

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

Published in Federal Register: October 23, 2006 ([71 FR 62065](#))

Comments due November 22, 2006

COMMENT #	SOURCE	SIGNER(S) OF LETTER	DATE	NUMBER OF PAGES
1.	Industry Coalition on Technology Transfer	Eric L. Hirschhorn, Executive Secretary (Submitted by Edward Gerwin)	November 20, 2006	2
2.	Sun Microsystems	Hans Luemers, Senior Director, International Trade Services (Submitted by Robert Rarog)	November 21, 2006	4
3.	Cogent Systems	James J. Jasinski, Executive Vice President (Submitted by James Cannon, Jr.)	November 22, 2006	83

Launch Act cross-waiver (49 U.S.C. 70101 *et seq.*) is applicable.

Michael D. Griffin,
Administrator.

[FR Doc. E6-17701 Filed 10-20-06; 8:45 am]

BILLING CODE 7510-13-P

DEPARTMENT OF COMMERCE

Bureau of Industry and Security

15 CFR Chapter VII

[Docket No. 061010262-6262-01]

Effectiveness of Licensing Procedures for Agricultural Commodities to Cuba

AGENCY: Bureau of Industry and Security, Commerce.

ACTION: Request for comments.

SUMMARY: The Bureau of Industry and Security (BIS) is requesting public comments on the effectiveness of its licensing procedures as defined in the Export Administration Regulations for the export of agricultural commodities to Cuba. BIS will include a description of these comments in its biennial report to the Congress, as required by the Trade Sanctions Reform and Export Enhancement Act of 2000 (Pub. L. 106-387), as amended.

DATES: Comments must be received by November 22, 2006.

ADDRESSES: Written comments (three copies) should be sent to Regulatory Policy Division, Bureau of Industry and Security, U.S. Department of Commerce, Room 2705, Washington, DC 20230 with a reference to TSRA 2006 Report, or to e-mail publiccomments@bis.doc.gov with a reference to TSRA 2006 Report in the subject line. Comments may also be emailed to Joan Roberts, Office of Nonproliferation and Treaty Compliance, at JRoberts@bis.doc.gov.

FOR FURTHER INFORMATION CONTACT: Joan Roberts, Office of Nonproliferation and Treaty Compliance, Telephone: (202) 482-4252. Additional information on BIS procedures and our previous biennial report under the Trade Sanctions Reform and Export Enhancement Act, as amended, is available at http://www.bis.doc.gov/licensing/TSRA_TOC.html. Copies of these materials may also be requested by contacting the Office of Nonproliferation and Treaty Compliance.

Copies of the public record concerning these regulations may be requested from: Bureau of Industry and Security, Office of Administration, U.S. Department of Commerce, Room 6883,

1401 Constitution Avenue, NW., Washington, DC 20230; (202) 482-2165. The Office of Administration 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) 482-2165 for assistance.

SUPPLEMENTARY INFORMATION: The Bureau of Industry and Security (BIS) authorizes exports of agricultural commodities to Cuba pursuant to section 906(c) of the Trade Sanctions Reform and Export Enhancement Act of 2000 (TSRA) (22 U.S.C. 7205(a)), under the procedures set forth in § 740.18 of the Export Administration Regulations (EAR) (15 CFR 740.18). These are the only licensing procedures currently in effect pursuant to the requirements of section 906(a) of TSRA. Please include the phrase TSRA 2006 on the envelope or in the subject line of the email as appropriate.

Under the provisions of section 906(c) of TSRA (22 U.S.C. 7205(c)), BIS must submit a biennial report to the Congress on the operation of the licensing system implemented pursuant to section 906(a) for the preceding two-year period. This report is to include the number and types of licenses applied for, the number and types of licenses approved, the average amount of time elapsed from the date of filing of a license application until the date of its approval, the extent to which the licensing procedures were effectively implemented, and a description of comments received from interested parties during a 30-day public comment period about the effectiveness of the licensing procedures. BIS is currently preparing a biennial report on the operation of the licensing system for the two-year period from October 1, 2004 to September 30, 2006.

By this notice, BIS requests public comments on the effectiveness of the licensing procedures for the export of agricultural commodities to Cuba set forth under § 740.18 of the EAR. Parties submitting comments are asked to be as specific as possible. All comments received by the close of the comment period will be considered by BIS in 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.

Copies of the public record concerning these regulations may be

requested from: Bureau of Industry and Security, Office of Administration, U.S. Department of Commerce, Room 6883, 1401 Constitution Avenue, NW., Washington, DC 20230; (202) 482-2165. The Office of Administration 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) 482-2165 for assistance.

Dated: October 17, 2006.

Christopher A. Padilla,
Assistant Secretary for Export Administration.

[FR Doc. E6-17707 Filed 10-20-06; 8:45 am]

BILLING CODE 3510-33-P

DEPARTMENT OF COMMERCE

Bureau of Industry and Security

15 CFR Chapter VII

[Docket No. 061005255-6255-01]

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 November 22, 2006.

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 Sheila Quarterman, Regulatory Policy Division, Bureau of Industry and Security, Department of Commerce, 14th Street & Pennsylvania Avenue, NW., Room 2705, Washington, DC 20230. Include "FPBEC" in the subject line of the message.

FOR FURTHER INFORMATION CONTACT: Joan Roberts, Director, 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/News/2006/foreignPolicyReport/Default.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); embargoed countries (part 746); countries designated as supporters of acts of international terrorism (§§ 742.8, 742.9, 742.10, 742.19, 746.2, and 746.7); 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 3, 2006 (71 FR 44551, August 7, 2006), 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 2006, 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 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 (if there are any differences) 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 the 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: October 12, 2006.

Christopher A. Padilla,
Assistant Secretary for Export
Administration.

[FR Doc. E6-17713 Filed 10-20-06; 8:45 am]

BILLING CODE 3510-33-P

DEPARTMENT OF THE TREASURY

Internal Revenue Service

26 CFR Part 1

[REG-110405-05]

RIN 1545-BE58

Limitations on Transfers of Built-in Losses

AGENCY: Internal Revenue Service (IRS), Treasury.

ACTION: Notice of proposed rulemaking.

SUMMARY: This document contains proposed regulations under section 362(e)(2) of the Internal Revenue Code of 1986 (Code). The proposed regulations reflect changes made to the law by the American Jobs Creation Act of 2004. These proposed regulations provide guidance regarding the determination of the bases of assets and stock transferred in certain nonrecognition transactions and will affect corporations and large shareholders of corporations, including individuals, partnerships, corporations, and tax-exempt entities.

DATES: Written or electronic comments and requests for a public hearing must be received by January 22, 2007.

ADDRESSES: Send submissions to CC:PA:LPD:PR (REG-110405-05),

Internal Revenue Service, PO Box 7604, Ben Franklin Station, Washington, DC 20044. Submissions may be hand delivered to CC:PA:LPD:PR (REG-110405-05), Courier's Desk, Internal Revenue Service, Crystal Mall 4 Building, 1901 S. Bell St., Arlington, VA. Alternatively, taxpayers may submit comments electronically directly to the IRS Internet site at www.irs.gov/regs or Federal e-Rulemaking Portal at www.regulations.gov (IRS REG-110405-05).

FOR FURTHER INFORMATION CONTACT:

Concerning the proposed regulations, Jay M. Singer, (202) 622-7530 (not toll-free number), or concerning submissions of comments, Richard A. Hurst, Richard.A.Hurst@irscounsel.treas.gov.

SUPPLEMENTARY INFORMATION:

Background

Prior to 1999, Congress grew concerned that taxpayers were engaging in corporate nonrecognition transactions in order to accelerate and duplicate losses. See S. Rep. No. 201, 106th Cong., 1st Sess. 46-48 (1999). Congress was primarily concerned with the acceleration and duplication of losses through the assumption of liabilities (including liabilities to which assets transferred in a corporate nonrecognition transaction were subject). As a result, in 1999, Congress enacted section 362(d) of the Code to prevent the bases of assets transferred to a corporation from being increased above such assets' aggregate fair market value as a result of a liability assumption. In addition, in 2000, Congress enacted section 358(h) to reduce the basis of stock received in certain corporate nonrecognition transactions, but not below fair market value, by the amount of any liabilities assumed in the transaction.

Following the enactment of sections 362(d) and 358(h), Congress remained concerned that taxpayers were engaging in various tax-motivated transactions to take more than one tax deduction for a single economic loss. Consequently, in the American Jobs Creation Act of 2004 (Pub. L. 108-357, 188 Stat. 1418), Congress enacted section 362(e), which limits the ability of taxpayers to duplicate net built-in loss in certain nonrecognition transactions.

Section 362(e)(1)(A) provides that if there would be an importation of a net built-in loss in a transaction described in section 362(a) or (b), the basis of certain property acquired in such a transaction shall be its fair market value immediately after the transaction. Section 362(e)(1)(B) provides that

property is described in section 362(e)(1) if gain or loss with respect to such property is not subject to tax in the hands of the transferor immediately before the transfer, and gain or loss with respect to such property is subject to tax in the hands of the transferee immediately after the transfer. Further, section 362(e)(1)(C) provides that there is an importation of net built-in loss in a transaction if the transferee's aggregate adjusted basis in such property would (but for the application of section 362(e)(1)) exceed the aggregate fair market value of such property immediately after the transaction.

Section 362(e)(2)(A) provides that if property is transferred by a transferor to a transferee in a transaction described in section 362(a) and not described in section 362(e)(1), and if the transferee's aggregate adjusted basis in the transferred property would (but for the application of section 362(e)(2)) exceed its aggregate fair market value immediately after the transfer, then the transferee's aggregate adjusted basis in the transferred property shall not exceed the fair market value of the property immediately after the transfer. Further, section 362(e)(2)(B) provides that this aggregate reduction in the basis of the transferred property shall be allocated among the property in proportion to their respective built-in losses immediately before the transaction. As an alternative to this reduction in the basis of the transferred assets, section 362(e)(2)(C) provides that if the transferor and the transferee both so elect, section 362(e)(2)(A) shall not apply, and the transferor's basis in the stock of the transferee received in exchange for the property that would otherwise be subject to basis reduction under section 362(e)(2)(A) shall not exceed its fair market value.

