N.W.
Room H-7205
Washington, D.C. 20230

RE: Request for Public Comments on Crime Control License Requirements in the Export Administration Regulations

Dear Mr. Borman:

The Laogai Research Foundation commends the efforts of the Department of Commerce to regulate and prevent the export of crime control equipment and technology to countries with repressive governments that have proven themselves willing to violate the human rights of their citizens. As a non-profit organization that monitors human rights in China, we believe that all peoples have a right to the freedoms we enjoy in the United States, be it freedom of life and security, freedom of opinion, association, and movement, or freedom of religion. Furthermore, we support an active role for the government of the United States in ensuring that these rights are respected worldwide.

While these export controls, and more specifically the crime control license requirements that are reflected in the Commerce Control List (CCL),ⁱ are indeed important, it is regrettable that they have not been updated for over a decade. Indeed, current restrictions on exports to China are based on a law passed immediately following the Tiananmen Square Massacre over seventeen years ago.ⁱⁱ There is a wide range of new technologies not included on the CCL list that are currently being used and developed by law enforcement agencies in the People's Republic of China (PRC) and other countries. While these technologies have legitimate law enforcement applications, when put into the hands of repressive regimes such as the government of the PRC, we fear these technologies will be used in ways that violate the human rights of the citizens of these countries. Many of these technologies were originally developed and produced in the United States and then marketed to the PRC, at times directly to the Public Security Bureau (PSB) and other Chinese government and law enforcement agencies. Though we would like to believe that US companies take the human rights records of countries into consideration when selling their products to foreign buyers, companies have a long history of working with and profiting from dictatorships and other questionable regimes. Recent revelations regarding IBM's involvement with Nazi Germany is one clear example.ⁱⁱⁱ This is why it has been, and should remain, the responsibility of the government to regulate these business relationships and ensure that we as a nation uphold our commitment to human rights globally.

Therefore, the Laogai Research Foundation respectfully offers the following recommendations regarding the items subject to crime control license requirements: that the list of items be expanded to reflect the advances made in crime control technology and equipment in the past decade; that a more effective mechanism for verifying end-users of dual-use products be put in place, and that licenses for dual-use technologies be granted only when end-users can be properly verified; and that improvements to export regulations be accompanied by better enforcement of the existing regulations. The need for such improvements to the CCL requirements is nowhere more evident than in the case of the PRC.

Human Rights Abuses and New Technology

It is a well-documented and widely known fact that China has a dismal record of respecting the human rights of its citizens. The State Department reported in March that in 2007, "the [Chinese] government's human rights record remained poor, and controls were tightened in some areas."^{iv} This year, Freedom House once again rated China as "Not Free," giving it the lowest and next to lowest possible ratings for political rights and civil liberties respectively. China's police and other law enforcement and security agencies, coordinated by the Ministry of Public Security, are not only chronic human rights abusers, but are also notoriously corrupt.^v Given the human rights record of China, we advocate for a total ban on exports of U.S. manufactured crime control products, equipment and technology to China.

Furthermore, given the increased use of the Internet and other technology by Chinese dissidents, as well as the Chinese government's willingness to track and arrest these "cyber-dissidents,"^{vi} we believe that there are also some seemingly innocuous technologies that should be added to the CCL list as "dual-use" items. Licenses for these products should be denied if the end-user is determined to be the Chinese government, particularly law enforcement and public security agencies. We support the export of these dual-use technologies to the private sector, and hope that Chinese individuals continue to use these technologies to spread ideas and advocate for greater freedoms in their country. Unfortunately, we know that the Chinese government is all too willing to use the same technologies to identify and persecute peaceful dissidents, monitor and suppress Falun Gong practitioners and members of other religious groups that do not have the approval of the state, and, more generally, to further government supervision of and intervention in the lives of the Chinese people.

Much of the technology the Chinese government is currently seeking will be used for the completion of the Chinese government's grand security project known as "Golden Shield." This project includes monitoring and censoring the Internet, including individuals' emails. It also includes monitoring phone conversations with advanced speech recognition technology, and monitoring citizens' movement through a vast network of surveillance cameras, equipped with face recognition technology. The information gathered could then be stored in a massive database along with individuals' fingerprints and other biometric data, their credit records, and other personal information. The ultimate goal is for police to use "Smartcard" technology to scan an individual's state-issued identity card and gain instant access to all of the information the government has collected on this individual. This would give the Chinese government an unprecedented level of control over its citizens and would be disastrous for the human rights of the Chinese people. Many American companies, most notably Cisco, have sold technology to the Chinese government that has helped make the Golden Shield project possible.

