Submission in Response to BIS Request for Public Comments on Crime Control License Requirements in EAR

June 17, 2008

For all inquiries, contact:

Fiona Gorton
Resources Officer
Omega Research Foundation
Bridge 5 Mill
22a Beswick St
Manchester, M4 7HR (United Kingdom)
info@omegaresearchfoundation.org

Colby Goodman,
Program Manager, Child Soldiers & Arms Transfers,
Amnesty International USA
600 Pennsylvania Ave. SE
Suite 500
Washington, DC 20003
cgoodman@aiusa.org
Submission in response to
BIS Request for Public Comments on Crime Control License Requirements in EAR

From Amnesty International USA & the Omega Research Foundation

17 June 2008

Summary of recommendations:

Amnesty International USA and the Omega Research Foundation propose several changes to the crime control licensing requirements:

- Adding several items to the CCL, including: goods designed for the execution of human beings, additional biometric technologies, communications interception technology, web filtering technology, certain surveillance technologies, acoustic weapons, water cannon systems, and law enforcement training simulators.

- Expanding and clarifying ECCNs covering: specially designed instruments of torture, restraint devices, police helmets/shields, saps, discharge type weapons, night vision, RFID chips, and smart cards.

- Disaggregating some ECCNs which combine civilian equipment with law enforcement equipment, for the purpose of increasing transparency in reporting.

- Removing the license exception for the export of restraints and discharge type weapons to Canada, as this exception may currently present a diversion risk.

- Adding a law enforcement catch-all for a small list of countries currently under US embargoes, which we propose to call "CC Column 4."

The following is a submission from Amnesty International USA (AIUSA) and the Omega Research Foundation in response to the Request for Public Comments on Crime Control License Requirements in the Export Administration Regulations (Docket No. 080229350-8434-01). We have drafted this submission to address the specific nature of the notice of inquiry, namely that the purpose of the crime control license is the “support of U.S. foreign policy to promote human rights throughout the world” (15 CFR 742.7(a)), and that BIS is seeking recommendations for the addition, removal or alteration of items subject to crime control restrictions. In addition, as far as possible, we have tried to provide reasoned explanations, and have attempted to mitigate excessive costs on transactions for US manufacturers.

The Omega Research Foundation is a UK-based nongovernmental organization, founded in 1990 to research the use and international transfer of Military, Security and Police (MSP) technologies, and these technologies’ impact on human rights. Over the last 15 years, Omega has developed unique expertise and resources to examine the manufacture of, and global trade in, equipment that can be used to commit torture, cruel, inhuman or degrading (CID) treatment or punishment, and other serious human rights violations. Omega has provided research support for numerous other human rights organizations, campaigning organizations, national governments, and intergovernmental bodies, including Amnesty International, Oxfam, Saferworld and the UN Special Rapporteur on Torture.

In drafting the recommendations below, Omega has been informed by its experience monitoring and evaluating the implementation and operation of European Council Regulation No 1236/2005 “concerning trade in certain goods which could be used for capital punishment, torture or other cruel, inhuman or degrading treatment or punishment” (OJ L 200, 30.7.2005, p. 1) (“Regulation 1236/2005” or “the Regulation”). This Europe-wide law provides for “rules governing trade with third countries in goods that could be used for the purpose of capital
punishment or for the purpose of torture and other cruel, degrading or inhuman treatment or punishment, and in related technical assistance." Although most of the equipment in this EC Regulation is covered already by the US Crime Control license requirements and other parts of the CCL, AIUSA and Omega have proposed several changes to fill gaps in US export control law.

We have separated our recommendations for additions and amendments into three sections: (1) categories of equipment not yet covered in the list, (2) expansion or clarification of existing categories, and (3) destination-specific license requirements.

We are grateful for the US Commerce Department's responsiveness to concerns from human rights organizations about the Commerce Control List in the past. We are aware that, in several instances, changes have been made to Crime Control ECCNs to improve the transparency and coverage of export authorizations for equipment often implicated in human rights violations and abuses. We hope the same will happen with the suggestions generated by this review.

1. Categories of equipment not covered in the list

(a) Goods designed for the execution of human beings.

Although the trade remains little publicized, specialized goods designed for the execution of human beings are manufactured and traded commercially. In the USA, for example, a Boston company, Fred A. Leuchter Associates Inc, claimed credibly to have supplied lethal injection execution systems to several US states on a commercial basis until its dissolution in October 1998. Similarly, the Omega Research Foundation and Amnesty International have presented evidence of an international trade in specially designed hanging ropes, and of detailed technical specifications for such ropes. Authorities in India and Trinidad & Tobago have reportedly purchased specially designed hanging ropes since 1999, in the latter case reportedly imported specially from the UK; and in 2001 a Sri Lankan company posted a tender to an EU-based tenders website for “Noose (Rope) to be used in the gallows.”

The introduction of specialized execution equipment has also been reported in certain countries seeking to exploit the bodies of executed prisoners. For example, execution by gunshot has reportedly been replaced with mobile execution vans fitted with lethal injection systems in some Chinese provinces, arguably facilitating an illegal trade in harvested organs, according to Amnesty International.

The grave humanitarian impact of specialized execution equipment, the proliferation of higher-technology methods of execution which are amenable to control through trade controls, and the existence of some international trading in such goods, all suggest the need and opportunity to add specialized execution equipment to the crime control list. Although the trade's opacity makes it difficult to gauge its size, basic limitations to the size of the "execution market" make it unlikely controls would have significant US commercial impact.