Since the enactment of section 362(e)(2), the IRS and Treasury Department have been exploring issues concerning the interpretation, scope, and application of the section and have proposed these regulations to address these issues. Additional guidance regarding the application of section 362(e)(2) to transfers between members of a consolidated group and the treatment of transactions that have the effect of importing losses into the U.S. tax system (to which section 362(e)(1) applies) will be addressed in separate guidance projects.

Explanation of Provisions

1. General Provisions

In general, these proposed regulations apply to transfers of net built-in loss property within the U.S. tax system in

ICOTT INDUSTRY COALITION ON TECHNOLOGY TRANSFER

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

November 20, 2006

Ms. Sheila Quarterman
Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
14th Street & Pennsylvania Avenue, NW
Room 2705
Washington DC 20230

Re: Effects of Foreign Policy-Based Export Controls (FPBEC), 71 Fed. Reg. 62065 (Oct. 23, 2006)

Dear Ms. Quarterman:

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

Ms. Shiela Quarterman

November 17, 2006

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 whose hundreds 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,

A handwritten signature in black ink, appearing to read "Eric L. Hirschhorn". The signature is fluid and cursive, with a long horizontal stroke at the end.

Eric L. Hirschhorn
Executive Secretary

cc: Hon. Mark Foulon
Hon. Stephen J. Hadley
Hon. Christopher A. Padilla
Hon. John Hillen
Hon. Condolezza Rice

November 21, 2006

Ms. Sheila Quarterman
Regulatory Policy Division,
Bureau of Industry and Security
Department of Commerce, Room 2705
14 St. and Pennsylvania Ave. NW
Washington, DC 02030

**Re: Effects of Foreign-Policy-Based Export Controls (Docket 0610055255-6255-01),
Federal Register, Oct. 23, 2006, Volume 71, No. 204**

Dear Ms. Quarterman:

Sun Microsystems, the world's leader in networked systems, again welcomes the opportunity to comment on foreign policy-based export controls administered by the Bureau of Industry and Security. Sun recognizes the necessity of such controls, but wishes to point out weaknesses in their general application, as well as particular issues with direct impact on Sun's ability to conduct global business operations.

As a general matter, export controls, including those imposed for foreign policy purposes, should meet three criteria:

- **Controls should support a defined objective.** Export controls should not be considered ends in themselves, but should be imposed with defined objectives. Only if the objective is defined can success be measured.
- **Controls must be consistent, predictable and flexible.** The specific execution of controls must be framed in a way to avoid unnecessary damage and to assist businesses in implementing them.
- **Controls should work.** If the objective of controls is to deprive the target country of a technology or commodity, issues like foreign availability and controllability must be regularly evaluated.

These principles are longstanding, and have been embodied in US export control legislation for many years. However, diligence is required to ensure that the imposition of new controls meets intended objectives and that their impacts do not change over time in unintended ways.

End-Use and End-User Controls

Sun is particularly concerned with the increasing recent emphasis on end-use and end-user controls. Sun has long felt (and has pointed out in previous annual comments on foreign policy controls), that this tool can be useful in limited circumstances, but has come to be overused.

Such controls, whether for foreign policy or other purposes, are not cost-free. End-use and end-user controls on broad categories of products require complex screening procedures, often including a combination of automated tools and internal processes. Moreover, it is typically the case that an analytical process must be developed in order to define screened entities (to distinguish between related, co-located or other apparently related organizations) and to determine end-use.

This process can be time consuming and, from the perspective of committing inadvertent violations, risky. As a result, it must be limited to export and reexports of items that have a reasonable probability of being employed to defeat an identifiable export control objective.

End-use/end-user controls on commonly available, non-strategic commercial items and routine service calls, combined with name screening against lists of thousands of proscribed entities, have become a major element of cost, delay and risk for US exporters. This is primarily because such requirements have become a defacto standard for all transactions, far in excess of their original, more focused intent. In aggregate, these controls have evolved over time into a major burden and competitive disadvantage.

As an example, the comprehensive end-use controls component of nonproliferation controls found in Part 744 are overly broad, do not advance the original intent of the Enhanced Proliferation Control Initiative, and produce disproportionate costs and compliance exposure for U.S. companies.

“Catch-all” controls of this sort are a very coarse and imprecise export control tool, and should not be used. As the range of items subject to EAR jurisdiction is extremely broad, catch-all controls by definition apply to items that have no substantive relevance to the proscribed proliferation (or other activity). Moreover, because such items may be produced in mass-market qualities, or are widely available in global markets, catch-all provisions administered by US companies may have no impact whatsoever in depriving particular entities of the non-listed items to which they apply.

Catch-all controls such as the EPCI requirements have two very real negative consequences. The first is that they are costly and divert compliance resources from elements of company control programs that do have a real strategic impact. Companies must assume that catch-all controls will be stringently enforced for even the most insignificant transactions, and must build their systems accordingly.

Second, as screening requirements springing from catch-all controls apply to items that are obviously irrelevant, they lessen respect for U.S. export controls in general among overseas customers, business partners, and employees.

We strongly urge that the “catch-all” dimension of EPCI controls be reviewed with a view to narrowing their scope to identifiable and achievable objectives. While end-use controls will continue to be an important export control tool, they can only be effective if

they are focused on specific geographic areas with well defined and narrow technological scope.

Sun strongly opposes the extension of catch-all type controls to other end-uses, such as those proposed on military end-uses in the July 6, 2006, notice on proposed controls for the People's Republic of China.

“Anti-Terrorism” (AT) Controls

There been no improvement in the last 12 months relevant to administration of anti-terrorism controls.

The range of items subject to AT controls exhibits no clear export control objective, and is at best grossly out of date. In the information technology area, control parameters have not been adjusted in over a decade and are now for the most part technologically irrelevant. However, they continue to be used as an alternative technological break point for selected foreign policy controls.

In many high-technology areas subject to controls based on performance or technological characteristics, controls must be periodically reviewed to account for normal and predictable technological advance. AT controls are no exception to this rule. To cite computer controls as an example, the current AT limit in 4A994 is set at .00001 Weighted Teraflops, while the Wassenaar limit (embodied in 4A003) has been raised in the last year to .75 WT.

In these circumstances, the practical effect of not adjusting controls to accommodate technological advance has been to shift to impact of controls from a focus on depriving target countries of specific technologies, to a selective economic embargo. Moreover, the selective nature of the embargo discriminates against those industries that are unlucky enough to be caught by out-of-date controls.

In the computer case, most companies no longer sell products below the .00001 cut-off, and have not for some time. As a result, such companies are subject to controls on all of their products, while companies in other industries can conduct substantial business simply because they have not been subject to technology-based controls in the past.

We strongly urge that AT controls be reviewed in order to more closely conceptualize and define their objectives (e.g., are they intended to inflict economic damage on terrorist supporting countries/governments, or are they intended to prevent particular items from being used by terrorists). This process is necessary in order to determine exactly where the appropriate levels must be set, particularly as most products caught by these controls are available from alternative sources in global markets.

In the computer area, we urge that the AT level be increased substantially to exclude mass-market computer products, and that it be converted to the new metric currently under discussion in Wassenaar.

Sun recognizes the important role of foreign policy-based controls, and is grateful for this opportunity to comment.

Sincerely,

Hans Luemers,
Senior Director,
International Trade Services,
Sun Microsystems

COGENT SYSTEMS

November 22, 2006

Sheila Quarterman
Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
14th Street & Pennsylvania Avenue, N.W.
Room 2705
Washington, DC 20230

Dear Ms. Quarterman:

Re: Effects of Foreign Policy-Based Export Controls

On behalf of Cogent Systems, Inc., enclosed please find the original and three copies of comments concerning the captioned proceeding. We are filing these comments pursuant to the notice published October 23, 2006. We are also filing these comments via email, but fear that the size of the file may cause technical difficulties.

Cogent Systems, Inc., a leading U.S. producer of one-to-many fingerprint retrieval systems, herein requests that the Bureau of Industry and Security and the President exclude such fingerprint systems from the Crime Control classification under the Export Administration Regulations (§ 7742.7). As outlined in detail in the enclosed submission, fingerprint retrieval systems from the world's leading producers are already installed in China. Continuing to suspend export licenses with respect to U.S.-made systems only ensures that a U.S. system will not be selected for the Olympics and that, long-term, U.S. producers will suffer a competitive disadvantage.

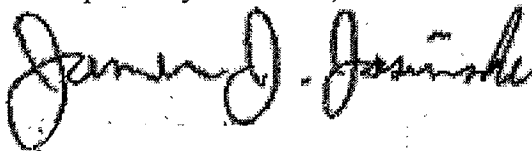
On the merits, the following points suggest that lifting the license suspension would be in the economic and foreign policy interests of the United States:

- Current technology for the analysis of fingerprints can be obtained from many third countries and is regularly exported to China from a leading producer in Japan;
- Equipment available from third countries is equal in terms of performance and technical sophistication to the equipment produced by U.S. manufacturers;
- U.S. manufacturers are prevented from developing new technology based upon the experience of applying fingerprint analysis technology to over one billion residents of China;

- U.S. exporters are prevented from exporting equipment that is competitive on the world market and are foreclosed from sales in one of the world's largest markets—sales that are accessible to the business competitors of the U.S. industry.
- Classification of fingerprint analysis technology under the “crime control” provision is inconsistent with the security requirements of the United States, as suggested by the Department of Homeland Security;
- China will be the host of the next Olympics and World's Fair and the use of U.S. fingerprint analysis equipment would provide heightened security against potential terrorist attacks; and
- China and the United States have already agreed in principle to develop “compatible” biometric systems in order to assist U.S. Customs in identifying people at the border.