Expand CCL Regulations

Therefore, in keeping with the spirit of the ban on exports to Chinese police passed after the Tiananmen Square Massacre and with the full impact of the Golden Shield project in mind, we suggest an outright ban on biometric technologies, surveillance analysis technologies, and riot control agents that have not already been banned or restricted by the CCL regulations. The ban on biometric and surveillance analysis technologies should include all face-printing technology, speech-signal processing, video-signal processing, and other forms of 'algorithmic surveillance' or digital signal processing. This equipment allows law enforcement to essentially gather a print based on the quality of an individual's voice or an individual's prominent facial features - a vast improvement to the fingerprinting equipment and technology that the CCL regulations already restrict. During the Lhasa riots, security officials took footage from CCTV surveillance cameras and, using this type of analysis

technology, captured and extracted images of Tibetan protesters. In the following days, hundreds of demonstrators were detained or imprisoned.^{vii} In the context of the Golden Shield project, access to this type of technology over a broad and unified network could be devastating to the privacy and freedom of dissidents and the wider Chinese public alike.

Moreover, in addition to the identification technology explained above, algorithmic surveillance technology automatically analyzes human behavior and sends alerts to law enforcement officers when it notices anything suspicious, such as a group of people gathering or a person running. The Chinese police hope to use this technology to react more quickly to instances of public unrest, ideally rounding up dissenters before larger demonstrations even take place. The rights of Chinese people, especially free expression, association, movement and the practice of religion, will be systematically curtailed by the PRC if Golden Shield reaches the level of coordinated control the Chinese government hopes to achieve.

We have also found that certain equipment, such as bulletproof fabrics developed specifically for riot police produced by the Dupont corporation,^{viii} has escaped the notice of the DOC, even though providing these items to the PRC is clearly a violation of at least the spirit of current regulations that prevent crime control equipment from being sold to Chinese law enforcement agencies. We would suggest that the DOC reconsider the narrow scope of crime control items that it currently restricts in order to include a broader array of items, thus ensuring that companies cannot so easily circumvent the law.

Dual-Use Items

There are also a number of dual-use items we propose be added to the CCL. Although these items have legitimate uses in the private sector, they also have the potential to be used to violate the human rights of the Chinese people, and thus we urge the Bureau of Industry and Security to deny export licenses for these items if the end-user is determined to be a Chinese state agency with law enforcement or public security functions. One such item is firewall technology. The so-called "Great Firewall of China" is made possible by firewall technology, much of which originates in the United States. The government uses this technology to manipulate news coverage on the Internet, block human rights groups' and other dissidents' blogs and web pages, and suppress negative coverage of the Communist Party. Similarly, we suggest that software modules for routers that enable the government to monitor Internet content and track dissidents be added to the CCL list as well. The recent leak of a Cisco internal marketing presentation that explains how Cisco's technology can assist the Ministry of Public Security in the goal of "Combating Falun Gong evil cult and other hostile elements"^{ix} shows the Chinese government's willingness to use technology acquired from U.S. companies to suppress the Chinese people, and, more disturbingly, U.S. companies' willingness to assist them in this goal.

U.S. companies should also be prohibited from selling "Smartcard" technology to the Chinese government. This technology enables the government to track the movement of the Chinese people, and is a crucial element in the Golden Shield project.

Finally, we recommend that the export of surveillance cameras and the accompanying surveillance networking technology be heavily restricted. The prevalence of surveillance cameras in Chinese cities is growing at an alarming rate. They were used to identify dissidents after the Tiananmen Square Massacre, continue to be used to monitor and identify Chinese citizens, and play an important role in the Golden Shield project. The Chinese government has plans to continue to expand its network of surveillance cameras and is clear in its intent to use these cameras in ways that we find unacceptable.

For example, the fall issue of China's Ministry of Public Security magazine specifically listed Internet cafes and places of worship as locations where increased surveillance is needed.^x

US Companies Courting Chinese Security Officials

It is crucial that the export of these dual-use technologies is carefully monitored to ensure that the end users are not repressive governments. Many U.S. companies already have close working relationships with the Chinese government, and, incredibly, many companies are specifically marketing their products to Chinese law enforcement agencies. These companies have been violating the spirit, and we believe, the letter, of the post-Tiananmen Square legislation by doing so. Though these corporations often state that they sell their products mostly to retailers who then resell the product to end-users of whom they have no knowledge, many companies have been specifically pursuing the PSB as a market for their technology. At *China's International Exhibition on Police Equipment* in Beijing, Dupont, Motorola, and a California-based company called Intelligent Computer Systems all marketed technology designed to enhance police surveillance, networking, and operational capabilities.^{xi} Cisco's Director of Corporate Affairs, Terry Alberstein, confirmed that Cisco sells police surveillance and computing technology directly to law enforcement agencies in the PRC.^{xii} Honeywell, General Electric, IBM and United Technologies have all sold surveillance and security equipment to the PRC, enabling law enforcement agencies to monitor a vast system of video data and automatically analyze it through smart technology.^{xiii} It is clear that these companies are fully aware that the end-users of their products will be the PSB and other state-controlled law enforcement agencies.

