

RECORD OF COMMENTS: EFFECTS OF FOREIGN POLICY-BASED EXPORT CONTROLS

Published in the Federal Register: September 5, 2007 ([72 FR 50912](#))

Comments due October 5, 2007

COMMENT #	SOURCE	SIGNER(S) OF LETTER	DATE	NUMBER OF PAGES
1.	Cogent Systems, Inc.	James Jasinski and Lee Moser (Cogent); Tovah LaDier (Williams Mullen Strategies); James Cannon and Dean Barclay (Williams Mullen)	October 5, 2007	20
2.	Industry Coalition on Technology Transfer	Eric Hirshorn (Executive Secretary)	October 5, 2007	2
3.	FICCI USA	Rajana Khanna (Asst. Secretary General)	October 5, 2007	3

Proposed Rules

Federal Register

Vol. 72, No. 171

Wednesday, September 5, 2007

This section of the FEDERAL REGISTER contains notices to the public of the proposed issuance of rules and regulations. The purpose of these notices is to give interested persons an opportunity to participate in the rule making prior to the adoption of the final rules.

DEPARTMENT OF COMMERCE

Bureau of Industry and Security

15 CFR Chapter VII

[Docket No. 070827486-7487-01]

Effects of Foreign Policy-Based Export Controls

AGENCY: Bureau of Industry and Security, Commerce.

ACTION: Request for Comments on Foreign Policy-based Export Controls.

SUMMARY: The Bureau of Industry and Security (BIS) is reviewing the foreign policy-based export controls in the Export Administration Regulations to determine whether they should be modified, rescinded or extended. To help make these determinations, BIS is seeking comments on how existing foreign policy-based export controls have affected exporters and the general public.

DATES: Comments must be received by October 5, 2007.

ADDRESSES: Written comments may be sent by e-mail to publiccomments@bis.doc.gov. Include "FPBEC" in the subject line of the message. Written comments (three copies) may be submitted by mail or hand delivery to Jeffery Lynch, Regulatory Policy Division, Bureau of Industry and Security, Department of Commerce, 14th Street & Pennsylvania Avenue, NW., Room 2705, Washington, DC 20230.

FOR FURTHER INFORMATION CONTACT: Joan Roberts, Foreign Policy Division, Office of Nonproliferation and Treaty Compliance, Bureau of Industry and Security, Telephone: (202) 482-4252. Copies of the current Annual Foreign Policy Report to the Congress are available at <http://www.bis.doc.gov/PoliciesAndRegulations/07ForPolControls/index.htm> and copies may also be requested by calling the Office of Nonproliferation and Treaty Compliance at the number listed above.

SUPPLEMENTARY INFORMATION: Foreign policy-based controls in the Export Administration Regulations (EAR) are implemented pursuant to Section 6 of the Export Administration Act of 1979, as amended. The current foreign policy-based export controls maintained by the Bureau of Industry and Security (BIS) are set forth in the EAR, including in parts 742 (CCL Based Controls), 744 (End-User and End-Use Based Controls) and 746 (Embargoes and Special Country Controls). These controls apply to a range of countries, items, activities and persons, including: Certain general purpose microprocessors for 'military end-uses' and 'military end-users' (§ 744.17); significant items (SI): Hot section technology for the development, production, or overhaul of commercial aircraft engines, components, and systems (§ 742.14); encryption items (§§ 742.15 and 744.9); crime control and detection commodities (§ 742.7); specially designed implements of torture (§ 742.11); certain firearms included within the Inter-American Convention Against the Illicit Manufacturing of and Trafficking in Firearms, Ammunition, Explosives, and Other Related Materials (§ 742.17); regional stability items (§ 742.6); equipment and related technical data used in the design, development, production, or use of certain rocket systems and unmanned air vehicles (§§ 742.5 and 744.3); chemical precursors and biological agents, associated equipment, technical data, and software related to the production of chemical and biological agents (§§ 742.2 and 744.4) and various chemicals included in those controlled pursuant to the Chemical Weapons Convention (§ 742.18); nuclear propulsion (§ 744.5); aircraft and vessels (§ 744.7); communication intercepting devices (software and technology) (§ 742.13); embargoed countries (part 746); countries designated as supporters of acts of international terrorism (§§ 742.8, 742.9, 742.10, 742.19, 746.2, 746.4, 746.7, and 746.9); certain entities in Russia (§ 744.10); individual terrorists and terrorist organizations (§§ 744.12, 744.13 and 744.14); certain persons designated by Executive Order 13315 ("Blocking Property of the Former Iraqi Regime, Its Senior Officials and Their Family Members") (§ 744.18); and certain sanctioned entities (§ 744.20). Attention is also given in this

context to the controls on nuclear-related commodities and technology (§§ 742.3 and 744.2), which are, in part, implemented under section 309(c) of the Nuclear Non Proliferation Act.

Under the provisions of section 6 of the Export Administration Act of 1979, as amended (50 U.S.C. app. §§ 2401-2420 (2000)) (EAA), export controls maintained for foreign policy purposes require annual extension. Section 6 of the EAA requires a report to Congress when foreign policy-based export controls are extended. The EAA expired on August 20, 2001. Executive Order 13222 of August 17, 2001 (3 CFR, 2001 Comp., p. 783 (2002)), which has been extended by successive Presidential Notices, the most recent being that of August 15, 2007 (72 FR 46137, August 16, 2007), continues the EAR and, to the extent permitted by law, the provisions of the EAA, in effect under the International Emergency Economic Powers Act (50 U.S.C. 1701-1706 (2000)). The Department of Commerce, insofar as appropriate, is following the provisions of section 6 in reviewing foreign policy-based export controls, requesting public comments on such controls, and submitting a report to Congress.

In January 2007, the Secretary of Commerce, on the recommendation of the Secretary of State, extended for one year all foreign policy-based export controls then in effect.

To assure maximum public participation in the review process, comments are solicited on the extension or revision of the existing foreign policy-based export controls for another year. Among the criteria considered in determining whether to continue or revise U.S. foreign policy-based export controls are the following:

1. The likelihood that such controls will achieve the intended foreign policy purpose, in light of other factors, including the availability from other countries of the goods, software or technology proposed for such controls;

2. Whether the foreign policy purpose of such controls can be achieved through negotiations or other alternative means;

3. The compatibility of the controls with the foreign policy objectives of the United States and with overall United States policy toward the country subject to the controls;

4. Whether reaction of other countries to the extension of such controls by the

United States is not likely to render the controls ineffective in achieving the intended foreign policy purpose or be counterproductive to United States foreign policy interests;

5. The comparative benefits to U.S. foreign policy objectives versus the effect of the controls on the export performance of the United States, the competitive position of the United States in the international economy, the international reputation of the United States as a supplier of goods and technology; and

6. The ability of the United States to enforce the controls effectively.

BIS is particularly interested in receiving comments on the economic impact of proliferation controls. BIS is also interested in industry information relating to the following:

1. Information on the effect of foreign policy-based export controls on sales of U.S. products to third countries (i.e., those countries not targeted by sanctions), including the views of foreign purchasers or prospective customers regarding U.S. foreign policy-based export controls.