For all of these reasons, Cogent respectfully requests that BIS and the President determine that classification of one-to-many fingerprint retrieval systems under the “Crime Control” provision is no longer in the national interest, within the meaning of Section 902(b) of the Tiananmen Square Sanctions. It is further requested that the annual report to Congress find that this export control should be rescinded in part.

Respectfully submitted,



James J. Jasinski
Executive Vice President
Cogent Systems

Enclosure

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

EFFECTS OF FOREIGN POLICY-BASED EXPORT CONTROLS:

*Request for Redetermination Pursuant to Section 902(b)
of the Tiananmen Square Sanctions (22 U.S.C. § 2151 note)
with respect to Certain Fingerprint Retrieval Systems
for Export to the People's Republic of China*

Cogent Systems, Inc.

November 22, 2006

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

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

Table of Contents

	<u>Page</u>
A. Executive Summary.....	1
B. Background.....	2
1. Cogent Systems, Inc.....	2
2. Fingerprint analysis systems.....	3
3. The Global market and industry producing fingerprint retrieval systems.....	4
4. The Tiananmen Square Sanctions.....	5
C. Removal of Certain Fingerprint Retrieval Systems from the “Crime Control” Provision is in the National Interest.....	8
1. The People’s Republic of China already has fingerprint retrieval systems from state-of-the-art suppliers.....	8
2. Barring U.S. exports from a major testing-ground for fingerprint technology has a negative impact on U.S. competitiveness.....	11
3. China’s use of compatible fingerprint retrieval systems is important to U.S. security policy.....	12
4. Access to U.S. fingerprint retrieval technology will not contribute to human rights violations in China.....	13
D. Review of the Factors for Consideration by BIS.....	15
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.....	15
2. Whether the foreign policy purpose of such controls can be achieved through negotiations or other alternative means.....	16
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.....	16
a. Megaports Initiative.....	17
b. Container Security Initiative.....	18

Table of Contents (Cont.)

	<u>Page</u>
c. Regional Cooperation	18
d. Anti-Money Laundering and Anti-Terrorist Investigations.....	19
e. Security Preparations for the Beijing Olympics	20
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	21
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, and the international reputation of the United States as a supplier of goods and technology	21
6. The ability of the United States to enforce the controls effectively	22
E. Conclusion	23

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

EFFECTS OF FOREIGN POLICY-BASED EXPORT CONTROLS:

***Request for Redetermination Pursuant to Section 902(b)
of the Tiananmen Square Sanctions (22 U.S.C. § 2151 note)
with respect to Certain Fingerprint Retrieval Systems
for Export to the People's Republic of China***

Cogent Systems, Inc.

A. Executive Summary

Cogent Systems, Inc., a leading U.S. producer of one-to-many fingerprint retrieval systems, herein requests that the Bureau of Industry and Security and the President exclude such fingerprint systems from the Crime Control classification under the Export Administration Regulations (§ 7742.7). This request is 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, 2006.¹ As outlined in detail below, fingerprint retrieval systems from the world's leading producers are already installed in China. Continuing to suspend export licenses with respect to U.S.-made systems only ensures that a U.S. system will not be selected for the Olympics and that, long-term, U.S. producers will suffer a competitive disadvantage.

On the merits, the following points suggest that lifting the license suspension would be in the economic and foreign policy interests of the United States:

- Current technology for one-to-many matching of fingerprints is available from Chinese vendors or can be obtained from many third countries, including leading producers in Japan and China;
- Equipment available from third countries is equal in terms of performance and technical sophistication to the equipment produced by U.S. manufacturers;

¹ *Effects of Foreign Policy-Based Export Controls*, 71 Fed. Reg. 62,065 (October 23, 2006) (Request for Comments).

**FINGERPRINT RETRIEVAL SYSTEMS FOR EXPORT TO CHINA
REQUEST OF COGENT SYSTEMS, INC.**

- U.S. manufacturers are prevented from developing new technology based upon the experience of applying fingerprint analysis technology to over one billion residents of China;
- U.S. exporters are prevented from exporting equipment that is competitive on the world market and are foreclosed from sales in one of the world's largest markets—sales that are accessible to the business competitors of the U.S. industry.
- Classification of fingerprint analysis technology under the “Crime Control” provision is inconsistent with the security requirements of the United States, as suggested by the Department of Homeland Security;
- China will be the host of the next Olympics and World's Fair and the use of U.S. fingerprint analysis equipment will provide heightened security against potential terrorist attacks; and
- China and the United States have already agreed in principle to develop “compatible” biometric systems in order to assist U.S. Customs in identifying people at the border.

For all of these reasons, Cogent respectfully requests that BIS and the President determine that classification of one-to-many fingerprint retrieval systems under the “Crime Control” provision is no longer in the national interest, within the meaning of Section 902(b) of the Tiananmen Square Sanctions (22 U.S.C. § 2151 note). It is further requested that the annual report to Congress find that this export control should be rescinded in part.

B. Background

1. Cogent Systems, Inc.

Cogent Systems is a leading provider of Automated Fingerprint Identification Systems (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, including: border security, event security, immigration, voting, asylum, citizen identification, driver's licenses, criminal investigations, and others.

FINGERPRINT RETRIEVAL SYSTEMS FOR EXPORT TO CHINA
REQUEST OF COGENT SYSTEMS, INC.

Cogent's technology was selected to support one of the United States Department of Homeland Security's top priority programs, U.S.-VISIT (United States Visitor and Immigrant Status Indicator Technology). Using biometric technology as the key identifier, this automated system expedites the entry/exit process for 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).

2. *Fingerprint analysis systems*

The specific fingerprint retrieval systems requested to be removed from the "Crime Control" provision include so-called "one-to-many" fingerprint retrieval software, technology and devices. One-to-many software relies upon an algorithm for matching a single fingerprint template to a database containing many fingerprint templates for purposes of identification. Commercially, such systems may be sold in the form of software, embedded in an application-specific integrated circuit (ASIC), or embedded in a hardware accelerator board that incorporates the algorithm.

Collective Exhibit 1 includes descriptive information concerning several Cogent products that fall within this category. The "Cogent Automated Palm and Fingerprint Identification System" ("CAFIS") and "CAFIS Prime" consist of software that can include the one-to-many matching algorithms or drive its hardware matchers, the "Programmable Matching Accelerator" or "PMA," also described in Exhibit 1. The PMA device includes one or more of Cogent's hardware accelerator boards with Cogent's embedded fingerprint template matching algorithm burned onto chips on the board. One or more PMA devices can be strung together and can perform one-to-many template matches at a rate of over 3 million images per second to 100 million matches per second depending on the system architecture. This product is used in the U.S.-VISIT program, discussed below.

Additionally, Cogent's algorithm is embedded in an ASIC or a commercial hardware device that contains the ASIC such as Cogent's "Mobile Ident II." and "BlueCheck" devices. These products are hand-held devices that permit a captured fingerprint to be matched against a database downloaded to the devices or send that fingerprint to a backend one-to-many matcher. These products may be used, for example, by local law enforcement or boarder patrol officers for matching captured fingerprints in the field.

FINGERPRINT RETRIEVAL SYSTEMS FOR EXPORT TO CHINA
REQUEST OF COGENT SYSTEMS, INC.

Similar one-to-many image retrieval systems are manufactured and distributed by several companies. Many of the producers of one-to-many algorithms, software and hardware are identified in Exhibit 2. Each company uses its own proprietary algorithms to perform the one-to-many matching that constitutes the core function of fingerprint retrieval systems. Although the algorithms are different, the accuracy and speed of the different systems are competitive.² Indeed, as described in greater detail below, software manufactured by two of the three leading producers is already in use in China.

3. *The Global market and industry producing fingerprint retrieval systems*

In addition to Cogent Systems in the United States, there are over 30 manufacturers of fingerprint analysis equipment and technology in the world. Exhibit 2 lists producers of fingerprint analysis equipment and technology. This list was compiled from various sources, including the National Institute of Standards and Technology (NIST) "Fingerprint Vendor Technology Evaluation 2003" (FpVTE)³ and the "FVC2004: Third Fingerprint Verification Competition."⁴

Fingerprint retrieval software and hardware are typically purchased by commercial and government or law enforcement end-users in a bid-auction process. That is, customers will typically issue requests for proposals and entertain bids from various qualified suppliers. In awarding contracts, consideration is given to each vendor's prior experience and installed systems. Purchasers will typically look for suppliers that have a history of manufacturing systems for very similar applications. Thus, if a purchaser is looking for a one-to-

² NIST and other government and academic bodies regularly perform studies regarding the accuracy and speed of different algorithms, as set forth in Exhibit 3 and discussed in section C(1) below.

³ Wilson, et al, "Fingerprint Vendor Technology Evaluation 2003," (hereinafter "FpVTE"), available online at <<http://fpvte.nist.gov/index.html>> (last visited November 17, 2006).

⁴ The University of Bologna, Michigan State University and San Jose State University conducted the "FVC2004: Third Fingerprint Verification Competition," available online at <http://bias.csr.unibo.it/fvc2004/results/Open_resultsAvg.asp> (last visited November 19, 2006). As indicated in the "background" section of the website, "The aim of FVC2004 is to track recent advances in fingerprint verification, for both academia and industry, and to benchmark the state-of-the-art in fingerprint technology."

FINGERPRINT RETRIEVAL SYSTEMS FOR EXPORT TO CHINA
REQUEST OF COGENT SYSTEMS, INC.

many image matching system that can handle a large database, including hundreds of millions of possible matches, the experience of the vendor in supplying large-database systems can be critical.

Different applications will present different challenges that can cause some algorithms to be more competitive than others. For example, a border-crossing application, such as U.S.-VISIT, requires both a high degree of accuracy and a high-speed match. A faster algorithm, all else being equal, will reduce wait times as persons queue up to the device. As the number of persons registered in the system grows, however, the database expands and both accuracy and speed will be affected. Thus, ongoing research and development is critical to the continued success of leading matching providers.