The following transactions do not conform to the objectives of the export restrictions put into place following the Tiananmen Square Massacre. We hope such transactions will be avoided in the future, either through stricter regulations, or through stricter enforcement of regulations already in place.

- *Cisco Systems, Inc.* first designed and supplied the "network sniffers" or mirroring routers that allow the government to monitor virtually all Internet traffic entering and exiting China.^{xiv} Cisco Systems, Inc. has also sold routers and switches to regional police departments, allowing them to modernize their computer networks.^{xv}
- *Sun Microsystems* worked with a Chinese company, Changchun's Hongda Group, to develop a computer network linking all 33 provincial level police bureaus and allowing for instant comparison of fingerprints with a nationwide database.^{xvi}
- *Honeywell International* has helped police install a computer monitoring system that will analyze video data from indoor and outdoor surveillance cameras installed in one of Beijing's most populated areas. They are working on a similar system for Shanghai.
- *General Electric (GE)* sold the VisioWave system to the Chinese government. This system allows security personnel to control and monitor thousands of video cameras simultaneously, and alerts officials to suspicious or fast-moving objects, including people.
- *IBM* is working with Beijing officials to install a system, similar to the VisioWave system, that also has the ability to analyze and catalog citizens' behavior. IBM also has plans to install the even more expansive Smart Surveillance System by next summer.
- *United Technologies Corporation (UTC)* has begun the installation of a pervasive citywide network of surveillance cameras in the city of Guangzhou.^{xvii}
- *Oracle Corporation* sold software to the Chinese Ministry of Public Security, which is using the software for management of the country's digital identity cards.^{xviii}
- *Motorola* is marketing radio systems to Chinese police, as well as wireless systems for transmitting video surveillance data.^{xix} Motorola has already sold the Chinese authorities hand held devices that allow police to remotely tap into large databases.^{xx}
- *DuPont* is marketing bulletproof fabric the Chinese riot police.
- *Intelligent Computer Solutions (ICS)* is marketing the ImageMasster RoadMasster to Chinese authorities. This computer system can search a 80GB hard drive for keywords in a few seconds without leaving evidence

of tampering, and is used by the Pentagon and the CIA.^{xxi}

- *L-1 Identity Solutions* licensed its facial recognition software to the Chinese firm Pixel Solutions in 2006. The Chinese firm is developing the software further and hoping to land a contract with the Chinese Ministry of Public Security.^{xxii}

Conclusion

In summary, we recommend that the following equipment and technologies be added to the CCL, and that licenses to export these items to China be denied in all cases: biometric technology, including face-printing technology; speech-signal processing; video-signal processing; other algorithmic surveillance and video-analysis technologies; and bullet proof fabrics.

We also recommend that the following equipment and technologies be added to the CCL, and that licenses for these items be granted only if the end-user is determined to be a private company or individual: firewall technology; software modules for routers, or any specialized routers, that allow monitoring of Internet content and tracking of Internet users; Smartcard technology; surveillance cameras; and video surveillance networking technology.

Furthermore, we strongly urge the BIS to create better mechanisms for determining the end-users of dual-use equipment and technologies being exported to China and other repressive regimes. These mechanisms could be based on methods used to determine the end-users of dual-use military exports to China. Many of the companies selling products to the Chinese government work in conjunction with Chinese firms through middlemen, but the end-users are all too often the Chinese government and, specifically, the Public Security Bureau. The burden of proof should lie with the companies to prove that their products will not end up in the hands of repressive regimes. If they cannot prove this, then licenses to export the above-mentioned dual-use products should be denied. Weak monitoring of dual-use products erodes the efficacy of the regulations that the BIS aims to improve.

Finally, we urge the BIS to improve not only the regulations themselves, but the enforcement of both new and existing regulations. We have found many instances of trade between US companies and the PRC that seem to violate laws already in place. Improving export regulations is meaningless if not accompanied by stricter enforcement.

We respectfully request that the Department of Commerce review the impact that American technologies have had on China and other countries with repressive governments, and consider the future impact we will have if we do not impose stronger restrictions on our foreign exports and demand greater corporate transparency. The CCL must include a wider array of products as it has become apparent that the existing regulations are insufficient in stopping American corporations from supplying equipment and technologies that can aid in repression and persecution. The Laogai Research Foundation hopes that the Department of Commerce will seriously consider banning products clearly exported only for police use, imposing licensing requirements on dual-use products, and improving the enforcement of all of its regulations. These changes are imperative if we wish to maintain our international commitment to human rights and uphold the values of our nation. We thank you for taking our suggestions into consideration.