2. Information on controls maintained by U.S. trade partners. For example, to what extent do they have similar controls on goods and technology on a worldwide basis or to specific destinations?

3. Information on licensing policies or practices by our foreign trade partners which are similar to U.S. foreign policy-based export controls, including license review criteria, use of conditions, requirements for pre and post shipment verifications (preferably supported by examples of approvals, denials and foreign regulations).

4. Suggestions for revisions to foreign policy-based export controls that would bring them more into line with multilateral practice.

5. Comments or suggestions as to actions that would make multilateral controls more effective.

6. Information that illustrates the effect of foreign policy-based export controls on trade or acquisitions by intended targets of the controls.

7. Data or other information as to the effect of foreign policy-based export controls on overall trade at the level of individual industrial sectors.

8. Suggestions as to how to measure the effect of foreign policy-based export controls on trade.

9. Information on the use of foreign policy-based export controls on targeted countries, entities, or individuals.

BIS is also interested in comments relating generally to the extension or revision of existing foreign policy-based export controls.

Parties submitting comments are asked to be as specific as possible. All comments received before the close of the comment period will be considered by BIS in reviewing the controls and developing the report to Congress.

All information relating to the notice will be a matter of public record and will be available for public inspection and copying. In the interest of accuracy and completeness, BIS requires written comments. Oral comments must be followed by written memoranda, which will also be a matter of public record and will be available for public review and copying.

The Office of Administration, Bureau of Industry and Security, U.S. Department of Commerce, displays these public comments on BIS's Freedom of Information Act (FOIA) Web site at <http://www.bis.doc.gov/foia>. This office does not maintain a separate public inspection facility. If you have technical difficulties accessing this Web site, please call BIS's Office of Administration at (202) 482-0637 for assistance.

Dated: August 29, 2007.

Christopher A. Padilla,
Assistant Secretary for Export Administration.

[FR Doc. E7-17525 Filed 9-4-07; 8:45 am]

BILLING CODE 3510-33-P

ENVIRONMENTAL PROTECTION AGENCY

40 CFR Part 62

[EPA-R07-OAR-2007-0655; FRL-8462-8]

Approval and Promulgation of State Plans for Designated Facilities and Pollutants; Iowa; Clean Air Mercury Rule

AGENCY: Environmental Protection Agency (EPA).

ACTION: Proposed rule.

SUMMARY: EPA is proposing to approve the State Plan submitted by Iowa on August 15, 2006, and revisions submitted on April 26, 2007. The plan addresses the requirements of EPA's Clean Air Mercury Rule (CAMR), promulgated on May 18, 2005, and subsequently revised on June 9, 2006. EPA is proposing to determine that the submitted State Plan fully meets the CAMR requirements for Iowa.

CAMR requires States to regulate emissions of mercury (Hg) from large coal-fired electric generating units (EGUs). CAMR establishes State budgets for annual EGU Hg emissions and requires States to submit State Plans to

ensure that annual EGU Hg emissions will not exceed the applicable State budget. States have the flexibility to choose which control measures to adopt to achieve the budgets, including participating in the EPA-administered CAMR cap-and-trade program. In the State Plan that EPA is proposing to approve Iowa would meet CAMR requirements by participating in the EPA trading program.

DATES: Comments must be received on or before October 5, 2007.

ADDRESSES: Submit your comments, identified by Docket ID No. EPA-R07-OAR-2007-0655, by one of the following methods:

1. <http://www.regulations.gov>: Follow the on-line instructions for submitting comments.

2. *E-mail:* jay.michael@epa.gov.

3. *Mail:* Michael Jay, Environmental Protection Agency, Air Planning and Development Branch, 901 North 5th Street, Kansas City, Kansas 66101.

4. *Hand Delivery or Courier:* Deliver your comments to: Michael Jay, Environmental Protection Agency, 901 North 5th Street, Kansas City, Kansas 66101. Such deliveries are only accepted during the Regional Office's normal hours of operation. The Regional Office's official hours of business are Monday through Friday, 8 a.m. to 4:30 p.m., excluding Federal holidays.

Instructions: Direct your comments to Docket ID No. EPA-R07-OAR-2007-0655. EPA's policy is that all comments received will be included in the public docket without change and may be made available online at <http://www.regulations.gov>, including any personal information provided, unless the comment includes information claimed to be Confidential Business Information (CBI) or other information whose disclosure is restricted by statute. Do not submit through <http://www.regulations.gov> or e-mail, information that you consider to be CBI or otherwise protected. The <http://www.regulations.gov> Web site is an "anonymous access" system, which means EPA will not know your identity or contact information unless you provide it in the body of your comment. If you send an e-mail comment directly to EPA without going through <http://www.regulations.gov>, your e-mail address will be automatically captured and included as part of the comment that is placed in the public docket and made available on the Internet. If you submit an electronic comment, EPA recommends that you include your name and other contact information in the body of your comment and with any disk or CD-ROM you submit. If EPA

Before the
Bureau of Industry and Security
U.S. Department of Commerce

EFFECTS OF FOREIGN POLICY-BASED EXPORT CONTROLS:

***The Adverse Impact of Current Policy Regarding Exports of
Automated Fingerprint Identification Systems (“AFIS”)
to the People’s Republic of China***

Cogent Systems, Inc.

October 5, 2007

James J. Jasinski
Lee Moser
Cogent Systems, Inc.
11480 Commerce Park Drive, Suite 150
Reston, VA 20191

Tovah LaDier
WILLIAMS MULLEN STRATEGIES
James R. Cannon, Jr.
Dean A. Barclay
WILLIAMS MULLEN
1666 K Street, N.W., Suite 1200
Washington, DC 20006

Contents

I. Executive Summary	1
II. Application of Six Factors for Consideration by the Bureau of Industry and Security Supports Removal of Fingerprint Retrieval Systems from the Crime Control Provision.	4
A. Controls will not likely “achieve the intended foreign policy purpose, in light of other factors, including the availability from other countries of the goods, software or technology proposed for such controls.”	4
1. A lack of complementary controls prevents the current control from achieving its foreign policy purpose.	4
2. In addition, China has local suppliers that are rapidly advancing	6
3. The nature of fingerprint retrieval systems makes these controls ineffective in preventing human rights violations.	6
B. The “foreign policy purpose of such controls can be achieved through negotiations or other alternative means.”	8
C. Controls are incompatible “with the foreign policy objectives of the United States and with overall United States policy toward the country subject to the controls.”	9
1. Controls are incompatible with maintenance of U.S. leadership with respect to standards for interoperability	9
2. Controls are incompatible with deployment of fingerprint identification systems for international border security	11
3. Controls are incompatible with identification of terrorists entering China’s Western border	11
4. Controls are incompatible with the 2007 National Export Strategy	12
D. The “reaction of other countries” to removal of AFIS systems from the scope of U.S. controls is not “likely to render the controls ineffective in achieving the intended foreign policy purpose” and will not “be counterproductive to United States foreign policy interests.”	13
E. In light of the negative “effect of the controls on the export performance of the United States, the competitive position of the United States in the international economy, {and} the international reputation of the United States as a supplier of goods and technology,” licensing exports of one-to-many fingerprint retrieval systems would provide greater “benefits to U.S. foreign policy” than would the continued suspension of licenses.	13
F. The United States can “enforce the {Crime Prevention} controls effectively” without suspending licenses for one-to-many fingerprint retrieval systems.	15