**Recommendation:** Other jurisdictions have introduced list-based controls on execution equipment, such as Regulation 1236/2005 of the European Union, which prohibits the export of:

3. Times of India, October 16 2006, "Special rope for Afzal's execution costs Rs 675": Daily Record, June 5, 1999, "THREE MURDERERS GO TO THE GALLOWS AS A FINAL PLEA FOR MERCY IS REJECTED"
4. www.ecurope.com accessed February 27 2001: "Offer to Buy. Subject Heading: [LK]: Noose (rope) to be used in the gallows. Category: Security & Protection Products. Preferred Region: Worldwide. Trade Lead Message: A supplier or a manufacture of Noose (Rope) to be used in the..."
5. Quoted in 'China makes ultimate punishment mobile', *USA Today*, June 15 2006
(b) Biometrics.

The current CCL already imposes broad crime control license requirements for two types of biometric technologies (fingerprint and voice print), which include any associated technology for their development, production or use. These are listed under a range of ECCNs including 1A985, 3A980, 3A981, 3D980, 3E980, 4A003, 4A980, 4D001, 4D980, 4E001 and 4E980.

Developments in biometric technologies have been rapid in recent years. Such technologies are now routinely used in combination with, for example, smart cards and computer information systems to provide governments with powerful tools for monitoring and tracking citizens’ activities. With such systems unique personal data can potentially be held and copied indefinitely. The use of such technologies in e-passports and national identity card systems is becoming widespread, including in Asian industrializing nations such as China and Thailand. It is of concern that in many countries adequate legal safeguards do not exist to prevent the misuse of such equipment to monitor and interdict human rights defenders; to curtail legitimate political, cultural, religious and social activities; and to identify and harass citizens based upon ethnicity, cultural background and other features.

We recognize that the range of biometrics now encompasses a large body of businesses and technologies: existing techniques include
- Hand geometry recognition
- Palm-vein recognition
- Ear canal acoustic properties recognition
- Vascular pattern recognition
- Iris recognition
- Retinal recognition
- Face recognition
- Facial thermography
- DNA profiling
- Gait recognition
- Odour / scent recognition
- Speech recognition
- Keystroke recognition
- Signature / handwriting analysis

However, it seems inconsistent to apply controls to certain biometric technologies and not others, given that all can be used in similar ways to identify, track and monitor individuals. We believe instead, therefore, that existing controls on voice printing and fingerprinting technologies should be replaced with a general control on devices and technology to recognize human biometric features.

**Recommendation:** In order to update the existing intention of the CCL to control biometric technologies, and to reflect developments in biometric technologies, the CCL include all devices, technology, computers and software for the recognition or analysis of human biometric features.

Components for such systems and technology for the development, production or use of such equipment should also be listed.
We recognize that the anticipated burden on industry resulting from such changes would be significant: although some biometric systems are already covered by the CCL, expansion of the list to cover all biometric technologies and systems would bring many companies under the purview of CCL / BIS for the first time.

However, the CCL already demonstrates an intent to control biometric equipment, as shown by existing stringent controls on fingerprint and voice print technology. An expansion of these controls would simply be consistent with this existing intent and developments in technology.

(c) Communications interception, web filtering, and surveillance technology.

The potential for misuse of a range of communications interception, surveillance and internet filtering technologies are beginning to be recognized by the human rights community. This is particularly the case as large-scale, integrated surveillance, interception and content filtering systems are applied to public spaces and entire communications infrastructure. These technologies are used by some states to suppress political and religious speech, and to target human rights defenders, political and religious activists for arrest and ill-treatment. In Vietnam, for example, four users of a PalTalk chat room in which criticisms were made of the Vietnamese government were arrested in October 2005 and accused of attempting to overthrow the government. The four were beaten, and three were held incommunicado for nine months. One was re-arrested six weeks later in an internet café in Ho Chi Minh City after logging onto a PalTalk chat room.

We believe that, where they are technically definable, technologies that make such monitoring and harassment possible should be brought within export controls, at least to a well-defined set of destinations.

Communications interception technology: CCL 5A980 covers “devices...primarily useful” for the interception of communications. Communications interception technology has developed well beyond discrete “devices” to encompass software or hardware facilities built into telephony and internet infrastructure for the lawful (or unlawful) interception of all communications. Such technical features of communications infrastructure like digital telephone exchange switches are, indeed, mandated by laws in several states, including the USA. In some states, however, such legislation lacks adequate human rights and privacy safeguards. These infrastructural items are not “primarily” designed for communications interception, but nonetheless make such interception possible on a far greater scale than the kinds of discrete wire-tapping or bugging devices listed in EAR guidance.

For example, US company UTStarcom announced in October 2005 that it is providing wireless internet telephony infrastructure for China Telecom in Jiangsu, Guangdong, Sichuan, Zhejiang and Yunan provinces, and Chongqing municipality, using its mSwitch routing platforms. We do not know where such routing platforms have been manufactured. Undated mSwitch specifications state that they incorporate “lawful intercept” (LI) facilities. If UTStarcom has supplied mSwitch platforms of these specifications to China, they could allow law enforcement agencies where the routing platforms are installed to intercept communications passing through the UTStarcom infrastructure.

To prevent these technologies reaching states likely to use them to facilitate human rights violations, we believe that the 5A980 category should be expanded to explicitly include devices, software and technologies enabling the interception of communications. We

---

See information on Amnesty International internet freedom campaign at www.irrepressible.info
Communications Assistance for Law Enforcement Act 1994
For example, EAR Sec. 742.13 (a)(2) definition of "Communications intercepting devices" includes the martini olive bug.
UTStarCom Press Release dated October 18 2005 (http://files.shareholder.com/downloads/UTSI/0x0x164976/4536a59a-93d0-4105-8468-782f3816ac71/176645.pdf)
recognize that the widespread use of lawful intercept protocols in many countries would lead this definition to catch much telephony and internet hardware and software, and we would not wish such an expansion of the CCL category to impede the beneficial spread of communications infrastructure. However, we would anticipate that manufacturers could produce export versions of their products which did not include interception facilities, allowing legitimate and beneficial communications products to be exported to problematic destinations without being caught by the category, as is already the case with some communications technologies incorporating export-controlled encryption.\(^\text{12}\)