Exhibit 4 includes a presentation by the China National Body made before the ISO committee on Biometrics in London on July 10, 2006. This presentation identifies several market segments in China, including Time Attendance, Access Control, Lock, Government, Information Security, Police AFIS, and Others. Some of these applications will rely more heavily on one-to-one systems (e.g., access control, lock, information security). Others (e.g., Police AFIS) utilize one-to-many systems. Because the Chinese market is growing and particularly because law enforcement authorities are beginning to acquire AFIS, the Police AFIS segment will very likely grow to a much larger share.

4. *The Tiananmen Square Sanctions*

By statute, the Bureau of Industry and Security (BIS) of the Department of Commerce currently cannot license exports of so-called "crime control" equipment or technology to the People's Republic of China. Section 902(a)(4) of the Tiananmen Square Sanctions (22 U.S.C. § 2151 note) suspended all export control licenses covering crime control and detection equipment exported to China. Prior to enactment of the sanctions, fingerprint retrieval systems were eligible for an export license for shipment to China. The 1990 statute provides as follows:

(4) Crime control and detection instruments and equipment. The issuance of any license under section 6(k) of the Export Administration Act of 1979 for the export to the People's Republic of China of any crime control or detection instruments or equipment shall be suspended, unless the president makes a report under subsection (b)(1) or (2) of this section.

**FINGERPRINT RETRIEVAL SYSTEMS FOR EXPORT TO CHINA
REQUEST OF COGENT SYSTEMS, INC.**

The statute does not define “Crime control and detection instruments and equipment.” The coverage of this provision is instead set forth in the Export Administration Regulations, Part 774, § 3A981, as follows:

3A981 Polygraphs (except biomedical recorders designed for use in medical facilities for monitoring biological and neurophysical responses); fingerprint analyzers, cameras and equipment, n.e.s.; automated fingerprint and identification retrieval systems, n.e.s.; psychological stress analysis equipment; electronic monitoring restraint devices; and specially designed parts and accessories, n.e.s.

The suspension of authority to grant export licenses can be lifted by the President on the basis of finding that “it is in the national interest of the United States to terminate a suspension.”⁵ 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.⁶

Moreover, although not the “sole factor,” the “economic interests of the U.S. and of individual American companies ... are part of the national interest.”⁷ That the suspension of licenses on exports of U.S. one-to-many fingerprint

⁵ Section 902(b)(2) (22 U.S.C. § 2151 note).

⁶ CRS Report, No. RL31910, “China: Economic Sanctions,” Updated February 1, 2006, at CRS-2.

⁷ H.R. Conf. Rep. 101-343, 1990 U.S.C.C.A.N. 43 at 81 (1989).

**FINGERPRINT RETRIEVAL SYSTEMS FOR EXPORT TO CHINA
REQUEST OF COGENT SYSTEMS, INC.**

retrieval systems hurts the U.S. economically therefore must weigh into the balance.

Also, the national security interests of the United States merit consideration.⁸ In exercising the “national interest” waiver on a case-by-case basis, Presidents have cited, among other things, “items related to counter-terrorism.”⁹ Likewise, the national interest comprehends cooperation with other countries to combat terrorism—even with China. As, President Bush stated within one month of the September 11th attacks:

We have a common understanding of the magnitude of the threat posed by international terrorism. All civilized nations must join together to defeat this threat. . . . The President and the government of China responded immediately to the attacks of September 11th. There was no hesitation, there was no doubt that they would stand with the United States and our people during this terrible time. There is a firm commitment by this government to cooperate in intelligence matters, to help interdict financing of terrorist organizations. It is—President Jiang and the government stand side by side with the American people as we fight this evil force.¹⁰

⁸ H.R. Conf. Rep. 101-343 at 81.

⁹ D. Rennack, “China: Economic Sanctions,” Congressional Research Service Report RL31910, at CRS-2 (Feb. 1, 2006).

¹⁰ “U.S., China Stand Against Terrorism: Remarks by President Bush and President Jiang Zemin in Press Availability” (Oct. 19, 2001), posted on-line at <<http://www.whitehouse.gov/news/releases/2001/10/20011019-4.html>> (last visited Nov. 20, 2006).

FINGERPRINT RETRIEVAL SYSTEMS FOR EXPORT TO CHINA
REQUEST OF COGENT SYSTEMS, INC.

C. Removal of Certain Fingerprint Retrieval Systems from the “Crime Control” Provision is in the National Interest

1. *The People’s Republic of China already has fingerprint retrieval systems from state-of-the-art suppliers*

NEC Corporation, SAGEM and Cogent Systems vie for the lead in terms of accuracy and speed in one-to-many fingerprint matching. The NIST evaluation compared commercial, off-the-shelf fingerprint analysis and retrieval systems offered by 18 companies.¹¹ NEC, Cogent and SAGEM systems were the top three performers.¹² Notably, the top-performing system in the FpVTE was NEC. NEC Corporation is headquartered in Japan and has operations at 28 locations in China.¹³

NEC not only achieved the highest results in terms of accuracy in the NIST FpVTE, but also is the world’s largest supplier of one-to-many fingerprint retrieval systems to law enforcement customers. As shown by NEC’s website, NEC claims to have 65 percent of the world’s AFIS market, including 49 installations in Japan, 37 in the United States and 5 in China.¹⁴ “NEC AFIS collectively store over 60 million records and process more than 500,000 transactions daily helping solve more crimes from latent prints than all other systems combined.”¹⁵ Although not suggesting that NEC Corporation of America has exported one-to-many fingerprint retrieval systems to China, it is clear from published materials that the Japanese parent company or an affiliated company has exported this technology.¹⁶

¹¹ 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).

¹² FpVTE, Summary of Results at 16-17.

¹³ NEC Corporation website, <<http://www.nec.com/cgi-bin/office/country.-cgi?id=046>> (last visited November 20, 2006).

¹⁴ NEC Corp. of America website, <<http://www.necam.com/IDS/AFIS/Worldwide-Deployment.cfm>> (last visited November 17, 2006), included in Exhibit 5.

¹⁵ NEC Corp. of America website, <<http://www.necam.com/IDS/AFIS/>> (last visited November 17, 2006).

¹⁶ As discussed below, only the United States has suspended the issuance of export licenses with respect to fingerprint retrieval software, technology, and devices.

**FINGERPRINT RETRIEVAL SYSTEMS FOR EXPORT TO CHINA
REQUEST OF COGENT SYSTEMS, INC.**

SAGEM SA similarly is both a world leader in installed AFIS systems and a state-of-the-art performer in the NIST evaluation.¹⁷ Although SAGEM does not publicly list its installed systems, as does NEC, SAGEM has conducted pilot-plant testing in China and has been bidding in competition with other producers to supply regional AFIS in China. The SAFRAN Group, SAGEM's parent company, has four industrial sites and headquarters in China and three joint ventures with Chinese companies.¹⁸ With respect to AFIS systems, SAGEM has a large installed base and market share:

SAGEM Morpho is a pioneer and the current world leader in the Automated Fingerprint Identification System (AFIS) market. SAGEM Morpho and its parent company SAGEM SA enjoy a 48.8% market share in terms of revenues in the AFIS market and have over 1.5 billion fingerprints under management worldwide.¹⁹

Notably, SAGEM's technology was developed in conjunction with the U.S. Federal Bureau of Investigation:

Morpho's conversion skills were honed on the FBI's Fingerprint Identification Conversion Operation (FICO), which entailed the hard-card conversion of more than 36 million tenprint cards. Following a highly successful FICO performance, SAGEM Morpho's biometric algorithm was adopted by the FBI for its Integrated Automated Fingerprint Identification System (IAFIS), which currently processes searches of the entire FBI forensic database.²⁰

¹⁷ FpVTE, Summary of Results at 16-17.

¹⁸ "SAFRAN Worldwide, About SAFRAN," available online at <http://www.safran-group.com/recherchelocalisation.php3?id_pays=522&lang=en> (last visited November 20, 2006).

¹⁹ SAGEM Morpho website, available at <http://www.morpho.com/products_solutions/law_enforcement/law_enforcement.html> (last visited November 17, 2006).

²⁰ *Id.*

FINGERPRINT RETRIEVAL SYSTEMS FOR EXPORT TO CHINA
REQUEST OF COGENT SYSTEMS, INC.

SAGEM Morpho, the U.S. subsidiary of the SAFRAN Group, may not export one-to-many fingerprint retrieval systems to China under current U.S. controls. However, this prohibition does not apply to SAGEM SA in France or other SAFRAN Group companies or joint ventures. That is, French and EU export control laws permit exports of one-to-many fingerprint retrieval systems under appropriate licenses.²¹

In addition to the top-performing fingerprint retrieval technology currently installed or available from NEC and SAGEM, China's own Academy of Sciences was awarded third place in the "open" category for fingerprint matching algorithms in the FVC2004.²² 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."²³ China therefore has its own high quality fingerprint retrieval algorithms and software.

There are also private vendors of one-to-many fingerprint retrieval systems in China. Exhibit 2 identifies five Chinese producers included in the FVC2004 test. The FpVTE included Golden Finger, ranked in the lower third of the systems evaluated by NIST.²⁴ However, several factors affect system accuracy. FpVTE found that "[t]he variables that had the largest effect on the system accuracy were the number of fingers used and fingerprint quality:"

²¹ In response to Tiananmen Square, The European Council adopted an embargo on trade in arms to China in the form of an EC Declaration (June 27, 1989). The declaration does not identify specific products. EU members implement the embargo pursuant to the 1998 Code of Conduct on Arms Exports. However, the embargo has been interpreted narrowly to apply only to military equipment that might be used for internal repression. See R.F. Grimmett and T. Papademetriou, European Union's Arms Control Regime and Arms Exports to China: Background and Legal Analysis, Cong. Research Serv. Rep. No. RL32785, CRS-4 (March 1, 2005) and references cited therein. According to the Stockholm International Peace Research Institute (SIPRI), France interprets the embargo only to prohibit the exportation of "lethal items and major weapon platforms." SIPRI online at <<http://www.sipri.org/contents/expcon/euchiemb.html/view?searchterm=china%20embargo>>.