Sincerely,

Harry Wu
Executive Director, The Laogai Research Foundation

Kirk Donahoe
Assistant Director

Megan Fluker
Intern, Tufts University

Rachael Watkins
Intern, Indiana University

-
- i Based on 15 CFR 742.7(a)(1) through (4)
- ii Section 902(a)(4) of the Foreign Relations Authorization Act for Fiscal Year 1990-1991, Public Law 101-246
- iii IBM's punch card technology enabled the Nazi party to find, document, persecute and kill undesirables with a speed and efficiency that never would have been possible otherwise, perhaps contributing to the mass scale of the holocaust. (Festa, Paul, "Probing IBM's Nazi Connection," *CNET News*, 28 June 2001, <<http://news.cnet.com/2009-1082-269157.html>> (11 June 2008).)
- iv "China (includes Tibet, Hong Kong, and Macau)," in *Country Reports on Human Rights Practices - 2007, U.S. Department of State*, 11 March 2008, <<http://www.state.gov/g/drl/rls/hrrpt/2007/100518.htm>> (9 June 2008).
- v *ibid.*
- vi The State Department report includes the following information on individuals who were detained or imprisoned for writings published on the Internet in 2007: "In August Internet blogger He Weihua was arrested by Hunan authorities and committed to a mental hospital, allegedly as punishment for antigovernment writings. On August 14, a court in Hangzhou sentenced Internet writer Chen Shuqing to four years in prison for inciting subversion after he criticized the government online. In March a court in Ningbo, Zhejiang Province, sentenced Internet writer Zhang Jianhong (also known as Li Hong) to six years in prison. Zhang was arrested in 2006 after writing an article calling for activist Gao Zhisheng's release. Zhang was a founder and editor of the literary and news Web site Aegean Sea (*Aiqinhai*), which authorities [shut down in March](#) 2006. On December 13, police in Guilin, Guangxi Province, arrested Internet writer Wang Dejia (also known as Jing Chu) after Wang posted several articles critical of the government. Other individuals who remained in prison for posting political or dissenting views on the Internet included journalist and Internet essayist Li Changqing, activist Ren Zhiyuan, Internet essayist Yang Tongyan (Yang Tianshui), and Internet author and human rights advocate Guo Qizhen." from "China (includes Tibet, Hong Kong, and Macau)," in *Country Reports on Human Rights Practices - 2007*.
- vii Klein, Naomi, "China's All-Seeing Eye," *Rolling Stone*, 29 May 2008, <http://www.rollingstone.com/politics/story/20797485?chinas_allseeing_eye> (11 June 2008).
- viii Bradsher, Keith, "At Trade Show, China's Police Shop for the West's Latest," *New York Times*, 26 April 2008, <<http://biz.yahoo.com/nytimes/080426/1194769047129.html?.v=13&prin>> (11 June 2008).
- ix Kessler, Glenn, "Cisco File Raises Censorship Concerns," *Washington Post*, 20 May 2008, <<http://www.washingtonpost.com/wp-dyn/content/article/2008/05/19/AR2008051902661.html>> (12 June 2008).
- x Bradsher, Keith, "China Finds American Allies for Security," *The New York Times*, 28 December 2007, <<http://www.nytimes.com/2007/12/28/business/worldbusiness/28security.html>> (11 June 2008).
- xi Bradsher, Keith, "At Trade Show, China's Police Shop for the West's Latest"
- xii MacKinnon, Rebecca, "My Conversation with Cisco," *Rconversation*, 22 July 2005, <http://rconversation.blogs.com/rconversation/2005/07/my_conversation.html> (9 June 2008).
- xiii Bradsher, Keith, "At Trade Show, China's Police Shop for the West's Latest"
- xiv Fallows, James, "The Connection Has Been Reset," *The Atlantic*, March 2008, <<http://www.theatlantic.com/doc/200803/chinese-firewall>> (13 May 2008).

-
- xv "Helping Big Brother Go High Tech," *BusinessWeek*, 18 September 2006,
<http://www.businessweek.com/magazine/content/06_38/b4001067.htm> (11 June 2008).
- xvi Walton, Greg, "China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China," *International Centre for Human Rights and Democratic Development*, 2001,
<<http://www.ichrdd.ca/english/commdoc/publications/globalization/goldenshieldeng.html>> (11 June 2008).
- xvii Bradsher, Keith, "China Finds American Allies for Security"
- xviii "Helping Big Brother Go High Tech"
- xix Bradsher, Keith, "At Trade Show, China's Police Shop for the West's Latest"
- xx "Helping Big Brother Go High Tech"
- xxi Bradsher, Keith, "At Trade Show, China's Police Shop for West's Latest"
- xxii Klein, Naomi, "China's All-Seeing Eye"