**Web filtering software and technology:** Internet filtering, which allows internet providers or users to filter out web content containing particular content or language, is widely used for unproblematic applications, such as to prevent child access to pornography in schools. However, installed in internet infrastructure itself, it is also used by a number of repressive governments to censor political and religious speech, and to prevent their citizens from accessing information critical to their governments. The Open Net Initiative, a joint research project between computing researchers at the Universities of Cambridge (UK), Oxford (UK), Harvard and Toronto, has identified the use of US-origin web filtering software by authorities in Burma to suppress free speech in this way.\(^\text{13}\)

For this reason, we believe that web filtering software and technology should be added to the crime control list for destinations where political activity and free speech are most seriously circumscribed. (See below, Section 3, “law enforcement catch-all for embargoed destinations.”)

**Surveillance video technology:** Much attention has recently been given to large-scale CCTV installations for public security authorities in China, often with the technical assistance or products of US companies.\(^\text{14}\) This concern has a long and justified pedigree: after the Tiananmen Square massacres in 1989 it was revealed that surveillance cameras installed in the Square, and reportedly used to identify protesters whose pictures were circulated on Chinese television, were produced by Pelco (USA), as part of a UK-supplied Scoot surveillance system.\(^\text{15}\)

Nonetheless the massive proliferation of CCTV cameras for governmental, commercial and domestic applications, and their widespread production outside of the USA, makes it both difficult and possibly ineffective to introduce export controls on CCTV cameras themselves.

However, controls could be applied to technologies that make CCTV and video surveillance systems amenable to facilitating human rights violations through the analysis of video images and feeds to identify individuals, spot proscribed activities and so on. These include biometric technologies discussed above such as facial recognition software, and also “intelligent” video analysis software. For example, US companies Texas Instruments and Object Video have reportedly entered into cooperative agreements with Chinese DVR manufacturer Hikvision, allowing Hikvision to adopt TI’s “DaVinci” package of digital signal processing chips and software, and to use ObjectVideo’s “intelligent video analysis” software.\(^\text{16}\) The Hangzhou government claims that Hikvision “is a subsidiary of the 52nd Research Institute of China Electronics Technology Group Corporation [CETC], as a Sino-Foreign joint venture.”\(^\text{17}\) CETC is a state-owned corporation; its 52nd Research Institute, according to industry news sources


\(^{16}\) “Technology Giants’ View of China”, *A & S Asia* magazine, July 2007

and the US Defense Department, is focused on military research, and make digital video
recorders with military-standard anti-shock protection for tanks and military vehicles.\(^{18}\)
According to Hikvision's advertising materials, Hikvision have been involved in the Chinese
Ministry of Public Security's "3111 Project," which aims to integrate surveillance systems in
several Chinese cities; and have also supplied security products for the Qinghai to Tibet
railway.\(^{19}\) HikVision promote themselves as the largest producer of CCTV cameras in China,
and suppliers of Digital Video Recording (DVR) equipment to the 2008 Beijing Olympics.\(^{20}\)

**Recommendation:** CCL crime controls be extended to cover these three technologies:
devices, technology and software enabling the interception of communications; devices,
technology and software for internet filtering; and devices, technology and software designed
to analyze images from CCTV or surveillance systems. BIS should work with industry and
academic technology experts to adequately define technical specifications for these
technologies.

We realize that this would impose some burden on US industry. This is inevitable if the US
government genuinely wishes to limit certain states' abilities to monitor and repress their
citizens' free speech, political and religious activities, facilitated by these key technologies.
While concerns about the abusive surveillance of citizens have global dimensions, at a
minimum these three types of equipment should be subject to crime control license
requirements for the limited list of countries we propose to be added as "CC Column 4." (See
Section 3(c), “law enforcement catch-all for embargoed destinations.”)

(d) New Less-Lethal Weapons.

*Long-Range Acoustic Device (LRAD):* One emerging category of technology that should be
added to crime control license restrictions is acoustic weaponry. Although Category XVIII of
the International Traffic in Arms Regulations (ITAR) imposes controls on directed energy
systems including laser, particle beam, high power radio-frequency systems. It is unclear
that this ITAR category includes acoustic weapons and crowd-control devices. Since
acoustic weapons have so far been primarily used by law enforcement authorities (including
some military units), they should be included in the Commerce Control List and subject to the
crime control license requirement.

For example, at the time of this writing (June 2008), the Long-Range Acoustic Device
(LRAD), manufactured by American Technology Corporation (ATC) has received
significant publicity following reported exports to Singapore, Korea and China; and its
reported 2007 use in breaking up nonviolent protests in Tbilisi, Georgia, where a researcher
for Human Rights Watch observing the demonstration described the noise produced
by the LRAD as "unbearable," and interviewed a witness who stated that the noise contributed

\(^{18}\) US DoD, Annual Report on The Military Power of the People's Republic of
China, 2002

\(^{19}\) HikVision advertisement, obtained October 2007

\(^{20}\) Photographs of HikVision marketing materials obtained at Securex security trade fair,
Johannesburg, June 2007
greatly to the initial panic among protestors.\(^{21}\) Most recently, the LRAD was exhibited at the April 2008 China Police exhibition in Beijing: the Asia-Pacific Xuanxhao Group (APX) are distributors of the LRAD in China, and the LRAD was also shown mounted on a military vehicle manufactured by Dong Feng. It is not clear whether Dong Feng has permission to distribute the LRAD, or if the Dong Feng with the LRAD was also an APX display.