III. The “National Interest” Favors Elimination of the Restriction on Exports
of AFIS to China..... 16

Before the
Bureau of Industry and Security
U.S. Department of Commerce

EFFECTS OF FOREIGN POLICY-BASED EXPORT CONTROLS:

***the Adverse Impact of Current Policy Regarding Exports of
Automated Fingerprint Identification Systems (“AFIS”)
to the People’s Republic of China***

Cogent Systems, Inc.

I. EXECUTIVE SUMMARY

Cogent Systems, Inc., a leading U.S. producer of Automated Fingerprint Identification Systems (“AFIS”), on November 22, 2006, formally requested that the Bureau of Industry and Security (“BIS”) and the President exclude such fingerprint systems from the Crime Control classification under the Export Administration Regulations (§ 7742.7).¹ To date, BIS has not acted on that request. Yet, in this case inaction amounts to a denial. So long as export licenses are suspended with respect to fingerprint retrieval systems, U.S.-made systems cannot participate in procurement opportunities in China. At stake is U.S. leadership in this technology and in establishing international standards for interoperability. Indeed, at stake is the U.S. industry’s economic viability. Delay in removing fingerprint systems from the sanctions list operates inexorably to the advantage of our Chinese and international competitors. As explained below, prohibiting the export of fingerprint retrieval systems is not in the national interest of the United States, nor does it help the United States achieve the objectives of the Tiananmen Square Sanctions.

The statute calls for a determination by the President whether maintaining the current suspension on export licenses is in the “national interest.”² This standard recognizes inherently that the President may have to balance competing

¹ The request was filed pursuant to Section 902(b) of the Tiananmen Square Sanctions (22 U.S.C. § 2151 note) and the Request for Comments published on October 23, 2006. *Effects of Foreign Policy-Based Export Controls*, 71 Fed. Reg. 62,065 (October 23, 2006) (Request for Comments).

² Section 902(b)(2) of the Tiananmen Square Sanctions (22 U.S.C. § 2151 note).

U.S. POLICY AND AFIS EXPORTS TO CHINA

objectives. Here, as shown below, there is little to gain by maintaining the sanctions with respect to AFIS—and much to lose.

Against the theoretical possibility that AFIS might indirectly assist Chinese authorities to track dissidents, the President should weigh the very tangible losses to the United States of not lifting the sanctions:

(1) As applied to AFIS, the sanctions jeopardize U.S. national security interests. The identification of individuals for preventing or permitting entry into the United States is critical to our national security. Foreign countries, including China, supply fingerprint (and other biometric) data with respect to suspected terrorists, international criminals and individuals identified on the Watch List. These data are incorporated into the U.S. biometric system currently deployed to identify terrorists, criminals or persons of special interest. Continued access to these data in a usable format depends upon the use of inter-operable systems. However, by preventing exports of U.S.-made systems to China, the sanctions undermine interoperability.

(2) Long-term the sanctions jeopardize U.S. technology leadership as well as U.S. leadership in setting international standards. Continued U.S. leadership in establishing the standards for the exchange of critical data concerning identification depends on technological leadership. Current U.S. AFIS technology enables users efficiently and accurately to identify an individual from a pool of candidates (one-to-many searching). However, innovation continues around the world, and AFIS systems steadily become faster and more accurate. The restriction prohibiting exportation of AFIS to China jeopardizes the continued leadership of the United States in shaping international standards and diminishes the economic viability and health of a U.S. industry.

(3) The sanctions will result in the movement of technology investment to China, with negative repercussions for national security and the U.S. economy. Already China has a growing industry producing fingerprint retrieval systems. Chinese companies and individuals have been award-winners in past international competitions. U.S. producers that do not want to lose their competitive edge will seek the best return on investment and will therefore invest where they can sell to the fastest-growing and largest market. Ultimately, if the U.S. sanctions prevent U.S. companies from maintaining technological leadership, imports from China will dominate the U.S. market, and there will be no local sources for this critical technology.³

³ See, e.g., Keith Bradsher, “An Opportunity for Wall St. in China’s Surveillance Boom,” The New York Times (Sept. 11, 2007) (“Over the last year, American hedge funds have put more than \$150 million into Chinese surveillance {sic} companies.”).

U.S. POLICY AND AFIS EXPORTS TO CHINA

(4) The sanctions do not help to achieve U.S. human rights objectives. Fingerprint retrieval systems are primarily and fundamentally used for identification. Such systems cannot be used for surveillance of individuals. Moreover, fingerprint retrieval technology is readily available in China from local sources and also from world-class producers in Japan and France. Japanese and French AFIS, as well as Chinese-made systems, are already in place in China. The United States gains no leverage by denying U.S. producers the ability to ship AFIS to China.

A compelling summary of the case was presented in an August 10, 2007 letter from the Chief of Staff for U.S. Representative Adam B. Schiff (CA-29), to Jonathan D. Farrar, Principal Deputy Assistant Secretary, in the U.S. State Department's Bureau of Democracy, Human Rights, and Labor:

As you may know, Mr. Schiff has been forceful in his criticism of China's human rights practices and believes that we should make human rights a core element of our policy towards Beijing. He favors export prohibitions on material that could be used by the Chinese to repress their own citizens.

Having said that, he is also mindful of the distinction between equipment that can be reasonably expected to be used for repression and equipment which is a standard tool for law enforcement and domestic security. Our understanding is that the AFIS technology (at least as Cogent describes it) falls into the latter category.

Mr. Schiff is concerned about ceding American leadership in a growing (albeit discrete) economic and technological sector to Europe, Japan or even China itself. Cogent argues that the US is in a position to set the global standards for fingerprint identification, but that leadership could be undermined if we are not allowed to enter the largest single market for such technology. Currently, the Watch List includes individuals whose biometrics have been obtained from both domestic and international sources. The exportability of this data is based upon interoperable biometric security systems around the world, many of which rely on U.S. technology. I

think that it is legitimate to be concerned about the impact of closing us out of the Chinese market.