²² "FVC2004: Third Fingerprint Verification Competition," available online at <http://bias.csr.unibo.it/fvc2004/results/Open_resultsAvg.asp> (last visited November 19, 2006).

²³ "ANFIS-based fingerprint-matching algorithm," Optical Engineering, August 2004, pp. 1814-19, available online <<http://adsabs.harvard.edu/abs/2004OptEn..43.1814H>> (last visited November 20, 2006).

²⁴ FpVTE Summary of Results at 9-15.

FINGERPRINT RETRIEVAL SYSTEMS FOR EXPORT TO CHINA
REQUEST OF COGENT SYSTEMS, INC.

- “Additional fingers greatly improve accuracy
- “Poor quality fingerprints greatly reduce accuracy”²⁵

To evaluate the performance of Chinese producers, therefore, it is important to consider the application. For example, authorities would presumably be able to obtain two or more high quality fingerprints from a person detained or in custody. Also, in contrast to a border security system that must find a match in seconds, a system attempting to match fingerprint images taken from a person in custody will be able to search the database for a longer time, with a resulting improvement in accuracy.

Hence, even a relatively poor fingerprint retrieval system could identify a person in custody for purposes that might implicate human rights violations. On the other hand, a border entry system that processes thousands of persons per day or a system that is attempting to identify a single latent fingerprint from a crime scene would benefit significantly from a greater degree of accuracy.

For these reasons, the existing domestic Chinese technology is adequate for the types of applications for which the Crime Control classification was devised. However, if China is to be a partner in identifying terrorists and international criminals, it would benefit by access to higher-performing U.S.-made systems.²⁶

2. *Barring U.S. exports from a major testing-ground for fingerprint technology has a negative impact on U.S. competitiveness*

Two considerations have a negative impact on the ability of U.S. producers to remain competitive: (1) lack of access to the largest world population and thus the largest possible fingerprint database; and (2) lack of testing and feedback concerning a variety of ethnic fingerprints. As discussed above, the procurement of fingerprint retrieval systems typically takes the form of a bid system, responding to requests for proposals. Past experience is a critical factor in evaluating the bids submitted. Hence, without access to the large database applications that exist in China, Cogent and other U.S. producers will

²⁵ FpVTE Summary of Results at 3.

²⁶ In this regard, it may be noted that FpVTE identified Motorola (U.S.) and Dermalog (Germany) as the most accurate systems after NEC, SAGEM and Cogent. FpVTE Summary of Results at 16.

**FINGERPRINT RETRIEVAL SYSTEMS FOR EXPORT TO CHINA
REQUEST OF COGENT SYSTEMS, INC.**

have more limited experience with these applications than their Japanese, Chinese, or European competitors.

Fundamentally, because the algorithms and technology are improved through use, U.S. producers will over time lack experience with the largest databases and with various types of ethnic fingerprints. NEC Corporation touts its experience and the value of customer feedback: "Current customers remain a valuable resource for Research and Development on how to improve AFIS design and operation."²⁷ To the extent that the U.S. industry is cut off from a huge potential customer base, U.S. research and development efforts will suffer.

Because the characteristics of different ethnic groups affect fingerprints,²⁸ this lack of experience will inevitably have a negative impact on the development of U.S. technology. Even the identification of terrorists may be affected if the U.S. industry loses technological parity. However, whether or not U.S. identification capabilities are degraded over time, it is in the national interest for U.S. producers simply to remain competitive with European, Japanese and Chinese producers.

3. *China's use of compatible fingerprint retrieval systems is important to U.S. security policy*

Assessment of the national interest demands consideration of U.S. economic interests, as well as national and international security interests. The Conference Report accompanying passage of the Tiananmen Square Sanctions 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."²⁹ Accordingly, the statute provided conditions under which the President could waive a suspension.

In this context, China's role in supporting the war on terror should be considered. As outlined below in section D(3)(c), China has worked generally to increase the regional support for counterterrorism through the Association of Southeast Asian Nations (ASEAN), ASEAN plus 3, the Asia Pacific Economic

²⁷ NEC America web site, <<http://www.necam.com/IDS/AFIS/>> (last visited November 20, 2006).

²⁸ See, e.g., A. Jasiorouski, "Regional Differentiation of Palm Dermatoglyphs in Rural Populations in Poland, *Ann. Agric. Env. Med.* 12 (2005) at 277-280 (finding that statistically significant differences result from ethnic isolation).

²⁹ H.R. Conf. Rep. 101-343 at 80.

FINGERPRINT RETRIEVAL SYSTEMS FOR EXPORT TO CHINA
REQUEST OF COGENT SYSTEMS, INC.

Cooperation organization (APEC), and the Shanghai Cooperation Organization (SCO). China has also provided support to specific anti-terrorist operations.

Currently, the Federal Bureau of Investigations is exchanging latent fingerprints through Interpol for matching against databases maintained by 186 countries, including China.³⁰ The FBI is also gathering terrorist fingerprints and biographical data from cooperative international exchange programs and foreign Legats.³¹ The FBI has opened a Legat in Beijing, China since September 11.³² The United States, therefore, has a vital interest in the accuracy and speed of the fingerprint retrieval systems used by China. As noted in the NIST evaluation, only the top-three systems (by NEC, Cogent and SAGEM) performed at a high level across different databases.³³ Although China now has NEC technology installed and has access to SAGEM technology, U.S.-made systems should also be made available in the interest of enhancing U.S. security.

Indeed, it has been reported that the Department of Homeland Security has discussed the use of compatible systems as a means of assisting U.S. Customs to identify persons entering the United States. "According to reports, China and the U.S. ... can develop cooperation in identification systems and identity documents, such as by China using biometric systems that are compatible with the U.S. and assisting U.S. Customs in identifying the status of people entering borders."³⁴

4. *Access to U.S. fingerprint retrieval technology will not contribute to human rights violations in China*

First, and most importantly, lifting the suspension on export licenses with respect to exports of fingerprint retrieval systems will not eliminate the need to obtain an export license. Coupled with new Validated End User requirements and

³⁰ See, e.g., Interpol member countries, online at <<http://www.interpol.int/Public/IPC/MNMembers/default.asp>>, (last visited November 22, 2006).

³¹ See Memorandum from the Attorney General, dated April 11, 2002, "Coordination of Information Relating to Terrorism" at 3 (directing the FBI to establish procedures for regularly collecting fingerprint information regarding known or suspected terrorists).

³² FBI, International Operations, online at <<http://www.fbi.gov/aboutus/transformation/international.htm>> (last visited November 22, 2006).

³³ FpVTE, Summary and Analysis at 17 ("The most accurate systems performed consistently well over a variety of image types and data sources").

³⁴ SINA, April 5, 2006, available online at <<http://www.sina.com.cn>> (last visited November April 8, 2006) (unofficial translation).

FINGERPRINT RETRIEVAL SYSTEMS FOR EXPORT TO CHINA
REQUEST OF COGENT SYSTEMS, INC.

the “know-your-customer” policies applied in granting licenses, the requirements found in the regulations will adequately protect against the potential use of U.S. technology as a means of identifying or persecuting dissidents in China.

In this regard, it is noteworthy that law enforcement and government account for only a small fraction of the market for fingerprint retrieval systems. The 2006 presentation by the China National Body³⁵ showed that law enforcement applications accounted for 7.58 percent of all installations; government use accounted for only 4.1 percent. The major end-uses were as follows:

Applications	Mkt Share
Time Attendance	42.2%
Access Control	27.6%
Lock	14.3%
Government	4.1%
Information Security	0.97%
Police AFIS	7.58%
Others	3.25%
Total	100.0%

Although it is anticipated that local law enforcement use of AFIS will increase substantially in the near term, there will continue to be a significant commercial market for fingerprint retrieval systems. Sales to such end-users can be licensed under rigorous conditions to ensure that the technology is not misused. Indeed, exports to government end-users, such as local law enforcement or security for the Olympics, are also susceptible to license requirements, end-user certification or post-shipment monitoring.

Second, as outlined above, existing technology in China is more than adequate to identify persons that are detained or in custody. Given that NEC and Golden Finger systems are already installed in China,³⁶ licensing U.S. exporters to

³⁵ Exhibit 4, attached.

³⁶ According to its website, Golden Finger has recently won several AFIS contracts, including contracts to supply the Xinjiang Uyghur autonomous region in May 2004, the Ministry of Public Security and Immigration in May 2005, the Shanghai Municipal Public Security Bureau in July 2005, and the Ministry of Public Security Technology in March 2004. Eastern Golden Finger website, <<http://www.etgoldenfinger.com/>> (last visited November 21, 2006) (unofficial translation).

**FINGERPRINT RETRIEVAL SYSTEMS FOR EXPORT TO CHINA
REQUEST OF COGENT SYSTEMS, INC.**

supply fingerprint retrieval systems will not have any effect on China's ability to commit human rights' violations. To the contrary, licensing exports of U.S. technology should forge relationships with China and Chinese law enforcement that provide the United States with additional leverage to reduce human rights violations.

D. Review of the Factors for Consideration by BIS

The October 23, 2006 invitation to comment identified six specific issues to be addressed.³⁷ As shown above and summarized below, each factor in this case supports removal of fingerprint retrieval systems from the Crime Control provision.

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

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 crime control and detection items, at this time these controls are maintained only by the United States.³⁸

In its 2006 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.”³⁹ Instead, BIS points to the

³⁷ Request for comments, 71 Fed. Reg. at 62,066.

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

³⁹ U.S. Bureau of Industry and Security, 2006 Foreign Policy Report, Chapter 2, § B(1), <http://www.bis.gov/News/2006/foreignPolicyReport/fprchap02_CrimeControl.html> (last visited November 20, 2006) (emphasis added).