Although ATC now claims the LRAD is not a weapon but a “communications system,”\(^{22}\) the LRAD was used in 2005 against pirates off the coast of Somalia and to disperse protestors in Georgia in November 2007.\(^{23}\) ATC press releases up to 2004 described the use of the LRAD for “area denial of personnel,” “crowd and riot control” and “psychological operations”, acting as “a less-than-lethal first responder acoustic capability to protect high value assets.”\(^{24}\) Describing the LRAD in an interview for CNN in 2004, Carl Gruenler, vice president of military and government operations for American Technology Corp, said: “Inside 100 yards, you definitely don’t want to be there”…adding that the device is recommended for a range of 300 yards or less.\(^{25}\)

**Recommendation:** We believe that the CCL should control acoustic and other emerging “less-than-lethal” technologies not controlled by the ITAR. If acoustic crowd control devices and weaponry are to be included in the CCL, the phrasing should be sufficiently broad to include future generations of acoustic weaponry and related technology, parts and service therefor.

(e) Water Cannon and other riot control delivery systems.

The CCL covers a wide range of riot control agents, but does not cover delivery systems specifically designed for them, or an ECCN for water cannons, a commonly used law enforcement item. These devices, including “backpack” chemical sprayers, fixed position “foggers” and vehicle-mounted water cannon, are widely used to suppress peaceful demonstrations.

In addition to the properties of controlled irritants themselves (most of which are widely available from sources outside the USA), several of these delivery mechanisms raise concerns regarding safety, lethality, discrimination and the potential for ill-treatment. Of particular concern are:

- **larger backpack or tank irritant “sprayer” devices,** whose number on the commercial law enforcement market have markedly increased in the last decade. These are designed for the wide-area delivery of irritant liquid or powder which was often previously delivered at close quarters in hand-held sprays. These raise questions about the possibility of their discriminate use, and their proportionality as area clearance devices, particularly since they deliver liquid or powder irritants which will adhere to subjects and, without decontamination, will continue to deliver pain and irritation even when the subjects have moved away from the area (unlike irritant smoke delivered through grenades and canisters). One of these devices promises to deliver screens of “up to 100%” CS (o-Chlorobenzylidene malononitrile) powder, which raise serious concerns about the safety of the device.\(^{26}\)

---


\(^{23}\) “Cruise Lines Turn to Sonic Weapon”, BBC News, November 8, 2005 (http://news.bbc.co.uk/2/hi/4418748.stm)


\(^{26}\) Company specifications for SNPE (France) Crotale 2000 irritant sprayer (n.d.): “Irritant agent generators can release either a screen of powder composed of 10 to 100% CS, or a screen of tiny droplets containing 2 to 20% dissolved CS.”
• **Fixed-position “fogging” devices, spray dispensers or smoke generation units** for indoor installation in secure rooms such as bank vaults, and also in places of detention.\(^{27}\) To our knowledge there has been little safety testing of these devices. It appears that some manufacturers and installers regard them as inherently “harmless,” and therefore do not produce guidelines regarding, for example, the minimum enclosed space in which their units are installed (which will alter the likely concentrations resulting from their use). This is despite their delivering OC or CS which may be harmful or even lethal in enclosed spaces at high concentrations.\(^{28}\)

• **Many commercially-available water cannon** are now designed to deliver chemical irritants.\(^{29}\) Even where chemicals are not used, anecdotal reports from crowd control situations where water cannon have been used indiscriminately and to exert excessive force, suggest the possibility of eye injuries if water cannon are misused.\(^{30}\) Although the scientific literature on injuries from high-pressure liquid jets and sprays remains very limited, some literature also records eye injuries from high-pressure water jets.\(^{31}\)

![Dragon 9500 irritant sprayer. According to accompanying specifications from the manufacturer:](image)

> “When fired at short range or within closed area, its effects can be devastating (The use of such irritant agent generators should only be considered for extreme situations)

> Irritant agent generators can release either a screen of powder composed of 10 to 100% CS, or a screen of tiny droplets containing 2 to 20% dissolved CS.”

---

\(^{27}\) See, e.g., Arias Tech Ltd ‘FlashFog’ unit, a fixed unit rapidly generating a dense vapour fog by forcing a glycol/water mixture (to which “lachrymatory agents (OC, etc.) can be added”) through a heated block assembly, boiling the water violently and breaking the glycol down into micro-droplets (Flashfog product specifications, n.d., obtained August 2007)

\(^{28}\) For instance, US manufacturer Federal Laboratories’ product specifications state that “Firing one Federal No. 230 Flite-Rite [tear gas projectile] in a room [eight-feet by eight-feet by seven-feet], could endanger the life of an average subject if he stayed in the room for seven minutes”

\(^{29}\) For example, Manta riot control water cannon vehicles produced by Protech Armor Systems (USA) incorporate “High-pressure chemical and dye dispensing cannon with adjustable spray stream features” (http://www.protecharmored.biz/systems/special/control.asp accessed June 16, 2008)

\(^{30}\) See, e.g., Korean broadcaster Korea 21 reported in early June that a high schoolgirl had received an eye injury from the water cannon in recent demonstrations and may lose her eyesight. “Demonstrators Blocked From Approaching Cheong Wa Dae”, *Korea Times*, June 1, 2008

Recommendation: In the spirit of existing controls on riot control agents, the CCL should be updated to include crowd-control technologies and systems designed to deliver water or chemical irritant sprays, including but not limited to:

- Water cannon specifically designed or modified for the purposes of police use, and armored or unarmored water cannon vehicles.
- Hand held or backpack mounted water cannon systems specifically designed or modified for the purposes of police use (e.g. for cell extraction or crowd / riot control including those modified for delivery of chemical agents)
- Fixed water cannon systems, for example installations and systems for use in correctional facilities

(f) Law enforcement training equipment and simulators.

The ITAR currently controls training equipment and simulators “specifically designed, modified, configured or adapted for military purposes.” Several US companies also market training equipment and simulators specifically for law enforcement use, which we are not clear would be necessarily controlled under this ITAR definition.