As articulated above, “the balance of equities” favors a waiver allowing Cogent to export its Automated Fingerprint Identification Systems (“AFIS”) technology to China. Balanced on a scale of national interest, a merely theoretical threat to the human rights of dissidents weighs less than do very tangible losses to U.S. national security and economic vitality. For the reasons elaborated below in terms of six factors for consideration by BIS, Cogent respectfully requests removal of controls on fingerprint retrieval systems from the Crime Control provision.

II. APPLICATION OF SIX FACTORS FOR CONSIDERATION BY THE BUREAU OF INDUSTRY AND SECURITY SUPPORTS REMOVAL OF FINGERPRINT RETRIEVAL SYSTEMS FROM THE CRIME CONTROL PROVISION.

The September 5, 2007 invitation to comment identifies six specific issues.⁴ As shown above and summarized below, each factor in this case supports removal of fingerprint retrieval systems from the Crime Control provision.

A. *Controls will not likely “achieve the intended foreign policy purpose, in light of other factors, including the availability from other countries of the goods, software or technology proposed for such controls.”*

1. A lack of complementary controls prevents the current control from achieving its foreign policy purpose.

Because no other countries deny export licenses to exports of one-to-many fingerprint retrieval systems, and because U.S. technology is equaled by European and Japanese systems, it is unlikely that continued suspension of export licenses on U.S.-made systems will induce China to improve its record of human rights violations. Section 742.7(d) of the EAR acknowledges that the United States has not obtained commitments from other countries that suspend exports of one-to-many fingerprint retrieval systems:

Although the United States seeks cooperation from like-minded countries in maintaining controls on

⁴ 72 Fed. Reg. at 50,912-13.

U.S. POLICY AND AFIS EXPORTS TO CHINA

crime control and detection items, at this time these controls are maintained only by the United States.⁵

In its 2007 Foreign Policy Report, BIS concedes that “[t]he lack of complementary controls by other producer nations limits the effectiveness of these controls in preventing human rights violations.”⁶ Instead, BIS points to the fact that “stringent licensing requirement for crime control items enables the U.S. Government to monitor closely items that could be used in human rights violations.”⁷ In the case of China, however, no licenses are issued to allow exports of fingerprint retrieval systems. Hence, even monitoring does not take place.

As outlined in Cogent’s 2006 comments, both NEC Corporation (Japan) and SAGEM (France) have supplied AFIS to China. A 2004 NIST evaluation of AFIS produced by eighteen companies established that systems from NEC, SAGEM and Cogent Systems were the leading AFIS in terms of accuracy and speed in one-to-many fingerprint matching.⁸

Thus, two of the top-three AFIS providers have already installed systems in China. NEC has at least five installations in China.⁹ SAGEM has an installation in Tianjin and has been bidding in competition with other producers to supply regional AFIS in China. In fact, the SAFRAN Group, SAGEM’s parent company, has four industrial sites and headquarters in China and three joint ventures with Chinese companies.¹⁰

⁵ 15 C.F.R. § 742.7(d) (2006) (emphasis added).

⁶ U.S. Bureau of Industry and Security, 2007 Foreign Policy Report, Chapter 2, <http://www.bis.doc.gov/News/2007/foreignpolicyreport/fprchap02_CrimeControl.html> (last visited Oct. 5, 2007) (emphasis added).

⁷ Id.

⁸ Wilson, et al, “Fingerprint Vendor Technology Evaluation 2003: Analysis Report,” Abstract at 2 (June 2004) (hereinafter “FpVTE”), available online at <<http://fpvte.nist.gov/index.html>> (last visited November 20, 2006).

⁹ NEC Corp. of America website, <<http://www.necam.com/IDS/AFIS/Worldwide-Deployment.cfm>> (last visited November 17, 2006), included in Exhibit 5.

¹⁰ “SAFRAN Worldwide, About SAFRAN,” available online at <http://www.safran-group.com/recherchelocalisation.php?id_pays=522&lang=en> (last visited Oct. 5, 2007).

2. In addition, China has local suppliers that are rapidly advancing

In addition to the top-performing fingerprint retrieval technology available from Japan and France, China has a national industry that is rapidly advancing in AFIS technology. In the 2004 international competition, “FVC2004,” China’s Academy of Sciences was awarded third place in the “open” category for fingerprint matching algorithms.¹¹ Separately, Shanghai Jiao Tong University, China Daheng Group, Inc., and Suranaree University of Technology are developing a new methodology for one-to-many fingerprint matching, “suitable for large-scale identification systems.”¹²

In the 2006 competition, The Chinese Academy of Sciences improved to one gold, one silver and one bronze metal in the open category. In addition, Ji Hui (an independent Chinese developer) won three gold metals, Maxis Biometrics Co., Ltd. won two gold metals, Xu Zengbo won two silver metals, and Unicomp Technology Co., Ltd. won silver and bronze metals.¹³ Another Chinese supplier, Golden Finger, was ranked in the NIST study.¹⁴

As shown by the performance of the Chinese industry and developers in international competitions, AFIS technology is both readily available in China and steadily improving in speed and accuracy.

3. The nature of fingerprint retrieval systems makes these controls ineffective in preventing human rights violations.

To understand a further reason why the current controls do not effectively prevent human rights violations, one must first understand the primary uses of AFIS systems.

¹¹ “FVC2004: Third Fingerprint Verification Competition,” available online at <http://bias.csr.unibo.it/fvc2004/results/Open_resultsAvg.asp> (last visited Oct. 5, 2007).

¹² “ANFIS-based fingerprint-matching algorithm,” *Optical Engineering*, August 2004, pp. 1814-19, available online <<http://adsabs.harvard.edu/abs/2004OptEn.43.1814H>> (last visited Oct. 5, 2007).

¹³ “FVC2006: Fourth Fingerprint Verification Competition,” available online at <http://bias.csr.unibo.it/fvc2006/results/Open_resultsMT.asp> (last visited October 4, 2007).

¹⁴ FpVTE Summary of Results at 9-15.

U.S. POLICY AND AFIS EXPORTS TO CHINA

Fingerprints enable both: (1) the identification of an individual from a pool of candidates (one-to-many searching); and (2) authentication of an individual (one-to-one searching). AFIS systems manage electronically stored data that fingerprints supply. While historically AFIS systems were primarily deployed by serviced law enforcement, their application has extended to both the civil and commercial sectors such as in border control and physical access devices.

Fingerprint retrieval systems are very effective in identification procedures—for example, validating or identifying an individual who is in custody or is confirming his identity for a visa. This process is quick, simple and automated. While fingerprint retrieval technology is also used for latent prints (partial prints captured incidental to an arrest),¹⁵ it is slow, complex and burdensome, requiring significant human intervention in both marking the latent and then reviewing the candidates. As such, the utility for the technology is in identification, not surveillance. Widely available non-AFIS technologies, by contrast, are expressly designed to serve surveillance purposes.