**FINGERPRINT RETRIEVAL SYSTEMS FOR EXPORT TO CHINA
REQUEST OF COGENT SYSTEMS, INC.**

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."⁴⁰ 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 documented above, China has access to top-rated one-to-many fingerprint retrieval systems from Europe and Japan, it has a government-developed algorithm that achieved third place in an international competition, and it has several domestic suppliers. In these circumstances, the suspension of U.S. export licenses is insufficient to achieve any foreign policy of the United States.

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

As outlined in section 3, 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. 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.

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*

The controls at issue are incompatible with a strong demonstrated U.S. foreign policy objective to enlist China's continuing cooperation in the global war against terror. According to the most recent Country Report of 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

⁴⁰ *Id.*

FINGERPRINT RETRIEVAL SYSTEMS FOR EXPORT TO CHINA
REQUEST OF COGENT SYSTEMS, INC.

Asia.⁴¹ China's actions in this area have most notably supported the following U.S. programs: 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.

a. Megaports Initiative

A nonproliferation program of the U.S. Department of Energy's National Nuclear Security Administration ("NNSA"), the Megaports Initiative works with foreign partners to enhance their capabilities to detect, deter and interdict illicit shipments of nuclear and other radioactive materials through the international maritime shipping network.⁴² Under this program, the United States and China have agreed to install special equipment at ports in China to detect hidden shipments of nuclear and other radioactive material.⁴³

Of China's participation in the Megaports initiative, NNSA Administrator Linton F. Brooks has said: "The United States and the People's Republic of China recognize the importance of joining forces against the threat posed by the trafficking of nuclear and other radioactive materials."⁴⁴ Accordingly, the Megaports initiative "represents a significant step forward in the effort to improve the security of the global maritime shipping network, and furthers both nations' efforts to work cooperatively in hindering terrorism."⁴⁵

⁴¹ *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").

⁴² *See* National Nuclear Security Administration (U.S. Department of Energy), "U.S. and the People's Republic of China Cooperate on Detecting Illicit Shipments of Nuclear Material" (Nov. 22, 2005), <http://www.nnsa.doe.gov/docs/newsreleases/2005/PR_2005-11-22_NA-05-30.htm> (last visited November 20, 2006).

⁴³ *See id.*

⁴⁴ *Id.*

⁴⁵ *Id.*

FINGERPRINT RETRIEVAL SYSTEMS FOR EXPORT TO CHINA
REQUEST OF COGENT SYSTEMS, INC.

b. Container Security Initiative

Further addressing the threat to border security posed by the potential terrorist use of a maritime container to deliver a weapon, the Container Security Initiative (“CSI”) seeks to identify and inspect all high-risk containers at foreign ports before they are placed on vessels destined for the United States.⁴⁶ China first joined CSI in 2002.⁴⁷ Shanghai⁴⁸ and Shenzhen⁴⁹ became operational CSI ports in 2005. Working together in Shanghai, Chinese Customs officials and a team of U.S. Bureau of Customs and Border Protection (“CBP”) officers target, identify and screen maritime containers destined for the United States and considered a potential terrorist risk.⁵⁰

When China first added Shanghai to the foreign ports participating in CSI, Clark T. Randt, Jr., the U.S. Ambassador to China, said: “I anticipate continuing the strong cooperative relationship in combating terrorism that has developed between the U.S. and China. CSI Shanghai will be a key link in the worldwide CSI chain that seeks to deter terrorist activity.”⁵¹

c. Regional Cooperation

China has actively increased regional cooperation in the U.S. war against terror. Regarding China’s actions, the U.S. State Department’s 2005 Country Report particularly notes that “Chinese officials signed statements with

⁴⁶ See U.S. Bureau of Customs and Border Protection, “China Joins the U.S. in Container Security Initiative” (Oct. 25, 2002), <http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/legacy/2002/102002/china_joins_csi_1025.xml> (last visited Nov. 20, 2006).

⁴⁷ See *id.*

⁴⁸ See U.S. Bureau of Customs and Border Protection, “China Implements Container Security Initiative at Port of Shanghai to Target and Pre-Screen Cargo Destined For U.S.” (Apr. 28, 2005), <http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/2005_press_releases/042005/04282005.xml> (last visited November 20, 2006).

⁴⁹ See U.S. Bureau of Customs and Border Protection, “Container Security Initiative Port of Shenzhen, China, is Operational” (June 24, 2005), <http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/2005_press_releases/062005/06242005.xml> (last visited November 20, 2006).

⁵⁰ See “China Implements Container Security Initiative at Port of Shanghai . . .,” *supra*.

⁵¹ See *id.*

FINGERPRINT RETRIEVAL SYSTEMS FOR EXPORT TO CHINA
REQUEST OF COGENT SYSTEMS, INC.

counterterrorism components in regional fora such as the Association of Southeast Asian Nations (ASEAN) Regional Forum (ARF), ASEAN plus 3, the Asia Pacific Economic Cooperation organization (APEC), and the Shanghai Cooperation Organization (SCO).⁵² Specifically:

- “China agreed to participate in APEC inspections of civilian airports to assess vulnerabilities. . . .”⁵³
- “China hosted an ARF Security Policy Conference and an ARF Seminar, where participants addressed non-traditional security threats, including counterterrorism issues.”⁵⁴
- “As a founding member of the Shanghai Cooperation Organization (SCO), China played an instrumental role in getting the SCO to issue a Joint Statement on increasing regional cooperation to fight terrorism, extremism, and separatism.”⁵⁵

Such regional cooperation is consistent with U.S. foreign policy interests and is consistent with relaxing the suspension of licensing authority regarding one-to-many fingerprint retrieval systems.

d. Anti-Money Laundering and Anti-Terrorist Investigations

The State Department’s 2005 report touts the China’s progress in anti-money laundering, a key component of the war against terror:

- “China has taken steps to strengthen regulatory measures to combat money laundering, and is finalizing money laundering legislation designed to broaden the scope of existing anti-money laundering regulations and to establish more firmly the PBOC’s [People’s Bank of China’s] authority over national anti-money laundering operations.”⁵⁶
- “Under the authority of the PBOC, China established a Financial Intelligence Unit (FIU) in 2004 to track suspicious transactions and is

⁵² Country Reports at 66.

⁵³ *Id.*

⁵⁴ *Id.*

⁵⁵ *Id.*

⁵⁶ *Id.*

**FINGERPRINT RETRIEVAL SYSTEMS FOR EXPORT TO CHINA
REQUEST OF COGENT SYSTEMS, INC.**

working closely with FINCEN [Financial Crimes Enforcement Network] in the United States to develop its capabilities.⁵⁷

- In 2005 China was granted observer status in the Financial Action Task Force (FATF): “China’s money laundering legislation, when completed, will go a long way toward satisfying FATF’s criteria for membership.”⁵⁸

China has also provided logistical and diplomatic support to specific anti-terrorist investigations consistent with U.S. foreign policy:

- At a U.N. Security Council meeting in 2005, China’s Permanent Representative called on U.N. members to adopt measures to “crack down” on an al-Qaida-affiliated East Turkistan Islamic organization that the United States also designated under Executive Order 13224.⁵⁹
- Formally established in 2004, the FBI Legal Attaché Office in Beijing during 2005 “bolstered U.S.-Chinese cooperation on counterterrorism investigations,” resulting in “substantive intelligence.”⁶⁰

Again, U.S. foreign policy and Chinese anti-terrorist action have been consistent. Allowing U.S. vendors to supply one-to-many fingerprint retrieval systems will complement U.S.-Chinese cooperation.

e. Security Preparations for the Beijing Olympics

As the 2008 Beijing Olympics loom, potential terrorism on Chinese territory poses a real threat. Accordingly, China has recently increased its efforts to build domestic counterterrorism capabilities:

- “China sent several officers to Greece for counterterrorism and Olympic security training; it also sent police chiefs to observe the 25th ASEAN Chief of National Police (APOL) Conference in Indonesia.”⁶¹

⁵⁷ Country Reports at 66-67.

⁵⁸ Country Reports at 67.

⁵⁹ *Id.*

⁶⁰ *Id.*

⁶¹ *Id.*

**FINGERPRINT RETRIEVAL SYSTEMS FOR EXPORT TO CHINA
REQUEST OF COGENT SYSTEMS, INC.**

- “China continued to participate in training programs at the International Law Enforcement Academy in Bangkok, Thailand.”⁶²
- “In 2005, China staged antiterror exercises in major cities throughout the country and implemented new antiterrorism training programs at several major police academies.”⁶³

It is expected that China will utilize a fingerprint retrieval system to ensure that workers hired for the Olympics are not terrorists. Soon, China will issue requests for proposals to supply such systems for use at the Olympics. A system that permits entry of workers, in the same manner as U.S.-VISIT authorizes travelers, will be a critical safeguard to prevent any terrorist incident. To the extent that a U.S. producer is able to win the bidding and supply a state-of-the-art system, the reputation of the United States, not to mention our relations with China, are enhanced.

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*

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.

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, and the international reputation of the United States as a supplier of goods and technology*

Maintaining the suspension on export licenses for one-to-many fingerprint retrieval systems will have little or no 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

⁶² *Id.*

⁶³ *Id.*

FINGERPRINT RETRIEVAL SYSTEMS FOR EXPORT TO CHINA
REQUEST OF COGENT SYSTEMS, INC.

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. 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;
- 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; and
- U.S. producers are unable to gain experience matching a large and diverse database of ethnic fingerprints.

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.

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

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 FY2005.⁶⁴ These approvals amounted to \$17 million in value.

⁶⁴ 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).

**FINGERPRINT RETRIEVAL SYSTEMS FOR EXPORT TO CHINA
REQUEST OF COGENT SYSTEMS, INC.**

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 items such as these....”⁶⁵ 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.