For example, the MILO Range produced by IES Interactive Training Inc is a portable simulator system providing training for a range of (BIS-licensable) weapon types including OC/Mace, Tasers and firearms, and a software library of policing scenarios including “car stop, building search, Corrections, SWAT, Hijack, Markmanship, Range programmes, Escort duty, Robbery, Burglaries, Search warrants.” IES exports its products, stating that it has a client base for its simulators in over 20 countries, including law enforcement training establishments in Mexico, Malaysia, Ecuador and the UAE.

It seems inconsistent to require export licenses for military training and simulator systems, but not for trainers and simulators for police and law enforcement weapons which are themselves licensable under the EAR.

Recommendation: We believe that, at a minimum, EAR categories covering law enforcement and security weapons - 0A978 (Saps), 0A984 (Shotguns), 0A985 (Discharge type arms) and 1A984 (chemical agents) - should be expanded to include “training equipment and simulators therefor.”

2. Expansion and clarification of existing categories

(a) 0A983: Specially designed instruments of torture

At present the CCL lists two illustrative items under this ECCN – thumbcuffs and thumbscrews, and there is a policy of denial for license applications for this category. We are also aware of two other types of commercially traded equipment whose only reasonable use is for torture or ill-treatment. The second device is reported in use by security forces in several countries with persistent reports of torture and ill-treatment. In accordance with the intention of the category to control all specially designed implements of torture, the descriptive text of 0A983 should be amended to explicitly include finger cuffs and spiked batons:

Finger cuffs: These items operate similarly to thumbcuffs, already explicitly controlled under 0A983: adding them is a logical extension of the existing control on thumb cuffs. Our data indicate that the two most prominent suppliers of finger cuffs are based in Israel, whereas 20

---

32 ITAR § 121.1 (“The United States Munitions List”), Category IX
34 Arotech Corporation (parent company) form 10-K for fiscal year ended December 31 2007.
US-based firms distribute thumb cuffs. Therefore, adding finger cuffs to the category is likely to have minimal commercial impact on US firms, but will effectively prevent the export of such emerging restraint equipment.

Spiked batons: Spiked batons, often referred to as “sting sticks” or “wolf sticks,” are mass-produced by Chinese policing equipment companies. They are evidently traded domestically and internationally; spiked batons matching this description have been reported in use on religious prisoners in China and demonstrators in Nepal, have been photographed in Nepal and Tibet, and have been recently exported to Thailand, according to a November 2007 interview with a Chinese police equipment manufacturer recently obtained by the Omega Research Foundation.

We know of no US manufacturers or traders in such batons, so effectively prohibiting their trade through inclusion in 0A983 would likely have little commercial impact. Their trade in other parts of the world, however, indicates the need for inclusion on the CCL.

(b) 0A982: Restraint devices.

Currently, the definition of restraint devices includes “leg irons, shackles, and handcuffs; straight jackets, plastic handcuffs; and parts and accessories, n.e.s.” Restraint technology has progressed since the writing of this definition, with the introduction of multiple-point (four-, five- and six-point or above) restraint devices, especially shackle boards and restraint chairs.

Within the US, the misuse of these devices — particularly restraint chairs — has led to prisoners’ deaths, usually by asphyxia, and serious accusations of abuse. Omega’s data

---

37 A February 2002 account from Falun Gong members details how Chinese police officers threatened to use such equipment at Wanyaoshan Detention Centre: “Policewoman Fan saw one of the practitioners lying on the ground motionless, so she kicked her brutally and said, “Get up! Don’t play dead. If you don’t get up now, I’ll use the spiked baton to beat you to death.”
38 Asian Human Rights Commission—Urgent Appeals Program, http://www.ahrchk.net.ua/mainfile.php/2003/461/: “He has lost his right eye after being subjected to an indiscriminate baton charge by the Police during a peaceful torch rally on 11May 2003 in Ratnapark, Kathmandu. Mr Sharma sustained severe injuries to both his eyes because the Police allegedly hit him several times with iron-spiked sticks and specifically targeted his eyes.”
suggests that almost all “restraint chair” manufacturers and distributors are US companies: there are four manufacturers and distributors in the US, one in China, and a distributor in Israel that appears to distribute US-made chairs.

One US manufacturer, AEDEC International Inc., makes restraint chairs specially designed to fit juveniles, which were displayed at the American Correction Association “Congress of Correction” in August 2003. AEDEC has also reportedly sold restraint chairs to the United Arab Emirates (although it is not known whether they included the juvenile version).

Because of the potential for misuse of such chairs—not only in law enforcement/corrections settings but also against children and the mentally ill—such restraint devices should be subject to crime control license restrictions, especially because the US is currently the primary source for this technology.

Even if such multiple-point restraint devices are already implied in the definition of 0A982, the definition should be changed to explicitly include them.

Last, BIS annual reports list “thumbcuffs” in the reported 0A982 licenses. While we realize this is likely because the code’s description has not been updated to reflect the inclusion of thumbcuffs in the 0A983 (specially designed instruments of torture) category, licenses for thumbcuffs should not be processed under the 0A982 ECCN.

(c) 0A978: Saps.