As described, AFIS systems are the key biometric system for border protection against terrorists and criminal elements because they can accurately and swiftly search large volumes of fingerprint records. Cogent Systems provides AFIS and biometric access control solutions to governments, law enforcement agencies and commercial customers worldwide. Cogent has established a reputation for successful deployment of identification system solutions that allow for real time identification of individuals in a wide variety of applications,

¹⁵ There are two basic types of searches, “known” and “latent.” Known searches use a complete fingerprint that is captured specifically for either storing or searching. The subject is in custody and fully aware of the search. This process is controlled and fully automated. Accuracy for this process is typically in the 99+ percentile. Searches are done in seconds and require limited computer resources per search. In relative terms, searches are low cost and quick. Searches can be either one-to-many (identification of an individual from a pool of candidates) or one-to-one (confirmation of an individual). These searches generate a single candidate and therefore involve a quick process. Latent searches generally are of only a partial fingerprint that is captured incidental to an event. The subject is generally not aware of the search. This process is done manually and requires special skills in locating, lifting, encoding and searching. Accuracy for this process is typically in the 50+ percentile for an average quality latent print. For a poor quality latent, accuracy is typically 10%. Searches are done over many minutes or hours and require significantly greater computer resources per search. These searches generate multiple candidates that then must be compared by an expert, a time and resource consuming process.

U.S. POLICY AND AFIS EXPORTS TO CHINA

including: border security, event security, immigration, voting, asylum, citizen identification, driver's licenses, criminal investigations and others.

Cogent's technology was accordingly selected to support a top priority program of the U.S. Department of Homeland Security, the US-VISIT. Using biometric technology as the key identifier, this automated system expedites the entry/exit process for those legitimate travelers to the United States. Cogent has also provided the core matching platform for EURODAC. EURODAC is a multinational system in the European Union used by 26 nations to verify political asylum applications. As a team member to Pacific Century Cyber Works (PCCW), Cogent technology is embedded in the largest biometric and smartcard program, Hong Kong's National Smart Identity Card System (SMARTICS). The technology at issue has thus supported the US-VISIT program, the FBI, Secret Service, and a myriad of state and local law enforcement organizations throughout the United States and abroad.

The above applications reveal a major misconception about AFIS systems. AFIS technology is primarily a law enforcement and border security tool that enables matching of a fingerprint against a criminal/watch list fingerprint database. It is an effective tool in identification procedures. Its use is limited to when the subject is already known and identified in a database.

AFIS technology is not surveillance or data mining technology. Because it cannot be used for physical or internet surveillance, it is not readily usable for the violation of a citizen's human rights. Indeed, identification, unlike surveillance, inherently protects human rights.

In these circumstances, the suspension of U.S. export licenses is insufficient to achieve any foreign policy of the United States. In particular, suspension of licensing does not achieve human rights objectives.

B. The "foreign policy purpose of such controls can be achieved through negotiations or other alternative means."

As outlined in section C, following, negotiations with China are achieving demonstrable progress, at least in enlisting China to assist in war on terrorism. It follows that negotiations should also be useful in reducing human rights violations in China and reducing the likelihood of another Tiananmen Square.

Moreover, this request applies only to one-to-many fingerprint retrieval systems, *i.e.*, AFIS. Other software, technology and equipment covered by Part 742.7 of the EAR would not be affected by lifting the suspension on fingerprint retrieval systems. Thus, the United States would not lose any negotiating

leverage obtained with respect to polygraphs and various other monitoring devices covered by the Crime Control provision. Indeed, the global condemnation of the events in Tiananmen Square, as well as the ongoing damage to China's reputation, are themselves more effective in preventing or discouraging human rights violations than are the sanctions on fingerprint retrieval systems.

C. Controls are incompatible “with the foreign policy objectives of the United States and with overall United States policy toward the country subject to the controls.”

The controls at issue are incompatible with strong demonstrated U.S. foreign policy objectives generally to engage with China and specifically to enlist China's continuing cooperation in the global war against terror. According to a Country Report on Terrorism from the U.S. Department of State, China's ongoing anti-terrorist initiatives have supported U.S. efforts both to prevent nuclear weapons and materials from entering U.S. borders and to prevent the spread of terrorist instruments throughout Asia.¹⁶ Cogent's 2006 comments outlined several U.S. programs that are supported by China: the Megaports Initiative, the Container Security Initiative, regional cooperation in the war against terror, anti-money laundering programs and anti-terrorist investigations, and security preparations for the Beijing Olympics.

In addition, allowing exports of AFIS to China will advance U.S. foreign policy objectives in several respects:

1. Controls are incompatible with maintenance of U.S. leadership with respect to standards for interoperability

International standards for the exchange of fingerprint identification information have long been based on U.S. AFIS technology. Beginning in the 1990s, established standards enabled interoperability among different proprietary systems. U.S. companies were the early developers of AFIS technology and propagated national standards that evolved into international interoperable

¹⁶ *E.g.*, “China supported several operational and logistical aspects of the global war on terror, including signing a memorandum of understanding on the Department of Energy's Megaports initiative to detect radiological materials and continuing its support for the Container Security Initiative. Beijing also played an instrumental role in getting the Shanghai Cooperation Organization to issue a joint statement in 2005 on increasing regional cooperation to fight terrorism.” U.S. Department of State, “Country Reports on Terrorism: East Asia and Pacific Overview” at 60 (2005), <<http://www.state.gov/documents/organization/65470.pdf>> (last visited Nov. 20, 2006) (hereinafter “Country Reports”).

U.S. POLICY AND AFIS EXPORTS TO CHINA

standards used by Interpol and other law enforcement organizations. Through these standards, systems deployed around the world can exchange fingerprint data for both storing and searching purposes.

During this process, the United States has been the world leader. As a direct benefit, the United States has been able to exchange fingerprint data at the local, state, national, and international level. This has enormously enhanced U.S. security. For example, through those standards the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program has prevented over 34,000 undesirable individuals from gaining entry into the United States. These standards permit foreign data to be incorporated into U.S. VISIT or the Integrated AFIS system (IAFIS) operated by the Federal Bureau of Investigation.

The ability of U.S. government and industry to continue to set standards is threatened by the loss of U.S. leadership in the AFIS technology. If the United States cedes its technological advantage (or, at least, parity) to European and Asian producers of AFIS technology, it will lose the ability to set international standards for sharing critical data. This trend is a serious threat to U.S. national interests.

Stated differently, the U.S. has a vital national security interest in both (1) continued improvement of U.S. technology and (2) wider access to international data identifying terrorists, illegal entrants, criminals and the like. According to the FBI:

“Dealing with other repositories has emerged as a major problem,” said James A. “Jim” Loudermilk II, deputy assistant director at the bureau’s Information Technology Operations Division, during the briefing.