E. Conclusion

For all of these reasons, Cogent respectfully requests that BIS and the President determine that classification of one-to-many fingerprint retrieval systems under the “Crime Control” provision is no longer in the national interest, within the meaning of Section 902(b) of the Tiananmen Square Sanctions (22 U.S.C. § 2151 note). It is further requested that the annual report to Congress find that this export control should be rescinded in part.

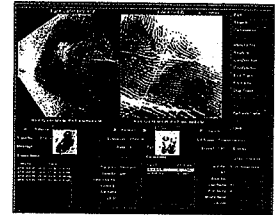
⁶⁵ 2006 Foreign Policy Report, Chapter 2 at 8 (emphasis added).

EXHIBIT 1

Product & Solution Overview

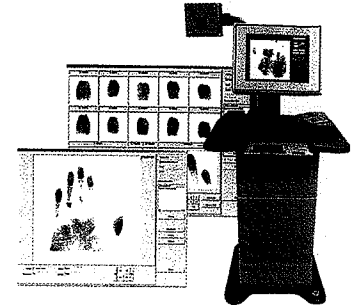
Cogent Automated Palm and Fingerprint Identification System (CAPFIS)

CAPFIS is a total system solution for large-scale distributed fingerprint and palm print identification/processing systems. Customized workflows allow integration with LiveScan, LiveID, mobile units, photo capture, criminal history, and other identification system components.



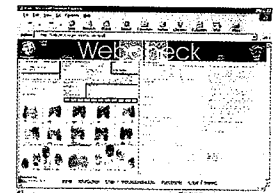
LiveScan Product Line

A full line of FBI-certified, advanced LiveScan workstations encompassing single fingerprint scanners, booking LiveScan stations, and desktop and portable LiveScans for civil applications. Models are available for both fingerprint and palm print capture.



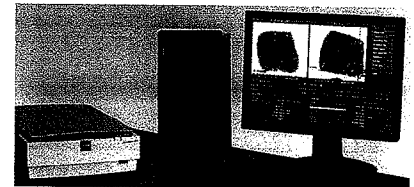
WebCheck

Web server application for use in processing fingerprint-based criminal history background checks.



Programmable Matching Accelerator (PMA)

The world's fastest and most accurate fingerprint and palm print matcher. Used in some of the largest and fastest fingerprint/palm print identification systems in the world. Each unit can perform up to 2,000,000 matches per second and can be used in parallel.

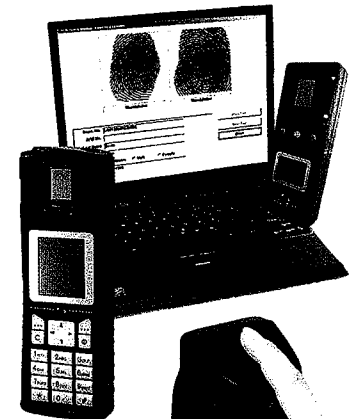


CAFIS Prime

A self-contained, desktop Automated Fingerprint Identification System for law enforcement applications. (Fingerprint and palm print identification)

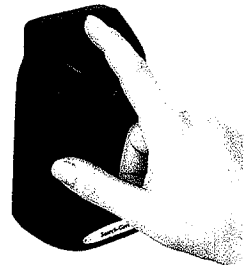
LiveID

Flat, single-finger identification solutions ranging from handheld devices to desktop workstations, to high-speed, distributed systems.



Mobile Ident II

Mobile Ident II is a handheld identification/authentication device. It uses Cogent's SecurASIC™ - best described as an AFIS on a chip allows a user to download a database of suspect fingerprints for local "on-board" searching. Mobile Ident II can also be connected to a central AFIS via a wireless link for searching a local or national database.



BioGate Product Line

Complete biometric access control product line, supporting 1:1,200 searching and 1:1 verification devices. Designed for industrial sites and corporate offices.

COGENT  SYSTEMS

Beyond Comparison

Cogent Systems, Inc.
209 Fair Oaks Avenue, South Pasadena, CA 91030 USA

Tel: +1 626 799 8090 Fax: +1 626 799 8996

www.cogentsystems.com email: Info@cogentsystems.com

COGENT

About Cogent Systems

Since 1990, Cogent (NASDAQ:COGT) has delivered the fastest, most accurate, and most sophisticated biometric fingerprint identification solutions in the world. Cogent has grown at an average annual rate of 25 percent since commercializing our first product in 1993, and is publicly traded on the NASDAQ Stock Market. As a world leader, Cogent provides first class Automated Fingerprint Identification Systems (AFISs) and biometric access control solutions to governments, law enforcement agencies, and commercial customers worldwide.

Cogent's products can be found at the heart of the largest automated identification systems in the world. These solutions are tailored to meet customer database size and throughput requirements using software-based technology, customized ASIC processors, or massively parallel/super-pipelined data flow computing servers. 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, including: immigration, voting, asylum, citizen benefits/rights, citizen identification, driver's licenses, criminal investigations, and others.

Most recently, Cogent was awarded a contract as the prime contractor for a new integrated Automated Fingerprint Identification System (AFIS) for the Royal Canadian Mounted Police (RCMP). The AFIS will be used by the RCMP as part of its Real Time Identification (RTID) initiative which will meet the growing demands for post 9/11 identification services for criminal, civil, immigration, and international needs.

Cogent's technology was selected to support one of the United States Department of Homeland Security's top priority programs, US-VISIT (United States Visitor and Immigrant Status Indicator Technology). Using biometric technology as the key identifier, this automated system expedites the entry/exit process for those legitimate travelers to the US.

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 smart card program, Hong Kong's National Smart Identity Card System (SMARTICS).

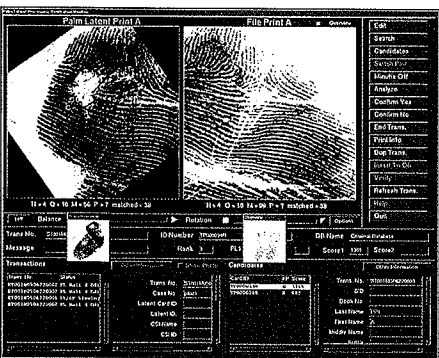
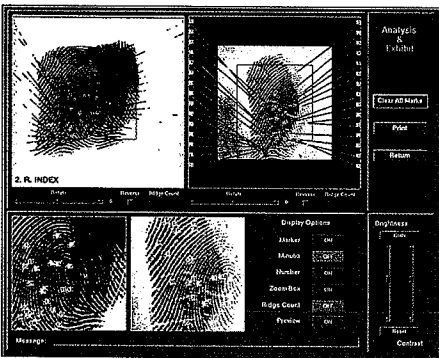
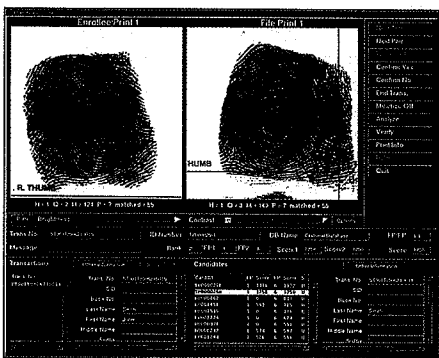
Using Cogent's patented image reconstruction and highly accurate fingerprint matching algorithm, Cogent's BioSwipe API is perfect for small processor PDAs and PC-based applications requiring fingerprint identification using a swipe sensor. BioSwipe has been used in four of HP's iPAQ products and the Lexar TouchGuard product, which won Time Magazine's 2004 Gadget of the Year award.

Cogent's vision is to provide the highest quality identification systems, products, and services with unparalleled innovation, accuracy, and speed.

CAFIS™ / CAPFIS™

Automated Fingerprint / Palm Print Identification System

CAFIS™ is a multifactor, scalable, and customizable software package that allows you to perform a wide range of tasks for processing, editing, searching, retrieving, and storing fingerprint images and subject records. It includes a variety of automated identification solutions – from a desktop AFIS (CAFIS Prime™) to distributed networked solutions for local, regional, and national systems. As one of the most accurate systems in the world, CAFIS ensures service resiliency while providing information safety through the use of built-in safeguards such as fault tolerant architecture, disk mirroring, automated database backups, and disaster recovery options.



Features

Superior searching capability: 100% penetration for tenprint, latent, and palm print searches. Performs searches in a variety of ways: tenprint to tenprint, tenprint to unsolved latent, latent to tenprint, latent to unsolved latent, palm to unsolved palm latent, palm latent to palm, and palm latent to unsolved palm latent.

Ease of integration/versatility: CAFIS can be integrated with external AFIS systems, computerized criminal history systems, LiveScans, handheld wireless devices, web-based Internet solutions, and other information systems.

Scalability: Modular and expandable architectural elements that can be scaled to meet any agency's database size, throughput, and integration requirements.

Handles a wide range of database sizes: Meets the needs of agencies with record collections of a few thousand to several million.

Fast: Using the power of Cogent's Programmable Matching Accelerator (PMA) servers, CAFIS provides rapid response time; CAFIS supports search speeds from 15,000 to 500,000 matches per second. Multiple PMA servers can be rack-mounted to linearly increase matching throughput to up to 1,500,000 matches per second.

Easy to Use: Provides you with a wide assortment of special image processing tools to enhance the viewing quality of an image before saving it in the database, to mark minutiae, to initiate database searches, and to verify matches.

CAFIS™ / CAPFIS™

For law enforcement agencies with finger and palm print record collections ranging from a few thousand to millions, Cogent provides automated identification solutions from a desktop AFIS (CAPFIS Prime) to distributed networked solutions for local, regional, and national systems (CAPFIS). Cogent is unique among AFIS vendors in that we use non-proprietary NIST record formats for our AFIS database records. As a result, the system can be integrated with external AFIS systems, computerized criminal history systems, LiveScan, handheld wireless devices, secure, web-based Internet solutions, as well as other information systems.