Other than saps, at present the CCL does not include any kinetic impact or striking weapons such as police batons. Such equipment is much more widely used than saps by law enforcement and security forces world-wide, and is often reported in cases of human rights violations. Our analysis of a selection of publicly available Amnesty International human rights reports, undertaken to investigate the use of particular types of equipment in instances of torture or CID treatment, showed that beatings accounted for almost 60 percent of a total of

---


41 Company Information obtained at ACA 2003 (August 2003)

1,132 instances of abuse – the highest figure for any “action” type. Of these beatings, the most common specialist implement use was a police baton.\footnote{Omega Research Foundation review of Amnesty International human rights documentation for 1996-2006, unpublished paper, 2007.}

In order to be consistent with 0A978’s intention to control easily misused kinetic impact weapons, the full range of kinetic impact or striking weapons should be listed on the CCL. The simplicity of many batons and striking weapons often makes it appear difficult to adequately define or control such implements through export controls. In fact, however, a range of specially designed impact weapons are both technically amenable to definition in export controls, and of particular human rights concern, given their ability to exert much greater force than “ordinary” batons and truncheons, and cause more serious injuries when misused by poorly-trained or unregulated users.\footnote{Police Complaints Authority, UK. (1998), ‘Striking a balance: the police use of the new batons’, (Crown) ISBN 0-9553157-1-1 ; See also ‘Police Switch to Baton’, New York Times, January 1, 1989 (http://query.nytimes.com/gst/fullpage.html?res=950DE3DA143FF932A35752C0A96F948260) : “Since the PR-24 generates three to four times the striking power of a nightstick, we stress, no blows above the shoulders”}

These include steel friction-lock extendable batons; sjamboks (used by law enforcement in Southern Africa and Zimbabwe); side-handle batons (T-batons, tonfas); whips; billies; and lead-lined “slapper” or “sap” gloves.

The feasibility of defining and controlling such equipment through export controls is demonstrated by controls already introduced in several countries. The UK has banned the unlicensed import or possession of side-handled and friction-lock batons since 2004.\footnote{The Criminal Justice Act 1988 (Offensive Weapons) (Amendment) Order 2004}

In 2001, the Australian government amended its Customs (Prohibited Exports) Regulations (1958) to include a range of equipment including: “batons, clubs, riot sticks and similar devices of a kind used for law enforcement purposes,” and “whips.”

Such devices are widely traded by US companies. For example, Master Cutlery Inc of New Jersey imports billy clubs “made in Taiwan,” according to marketing literature;\footnote{Company brochure obtained March 2006} PR24 aluminium nightsticks manufactured by Monandock Lifetime Products Inc are offered for sale by a Hong Kong police equipment supplier, Selpro Tactical Ltd.\footnote{http://www.selpro.com.hk/new/riot.htm accessed 15 June 2008; “King Beating Focuses Attention on Police Taser, Nightstick”, Associated Press, March 29, 1991}

\begin{center}
\textbf{Recommendation:} ECCN 0A978 should be expanded to include::
\end{center}

- Straight, expandable (extendable) and side-handle batons (T-batons, tonfas) of any length or any other batons and similar devices designed for law enforcement purposes,
- Whips, sjamboks and other similar devices,
- Saps, Billys, Slappers and Sap Gloves.

(d) 0A985: Discharge type arms (electroshock).

Electroshock devices are becoming one of the most widely used police technologies capable of abuse for torture and ill-treatment, and thus, as the Commerce Control List recognizes, a category of items particularly necessary to subject to crime control license restrictions.\footnote{Amnesty International, The Pain Merchants (December 2, 2003) (http://www.amnesty.org/en/library/info/ACT40/008/2003)} Although the description of ‘discharge type arms’ may act as a catch-all to include all electroshock devices from weapons to electrified restraints, we believe that it would be helpful for exporters, and in enforcing the comprehensiveness of this category, to expand the illustrative list in 0A985 to include explicitly some newer and emerging electroshock devices.
Recommendation: The illustrative list of devices in ECCN 0A985 should be expanded to explicitly include fixed-position electroshock weapons and munitions, electroshock projectile munitions, "stun cuffs" and other items designed for restraining human beings through the administration of an electric shock. All of these are produced by US manufacturers with overseas distributors.49

The phrase “discharge type arms” could also be replaced with an explicit statement that the category covers all weapons and devices designed to incapacitate or immobilize human beings through the administration of electrical shocks or impulses.

Since this amendment would simply have the effect of clarifying the competence and comprehensiveness of the category, rather than expanding its coverage, we do not believe it will have a commercial impact, other than to encourage manufacturers of already- licensable equipment to seek export licenses correctly.

(e) Widely available commercial technology useful for internal repression.

A number of other widely available technologies fall only partially within crime control licensing and are particularly useful for internal repression, but also have wide commercial applications. In particular these include 1st and 2nd Generation night vision devices, and smart cards/RFID chips useful for tracking and detecting people.

Night vision: Commerce Department currently has crime control license restrictions on Generation III and IV night vision equipment, according to 6A002.c. Other night vision devices are not, however, controlled. Yet there exists some evidence that Generation I and II night vision equipment of US origin is being traded for police use in China, posing as much of a risk of contributing to internal repression as Gen III or Gen IV equipment. For example, a catalogue for a Chinese police equipment company, HJGA, obtained in November 2007, includes pictures of Yukon Optics (Generation I) NVMT laser night vision riflescopes, and three types of Bushnell (USA) Generation I night vision monoculars: often used for hunting in domestic settings, but here clearly being intended by the Chinese supplier for police or security use, since they are presented alongside police clothing and a submachine gun mounted with a holographic sight. We have not been able to verify whether Yukon Optics or Bushnell have in fact supplied such devices to HJGA, but without CCL licensing requirements, supplying such devices to known Chinese police suppliers would be uncontrolled.

<table>
<thead>
<tr>
<th>Recommendation: all night vision devices (all generations) should be added to the CCL and subject to crime control license restrictions for the most egregiously repressive or human-rights-abusing states (see Section 3(c) for proposal on CC Column 4).</th>
</tr>
</thead>
</table>

The European Union has already introduced such controls with respect to Burma through EC Regulation No 817/2006 of 29 May 2006, which prohibits the sale of any “[n]ight vision and thermal imaging equipment and image intensifier tubes or solid-state sensors therefor” to Burma (Annex I of Regulation 817/2006).