* * * the bureau’s Integrated Automated Fingerprint Identification System already exchanges specified groups of fingerprints gathered from individuals who qualify as “the worst of the worst” among immigration law violators, known or suspected terrorists (KST) and similar wrongdoers.

* * *

The bureau’s biometric technologists have consulted with their counterparts abroad to help develop regional biometric information repositories, Loudermilk said. For example, some Middle Eastern countries seek to build a regional biometric

database of criminals and other social enemies, and the bureau has advised them, he said.¹⁷

2. Controls are incompatible with deployment of fingerprint identification systems for international border security

Increasingly, fingerprint systems are being deployed on an international basis to assist in the identification of suspected terrorists, illegal immigrants or other persons crossing national borders. The United States is not alone in utilizing fingerprint retrieval systems as a tool for automation of border control. Such systems are in place around the world, including in China, which uses a system developed by China Public Security Technology, Inc. for port security.¹⁸

Japan has amended its immigration law and will, on November 20, 2007, require fingerprinting and photographing of all foreigners age 16 or older upon entry into the country.¹⁹ Since 2003, the European Union has maintained a database called “EURODAC” that includes the fingerprints of any person over the age of 14 who applies for asylum upon entering the EU, Norway or Iceland. EURODAC is shared among all of the EU countries from a central database. Other countries currently using biometric data in order to identify persons crossing international borders include Bulgaria, Slovakia, Romania, Australia, Canada, Hong Kong, Macedonia, Malaysia, New Zealand, Pakistan, Singapore, Switzerland, Thailand, Ukraine and Venezuela.

As the world’s databases of fingerprints grow, the United States has a national security interest in maintaining its access to those data and in maintaining adequate technology to search the data.

3. Controls are incompatible with identification of terrorists entering China’s Western border

Currently, China collects data on *al Qaeda* and drug gangs on its western border. This includes data on people entering China as well as people in China working with terrorists and drug lords that are acquired through travel, arrests,

¹⁷ “Bureau to Seek Proposals for NGI Improvements,” Washington Technology (May 22, 2007).

¹⁸ China Public Security Technology, Inc. has received a great deal of attention as the first Chinese security company to be listed on the U.S. stock exchange.

¹⁹ “Japan to Begin Fingerprinting, Photographing Foreigners 20 November,” BBC & Kyodo (Oct. 4, 2007).

and information from other law enforcement agencies in neighboring countries. In many cases, the United States does not have access to this information.

Given the potential movement of terrorists across China's Western borders, the United States has an interest in ensuring that fingerprint data collected by China are available to U.S. authorities and will be compatible with U.S. AFIS systems. Homeland Security Secretary Chertoff was quoted in April 2006 as supporting U.S.-China cooperation in identification systems: "According to reports, China and the US, despite some differences on questions of repatriation, can develop cooperation in identification systems and identity documents, such as by China using biometric systems that are compatible with the US and assisting US Customs in identifying the status of people entering borders."²⁰

4. Controls are incompatible with the 2007 National Export Strategy

The Administration's 2007 National Export Strategy outlines the many actions that have been initiated in order to engage China to address trade generally, IPR strategy, law enforcement, and the importance of free enterprise and fair competition.²¹ Among other steps, the National Export Strategy singles out the "safety and security" sector for commercial development.²² AFIS systems are precisely the type of technology that China's security sector is seeking. And, so long as U.S. firms, such as Cogent, continue to be market leaders, their products are attractive candidates. At the same time, as explained above, AFIS hardware cannot be reverse-engineered. The systems therefore cannot be copied or misappropriated. Allowing exports, under appropriate licenses, is entirely consistent with the National Export Strategy.

²⁰ April 5, 2006 from www.sina.com.cn (unofficial translation).

²¹ Trade Promotion Coordinating Committee, "The 2007 National Export Strategy," at 106-112 (June 2007).

²² *Id.* at 112.

- D. The “reaction of other countries” to removal of AFIS systems from the scope of U.S. controls is not “likely to render the controls ineffective in achieving the intended foreign policy purposed” and will not “be counterproductive to United States foreign policy interests.”*

Given that no other countries ban exports of one-to-many fingerprint systems to China, the current controls are ineffective. If the current controls are modified to permit the exportation of one-to-many fingerprint retrieval systems, there is not likely to be any reaction by other countries, because they do not maintain similar controls.

- E. In light of the negative “effect of the controls on the export performance of the United States, the competitive position of the United States in the international economy, {and} the international reputation of the United States as a supplier of goods and technology,” licensing exports of one-to-many fingerprint retrieval systems would provide greater “benefits to U.S. foreign policy” than would the continued suspension of licenses.*

Maintaining the suspension on export licenses for one-to-many fingerprint retrieval systems will have little or no positive impact on U.S. foreign policy objectives. China has access to the leading algorithms and software from Europe and Japan. China has ongoing, government-sponsored research, which has recently been awarded third place in an international competition. China’s domestic industry includes at least one producer that was favorably evaluated by NIST. As such, denying U.S. producers the ability to export to China does not provide any leverage with respect to U.S. foreign policy objectives.

On the other hand, continued suspension of the ability of U.S. exporters to obtain export licenses with respect to fingerprint retrieval software and devices will have a severe impact on the long-term competitiveness of the U.S. industry.²³ Among others, the following negative consequences are likely to continue:

- U.S. producers lack access to customer feedback and research and development from a large and growing population;

²³ Four companies are recognized to be the market leaders for one-to-many searching systems. The systems offered by these four companies are in over 90 percent of the world deployments requiring one-to-many searching.

U.S. POLICY AND AFIS EXPORTS TO CHINA

- U.S. producers are unable to include Chinese law enforcement AFIS systems within their relevant experience lists for purposes of bidding new work;
- U.S. producers are denied access to potentially the largest population database;
- U.S. producers are unable to gain experience matching a large and diverse database of ethnic fingerprints; and
- U.S. producers seeking the best return and competitive edge invest not in the United States but in foreign locations from which they can sell to the fastest-growing and largest market.

Taken together, these disadvantages will over time impair the continuing research and development efforts of the U.S. industry. Consequently, the international reputation of the U.S. industry as technology leaders in this field will suffer and decline.

Suspension thus jeopardizes both U.S. technological leadership and U.S. leadership in setting international standards.

With regard to technological leadership, EU and Asian country consortiums are challenging U.S. leadership. Recent NIST studies rate AFIS systems produced by Sagem (France) and NEC (Japan) equal to or exceeding the capabilities of systems produced by U.S. companies. These international suppliers, and newly-emerging Chinese companies, are deployed and operating in China, the United States and around the world. Exclusion from the Chinese market, the largest in the world, will severely limit the competitive advantage of the U.S. industry by limiting advanced R&D. Advances in technology depend on empirical research and require access to fingerprint data from different demographic groups and ethnicities. Thus, the effectiveness of matching algorithms is directly dependent upon the availability of fingerprint data from all sources.

With regard to U.S. leadership in setting international standards,²⁴ the United States has led in the establishment of international AFIS standards. U.S. companies were the early developers of the technology and propagated national standards that evolved into international interoperable standards used by Interpol and other law enforcement organizations. These permit foreign data to be incorporated into US-VISIT or the FBI's IAFIS system. The ability of U.S. government and industry to continue to set standards is threatened by the loss of U.S. leadership in the AFIS technology. At the same time, theft of U.S. technology is not an issue because the AFIS system is technically impenetrable.

F. The United States can “enforce the {Crime Prevention} controls effectively” without suspending licenses for one-to-many fingerprint retrieval systems.

As noted above, lifting the suspension of export licenses with respect to one-to-many fingerprint retrieval systems will not exempt such exports from the EAR or the need for a license. If past history is a guide, nor will lifting the suspension reduce the ability of the United States to enforce controls effectively. Indeed, according to the BIS 2006 Foreign Policy Report, 319 applications for licenses for “polygraphs, fingerprint analyzers, cameras and equipment,” have been approved under ECCN 3A981 in FY2005.²⁵ These approvals amounted to \$17 million in value.

The BIS 2006 Report concluded that the United States is able to enforce the Crime Control provisions effectively, although “enforcement cooperation with other countries generally is difficult” in cases involving unilaterally controlled

²⁴ Standards for interoperability are based upon either the fingerprint image or the features from that image. For one-to-many searching, interoperability standards are based upon the fingerprint image. For one-to-one searching, standards are based upon features from that image. Testing to date has shown a significant drop-off in matching accuracy for one-to-many searching when using the interoperability standards based upon the features from the fingerprint image, compared to using the fingerprint images themselves. The standards field is a dynamic area with multiple regions (e.g., European, Asian blocks) attempting to assume a leadership role. Controlling the standard, as the United States now does, helps to maintain our technological leadership and enhances our ability to share data and maintain border security.

²⁵ U.S. Bureau of Industry and Security, 2006 Foreign Policy Report, Chapter 2, Table 1, available online at <http://www.bis.gov/News/2006/foreignPolicyReport/fprchap02_CrimeControl.html> (last visited November 20, 2006).

items such as these....”²⁶ Given that China already has access to comparable technology, any damage to enforcement cooperation is not justified. In the context of growing U.S.-China cooperation to combat terrorism, removal of the suspension regarding one-to-many fingerprint retrieval systems could be very effective.

III. THE “NATIONAL INTEREST” FAVORS ELIMINATION OF THE RESTRICTION ON EXPORTS OF AFIS TO CHINA

The foregoing factors should be analyzed in the context of the “national interest” test established by law. In 1990, the Tiananmen Square Sanctions (22 U.S.C. § 2151 note, hereinafter “the Sanctions”) suspended all export control licenses covering crime control equipment exported to China. The President, however, may terminate the license suspension on the basis of finding²⁷ that “it is in the national interest of the United States to terminate a suspension.”²⁸

The “national interest” is regarded as the lowest standard applied in the case of sanctions. As explained by the Congressional Research Service,

It should be noted that “national interest” is considered the easiest standard to meet in legislation that requires or authorizes the imposition of sanctions (by comparison to what many consider the most rigorous standard, that a sanction not be waived unless it is “essential to national security interests”). President Bush and his successors have exercised the waiver on a case-by-case basis, in instances of satellite exports and items related to counter-terrorism, or wholesale, in the case of restoring USTDA funding, nuclear cooperation, and liberalization of export controls.²⁹

²⁶ 2006 Foreign Policy Report, Chapter 2 at 8 (emphasis added).

²⁷ The President, through BIS, submits a report each year concerning “Foreign Policy” export controls to the House Foreign Affairs Committee and the Senate Committee on Banking, Housing, and Urban Affairs and to other committees as requested. 50 U.S.C. App. §§ 2405(f)(1). No Congressional action is required.

²⁸ See *id.*, Section 902(b)(2) of the Sanctions.

²⁹ Dianne E. Rennack, CRS Report No. RL31910, “China: Economic Sanctions” at CRS-2 (May 18, 2005).

U.S. POLICY AND AFIS EXPORTS TO CHINA

In the Conference Report accompanying passage of the Sanctions, Congress expressly recognized “that the United States and the PRC government share geopolitical interests” and acknowledged “the need for the President to retain flexibility in the conduct of foreign policy.”³⁰ Accordingly, the statute provided conditions under which the President could waive a suspension. Of the President’s authority to grant a waiver based on “national interest” under Sec. 902(b)(2), the Conference Report recognized “that the President must weigh several elements in determining what is in the U.S. national interest, especially human rights and national security considerations.”³¹

As outlined above, the U.S. national security interest is served by maintaining U.S. leadership in a critical technology and U.S. leadership in the establishment of international standards for inter-operability. Moreover, although the Conference Report stated that “the economic interests of the U.S. and of individual American companies” should not be “the sole factor,” the Report nevertheless acknowledged: “U.S. economic interests are part of the national interest.”³² The fact that the suspension hurts the U.S. economically therefore should also weigh into the balance.

In light of concrete negative impacts on the national security and economic interests of the United States, and in the context of current technological and economic realities, prohibiting exports of AFIS to China does not in any meaningful way contribute to the prevention of human rights violations. In short, the balance should be struck in favor of removing the suspension with respect to export licenses.

1510436v5

³⁰ H.R. Conf. Rep. 101-343, 1990 U.S.C.C.A.N. 43 at 80 (1989).

³¹ H.R. Conf. Rep. 101-343 at 81. Notably, the Report’s sentence structure does not give human rights greater weight than national security. Because “national interest” includes “national security,” and “national security” includes anti-terrorism, an anti-terrorism technology merits a “national interest” waiver.

³² Id. (emphasis added).

ICOTT INDUSTRY COALITION ON TECHNOLOGY TRANSFER

1700 K Street, N.W., Washington, D.C. 20006 (202) 282-5994

October 5, 2007

Via E-Mail and First Class Mail

Mr. Jeffrey Lynch
Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
14th and Pennsylvania Avenue, NW, Room 2705
Washington DC 20230

Re: Effects of Foreign Policy-Based Export Controls, Fed. Reg./Vol. 72, No. 171 (Wednesday, September 5, 2007) Docket No. 070827486-7487-01

Dear Mr. Lynch:

The Industry Coalition on Technology Transfer (ICOTT) is pleased to respond to the Department's request for comments on the renewal of foreign policy-based export controls.

In large measure these controls are unilateral in character. Therein lies their ineffectiveness. While there can be instances where unilateral controls are justified, they are rarer than the broad array of such United States controls would indicate. From the standpoint of effectiveness, unilateral controls are like damming half a river. The builder may take pride in the majesty of the dam but there is every bit as much water downstream as before the first shovelful of earth was turned. For this reason, unilateral controls should be invoked—or continued—only where the resulting injury to American workers and businesses can be justified when balanced against the symbolic character of the restrictions. “National security” includes economic as well as military security, and both of these elements must be taken into account in the administration of our export control system.