Smart cards and RFID chips: Similarly, the licensing of “smart cards” (5A992.a) currently falls under anti-terrorism controls (AT Column 2), rather than crime controls, and does not explicitly include Radio-Frequency Identification (RFID) chips. RFID chips are increasingly widely used as tracking devices. Despite their numerous commercial uses, they can also allow a government to track its citizens, and therefore should be controlled to certain destinations where they are likely to be used to track and target political or religious activists,
to facilitate unlawful detention and for other human rights violations. China, for instance, is reportedly planning to include RFID chips in its new national ID cards.  

**Recommendation:** Smart cards and RFID chips should be included in crime control licensing, at a minimum for destinations where the most egregious human rights violations involving the surveillance and harassment of citizens persist.

We recognize the wide and legitimate use of night vision for security and sporting activities, and of RFID chip systems for applications such as inventory tracking and commercial stock control. We therefore understand that to impose license requirements for all night vision, smart cards and RFID chips to all CC Column 1 destinations would be extremely burdensome on industry. Therefore, we propose RFID chip systems and the uncovered night vision devices (Generations I and II) be subjected to crime control license requirements only for the extremely limited “CC Column 4” list of countries proposed later in this document (see Section 3(c), “law enforcement catch-all for embargoed destinations”). (Night visions of types Generations III and IV should remain controlled by Column 1 destinations.)

(f) Disaggregating military and civilian equipment in the same ECCN.

Several crime control categories combine primarily civilian equipment with primarily law enforcement equipment, and combine equipment with wildly different technical characteristics. Some examples of these include:

- **0A982**, which includes straight jackets (primarily used in psychological and medical establishments) in a category with metal shackles, handcuffs and leg cuffs (primarily used by law enforcement and corrections officials).
- **1A984**, which includes commercial pyrotechnics and tear gas canisters, as well as pyrotechnic devices with dual commercial and military use.

It is important for Congress and the public to be aware of whether export authorisations granted for sensitive destinations constitute specially-designed law enforcement goods, or commercial products. In these cases, either (a) the categories should be split to clearly differentiate between different users for equipment (police/corrections versus medical, commercial versus military), or (b) reporting in BIS annual reports for Category D countries should disaggregate the medical/police and commercial/military uses of such equipment.

3. Destination-specific recommendations

(a) Canada exception for restraints and electroshock.

Restraints (handcuffs, leg cuffs) and discharge-type weapons are currently controlled to all export destinations except Canada. However, unlike several destinations that do require export licenses for crime control-restricted items from the US, Canada does not have export controls of this equipment, posing a diversion risk. The inadequacies of the Canadian export controls on restraints and electroshock weapons make it impossible to know if a reexport has occurred.

**Recommendation:** The exception for exports of ECCN 0A985 and 0A982 for Canada should be removed.

(b) Licensing and human rights concerns

Licensing decisions should be made with more attention to the human rights records of destination countries. Several US laws anticipate curbing the foreign assistance and export of police and military goods to countries with persistent human rights violations. For example, 22

---

U.S.C. §2304(2) states that: "no security assistance may be provided to any country the government of which engages in a consistent pattern of gross violations of internationally recognized human rights ... [L]icenses may not be issued ... for the export of crime control and detection instruments and equipment to a country, the government of which engages in a consistent pattern of gross violations of internationally recognized human rights."

The following are a sampling of US Department of Commerce-approved export license applications, reported by the BIS, about which we have questions about the destination countries’ human rights records:

- To Bulgaria for discharge type arms ($118,200 in 2004, $60,828 in 2007) and restraints ($3,858 in 2004, $17,290 in 2007), although the State Department’s 2007 country report for human rights noted that “police frequently beat criminal suspects, particularly members of minority groups.”

- To Russia for discharge type arms ($13,000 in 2004) and thumbcuffs, leg irons and shackles ($5,010 in 2005 and $65,065 in 2006), despite the State Department’s 2003 observation that “[p]hysical abuse by police officers usually occurred within the first few hours or days of arrest and usually took one of four forms: Beatings with fists, batons, or other objects; asphyxiation using gas masks or bags (at times filled with mace); electric shocks; or suspension of body parts (e.g., suspending a victim from the wrists, which are tied together behind the back).” A similar list of torture methods is given in the 2005 report.

- To Tajikistan for thumbcuffs, leg irons and shackles ($50,100 in 2006), although the State Department’s 2006 report noted that “[p]rison conditions remained harsh and life threatening,” and that “arbitrary arrest and detention remained serious problems.”

- To Ukraine for discharge-type arms ($90,000 in 2007), despite the State Department’s 2007 report’s observation that “police frequently employed severe violence against persons in custody,” and two deaths in police custody that year.

- To Vietnam for thumbcuffs, leg irons and shackles ($65,000 in 2006), although the State Department’s 2006 report noted that “the government continued to arrest and detain citizens for their political activities.” In March 2005 the Center for Religious Freedom noted that several arrested Vietnamese church leaders were “put in shackles, handcuffs and fetters for three days and nights. Their families brought them rice and water but the border guards did not allow them to eat or drink. Each day they allowed them to eat only two small bowls of rice and drink one bowl of water. Even at night they were not allowed to have the shackles taken off. The border guards said, ‘They are asking for help from their God, let us see if their God is going to help them or not’....When the people in the local government knew that we went to Hanoi to appeal, they continued to arrest many men, put them in shackles, and poured water into their nostrils.”

Without knowing the identities of the end users for this equipment, it is difficult to know whether it is likely they will be used in human rights violations. If the end users for this crime control equipment listed above is, however, the security forces, we would have concern about the patterns of human rights violations perpetrated by those end users. We may also have questions about the granting of licenses for crime control list equipment to other end users who have patterns of gross violations of human rights in countries not included in the “Country Group D:1 and Cuba” list.