Another argument frequently advanced in support of unilateral controls is that their imposition is necessary while the United States seeks multilateral support. The historical record of this tactic has been mixed at best. At a minimum, controls imposed unilaterally under this rationale should be of limited duration unless sufficient multilateral control is achieved.

We urge that any controls that do not meet the foregoing criteria be removed.

In addition to noting the general ineffectiveness of unilateral controls, we recommend that where such controls are imposed for anti-terrorism reasons, License Exception RPL be available for emergency services, including one-for-one replacement of parts, rendered to commercial aircraft that are located in, owned by, or registered in sanctioned countries. Were

INDUSTRY COALITION ON TECHNOLOGY TRANSFER

Mr. Jeffrey Lynch

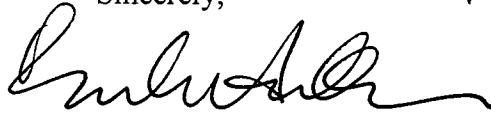
October 5, 2007

Page 2

an aircraft to crash because maintenance was unavailable due to United States export controls, the adverse publicity for our country would far outweigh any benefit derived from the controls themselves. Moreover, even absent a safety problem, the unavailability of scheduled aircraft could inconvenience nationals of many countries that are not sanctioned by the United States and be costly to affected airports and other international airlines (i.e., not of sanctioned countries) providing connecting flights.

Founded in 1983, ICOTT is a group of major trade associations (names listed below) whose thousands of individual member firms export controlled goods and technology from the United States. ICOTT's principal purposes are to advise U.S. Government officials of industry concerns about export controls, and to inform ICOTT's member trade associations (and in turn their member firms) about the U.S. Government's export control activities.

Sincerely,



Eric L. Hirschhorn
Executive Secretary

ICOTT Members

American Association of Exporters and Importers (AAEI)
Semiconductor Equipment and Materials International (SEMI)
Semiconductor Industry Association (SIA)



Attached herewith are FICCI's observations on the Export Controls. I would sincerely appreciate your help in getting them to the concerned person.

With best regards,

Ranjana Khanna
Assistant Secretary General
FICCI USA
1050 17th Street NW, Suite 600
Washington DC 20036
Tel: 202 776 7181
Fax: 202 331 8703
EMail: ranjana@ficci.com
www.ficci.com

US Export Controls and Entities List

(A) Export Administration Regulations – Commerce Control List

Bureau of Industry and Security of the Government of USA maintains the Commerce Control List within the export administration regulations. The BIS also maintains the Commerce country chart which contains licensing requirements based on destination and reasons of control. Whilst reviewing the Commerce country's chart pertaining to India, we find that on the following counts exports to India from US are restricted and under export control procedures for issue of licenses.

- (i) Chemical and Biological Weapons : The controls under this category are maintained to support US Foreign Policy of opposing the proliferations and illegal use of chemical and biological weapons.
- (ii) Nuclear Non-Proliferation : Under this controls are exercised for export of such items which could be of significance for nuclear explosive purposes. Amongst other issues the non-proliferation credentials of the importing country are also taken into account.
- (iii) National Security : Under this category the US restricts the export and re-export of items that could make significant contribution to the military potential of any other country that could prove detrimental to the national security of the U.S.
- (iv) Missile Technology : The licensing requirements in this category are to support U.S. Foreign Policy to limit the proliferation of missiles. The term "missile" is defined as rocket systems, unmanned air vehicle systems etc.
- (v) Regional Stability : Under this category export and re-export of items is reviewed to determine whether export or re-export would contribute directly or indirectly to any country's military capability in a manner that could alter or destabilise region's military balance control to the foreign policy interest of the U.S.
- (vi) Crime Control : The licensing requirements here are to support U.S. Foreign Policy to observe human rights through out the world.



Classification of India under all these categories needs to be reviewed. There have been no occasions over the last 60 years since India became independent to categorise India for purposes of control of high technologies sales on the grounds of proliferation of chemicals or biological weapons. India's record in this aspect has been exemplary. In addition to this, any actions of this country can or have ever been attributable to be detrimental to the national security of either the U.S. or any other country including the South East Asian region. In fact India has been at the receiving end on various counts and has never been even a threat perception for any other country. India's record of human rights within the democratic system that we have is for all to see and does not at all justify controls for high technologies sales on these grounds.

(B) Entities List

The Entities List of the U.S. Government still includes establishments like ISRO, DRDO etc. In the current juncture of space and nuclear cooperation between India and the U.S.A. there is no justification for such organizations to remain under any restricted list by Government least of all from U.S. and this also needs to be reviewed.

Following Indian organizations are still on the US Entities List:

(a) Bharat Dynamics Limited

(b) The following subordinates of **Defense Research and Development Organization (DRDO)**:

Armament Research and Development Establishment (ARDE)
Defense Research and Development Lab (DRDL), Hyderabad
Missile Research and Development Complex
Solid State Physics Laboratory

(c) The following **Department of Atomic Energy** entities:

Bhabha Atomic Research Center (BARC)
Indira Gandhi Atomic Research Center (IGCAR)
Indian Rare Earths
Nuclear reactors (including power plants) not under International Atomic Energy Agency (IAEA) safeguards (excluding Kundankulam 1 and 2), fuel reprocessing and enrichment facilities, heavy water production facilities and their collocated ammonia plants.

(d) The following **Indian Space Research Organization (ISRO)** subordinate entities:

-Liquid Propulsion Systems Center
-Solid Propellant Space Booster Plant (SPROB)
-Sriharikota Space Center (SHAR)
-Vikram Sarabhai Space Center (VSSC), Thiruvananthapuram

(C) Upgrading the category of restriction from Tier 3 to 1:

Under the U.S. DOC Export Regulations India is still under Tier 3 and hence certain strategic activities including joint research and production is not possible.



If we are upgraded to Tier 2 instead of 3, we can do the above activities by sharing resources and data like some of the countries such as U.K., Germany, Japan etc.,

Of course, where U.S. has strategic reasons like nuclear weapons or certain rocket delivery systems this can be still be in the denial list, but, there are many where, if transparency is there and resources and information are shared, many activities can take place in the areas of Defence, Space, Advanced Scientific R&D by use of advanced technology tools.

Upgrading the category of restriction from Tier 3 to 2, number of large as well medium size corporations and research organisations can leverage each other's strengths without compromising strategic concerns, which can be leveraged by both sides. Although the threshold limits, for eg. for Super Computers, has been revised only last year, this limit is still not high enough considering the present state of technology. This necessitates going through the cumbersome export license process for many high end technological endeavors. The same logic applies to many other high tech products and applications.