---


A particularly obvious example of this apparent inconsistency in applying human rights considerations to license authorizations is the number and value of crime control category licenses granted for exports to China in recent years. The Tiananmen Square sanctions envision a suspension of the issuance of licenses for the export “of any crime control or detection instruments or equipment” (22 U.S.C. §2151). This law does not envisage the lifting of these sanctions until the President notifies Congress that China has lifted martial law, halted “executions and other reprisals against individuals for the nonviolent expression of their political beliefs,” released political prisoners, increased respect for internationally recognized human rights (freedom of expression, the press, assembly and association), and permitted a freer flow of information.

The following are the crime-control ECCNs with approved licenses valued at more than $5,000 to China, according to BIS annual reports since 2002:

<table>
<thead>
<tr>
<th>Year</th>
<th>ECCN</th>
<th>Number applications</th>
<th>Dollar value</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007</td>
<td>0A979: Police helmets, shields and parts</td>
<td>2</td>
<td>$61,832</td>
</tr>
<tr>
<td>2007</td>
<td>0A987: Optical sighting devices for firearms</td>
<td>4</td>
<td>$106,083</td>
</tr>
<tr>
<td>2007</td>
<td>4A003*: Digital computers/assemblies and related equipment</td>
<td>3</td>
<td>$4,000,255</td>
</tr>
<tr>
<td>2006</td>
<td>0A984: Shotguns, buckshot, shotgun shells</td>
<td>1</td>
<td>$204,000</td>
</tr>
<tr>
<td>2006</td>
<td>0A987: Optical sighting devices for firearms</td>
<td>11</td>
<td>$499,286</td>
</tr>
<tr>
<td>2006</td>
<td>6A002*: Optical sensors</td>
<td>1</td>
<td>$49,611</td>
</tr>
<tr>
<td>2005</td>
<td>0A979: Police helmets, shields and parts</td>
<td>1</td>
<td>$7,120</td>
</tr>
<tr>
<td>2005</td>
<td>0A984: Shotguns, buckshot, shotgun shells</td>
<td>1</td>
<td>$208,000</td>
</tr>
<tr>
<td>2005</td>
<td>0A987: Optical sighting devices for firearms</td>
<td>5</td>
<td>$355,600</td>
</tr>
<tr>
<td>2005</td>
<td>4A003*: Digital computers/assemblies and related equipment</td>
<td>6</td>
<td>$2,308,826</td>
</tr>
<tr>
<td>2005</td>
<td>6A002*: Optical sensors</td>
<td>2</td>
<td>$29,500</td>
</tr>
<tr>
<td>2003**</td>
<td>0A987: Optical sighting devices for firearms</td>
<td>2</td>
<td>$388,591</td>
</tr>
<tr>
<td>2003</td>
<td>6A002*: Optical sensors</td>
<td>1</td>
<td>$10,000</td>
</tr>
<tr>
<td>2002</td>
<td>0A987: Optical sighting devices for firearms</td>
<td>4</td>
<td>$41,007</td>
</tr>
</tbody>
</table>

Notes:
* indicates an ECCN in which there are other items not controlled for crime control reasons
** 2004 data was not available from the BIS website.

As this table clearly shows, crime control licenses were rarely approved in 2002, but approvals are far more frequent for this equipment in the past two years. At the same time, US equipment covered by the crime control requirements is being actively marketed in China at trade fairs. Chinese distributors have been marketing weapons scopes they claim are from two US companies, ATN and EOTech, at Chinese police and security equipment trade fairs since at least 2004. According to Commerce Department regulations, all such scopes require license approval for export to China. Although EOTech’s website acknowledges the requirement to get a license, Omega has identified sights which appear visually identical to distinctive EOTech scope models on Type 79 submachine guns in use by Chinese police in Xi’an during 2005, although we are unable to confirm without close inspection whether these are genuine US-produced EOTech scopes.

---

58 Omega Research Foundation database
59 Getty Images newswire photographs taken during police demonstration, Xi’an, China, February 2005 and July 2005
There is no suggestion of wrongdoing by EOTech: even if these are genuine EOTech scopes, they may have fallen within the licenses for optical sights listed above. The question remains of whether the Commerce Department should license such equipment, in light of the wording and intent Tiananmen Square sanctions.

These recommendations are not intended to focus specifically on China, however, but instead encourage the Commerce Department to fulfill the legal requirements set out in these and other laws concerning the exports of US products to countries consistently carrying out gross human rights violations against their citizens.60

(c) Law enforcement catch-all for embargoed destinations.

We are aware that several of our proposed changes would place a significant extra burden of compliance on industry — in particular, the introduction of controls on night vision, smart cards, RFID chips, surveillance video technology, web filtering software/technology, and communications interception technology. On the other hand, we also believe strongly in the need for US export controls to restrict the export of such technologies where they are likely to be used in the commission of gross and persistent human rights violations. At a minimum, we believe the US Department of Commerce has a legal duty to prevent such exports to those countries with the records of the most persistent human rights violations.61

To balance these two imperatives, we propose a law enforcement catch-all, requiring licensing for all equipment listed on the CCL to law enforcement and security users in a limited set of destinations. Commerce should define a “CC Column 4,” specifying crime control licenses for export of items on the CCL at a minimum to destinations under general US arms embargoes (including Burma, China, Cuba, Iran, North Korea, Sudan, and Zimbabwe). We believe this should also be extended to other countries with the most

60 22 U.S.C. §2304(2)
61 22 U.S.C. §2304(2)
persistent human rights violation records, a list which could be drawn up in consultation with
the State Department’s human rights staff and based on State Department’s reporting.
Although such a list would not address all concerns about all end users with patterns of gross
human rights violations, it could prevent some acquisition of technologies and equipment that
could enable further human rights violations.