Featuring a 100% database search for tenprint, latent, and palm print identification, CAPFIS has proven itself to be one of the most accurate systems in the world. CAPFIS can be configured with a number of built-in safeguards that ensure service resiliency while providing safety of information (via fault tolerant architecture, disk mirroring, automated database backups, and disaster recovery options). CAPFIS features modular and expandable architectural elements that can be scaled to meet any agency's database size, throughput, and integration requirements.

CAFIS/CAPFIS provides the solution for agencies that:

- > Require fingerprint/palm print matching systems with databases of up to tens of millions of records
- > Need rapid response times
- > Must support a few users to thousands of users
- > Want to include LiveScans and wireless biometric input devices
- > Require integration of existing information systems
- > Need to provide secure web-based identification services

For agencies with modest throughput requirements, systems can be configured using an NT- or UNIX-based transaction server hosting the Image Flow, Data Flow, and Information Fusion software. Any number of modular elements can be configured, including workstations for tenprint, latent, and palm print processing; LiveScan for tenprint and palm print capture; and wireless handheld computers.

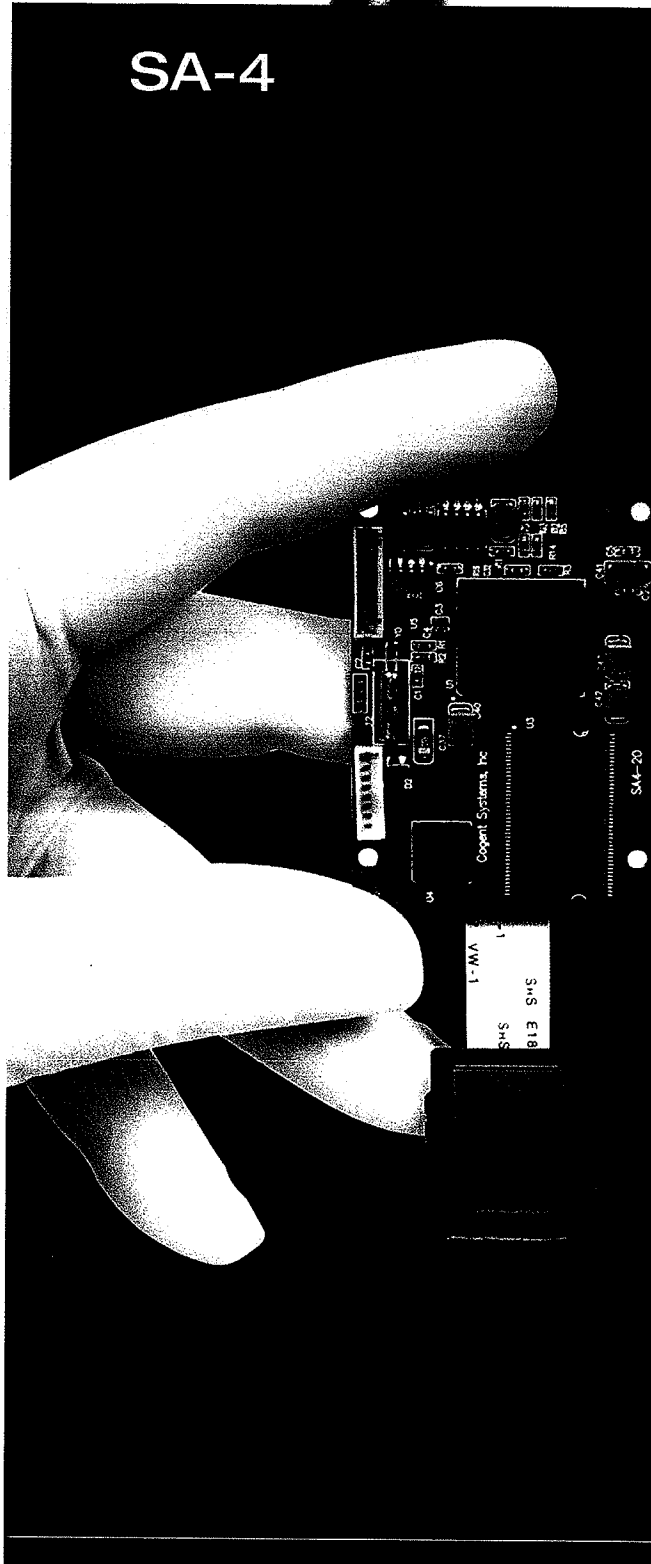
For agencies with databases containing tens of thousands to millions of records and requiring real-time identification results, Cogent's Programmable Matching Accelerator (PMA) servers can be used. Multiple PMA servers can be rack mounted to linearly increase matching throughput and to support system growth and expansion. This proven technology is widely used by cities, counties, states, and national governments as a cost-effective and modular data flow computing technology to meet their needs today and well into the future.

All Cogent AFIS product improvements ensure full backward compatibility with systems previously delivered. Our standard configuration mechanisms also enable the introduction of new features without impacting existing baselines. This ensures that no customer is left behind - our guarantee to each customer.

COGENT  SYSTEMS

Beyond Comparison

SA-4



Cogent's SA-4 SecurARM™ OEM Module is an image processing and matching unit designed specifically for OEM devices requiring highly secure biometric authentication and identification. Powered by Cogent's proprietary SecurARM microprocessor, the SA-4 also features Cogent's two-dimensional D2SP engine and an ARM940 32-bit microprocessor core – both on a single ASIC chip.

The SA-4 OEM Module is equipped with a 500-DPI silicon fingerprint sensor and two RS232 ports. These ports can be used to communicate with the PC host or can be connected to magnetic stripe, contact or contactless smart card readers. Because the SA-4 has built in commands to deal with industry standard smart card technology, there is no need for additional components to deal with communication needs.

The SA-4 offers both 1:1 authentication and 1: N identification applications giving customers biometric matching options never before available. Application host systems can manage the OEM module using our standard communication protocol. To achieve maximum security, the module provides an optional 3DES encryption and decryption algorithm for data transmission between the module and host PC. Additionally, the SA-4 provides support for standalone and match-on-card applications.

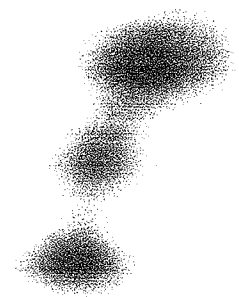
Beyond Comparison

Beyond Comparison



SA-4 Technical Specifications

Fingerprint Sensor	Silicon Sensor (500 DPI)
Enrollment Method	Single Finger, Multi-Touch Enrollment
Extraction & Verification Time	~ 1 Second
FRR	FRR = .1% - .001%
FAR	FAR = .01% - .0001%
Security Level	Configurable
Allowable Finger Rotation	+/- 15% For 1: N +/- 180° For 1:1
Template Storage	1,200 2MB; 9,000 + 8MB Flash
Data Encryption	3DES (Optional)
Search Speed	Up To 500 Templates Per Second
Image Data Compression	JPEG Compression Ratio: ~ 8:1
WSQ Compression Ratio	~ 15:1
I/O Interface	Two RS 232 Ports
RS232 Baud Rate	9600 To 115 Kbps Programmable
Memory	2MB Flash, 8MB SDRAM
Power	5.0 – 9.0 VDC, 300mA Regulated
Operating Temperature	0° to 55° C (32° - 131° F)
Dimension (L x W x H)	2.2" x 1.4" x 0.3" (55.0mm x 36.1mm x 7.6mm)
Software Options	OEM Development Kit



COGENT  SYSTEMS®

PMA

Programmable Matching Accelerator

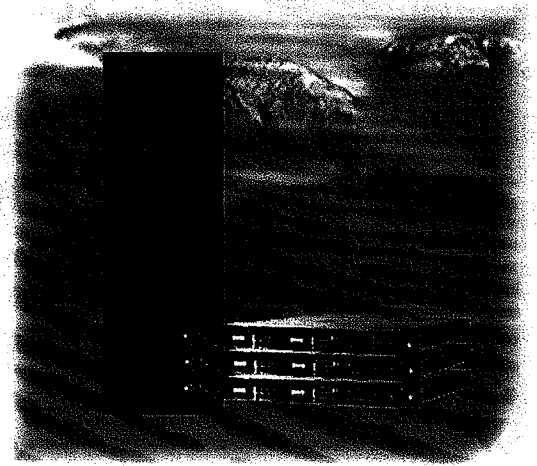
Cogent's **Programmable Matching Accelerator (PMA)** product line leads the industry in high-speed, high-accuracy finger and palm print matching. Based on an advanced "Super Pipeline, Super Parallel" design architecture and a new generation of field-programmable gate arrays, the PMA is quickly becoming the industry standard for AFIS matching.

Cogent's PMAs are the first commercially available fingerprint comparison servers based on advanced data flow computing. PMAs can support real-time identification – supporting applications that require searching databases of tens of millions of subjects in seconds.

The PMA product line is successfully being used by law enforcement and civilian agencies around the world. Providing 99.9% accuracy, the PMA architecture is the leader in identification accuracy. The PMA's COTS approach and modular design, combined with its "on demand" architecture, provides customers with improved reliability, increased availability, and lower total cost of ownership.

Scalability:

PMAs can be combined in modular units that are linearly scaled to handle databases of tens of millions of fingerprint records with response times of seconds. Utilizing Field Programmable Gate Arrays, the PMA subsystem can be programmed to perform a variety of matching tasks for fingerprints, palm prints, facial images, and other biometric identifiers. The linear scalability of the PMA subsystem architecture can accommodate almost any database size and response time requirement. Additional PMAs can be configured to upgrade systems that must meet evolving needs for larger databases while maintaining or increasing system throughput.



The Outstanding Matching Engine

Investment Protection

Featuring a mirrored hardware architecture, the PMA provides both data and hardware fault tolerance. With an "active-active" processor configuration, the PMA subsystem dynamically optimizes throughput performance should a failure occur. A PMA subsystem can easily be upgraded with Cogent's latest biometric matching technology to support growth, expansion, new technology insertion, and ensure investment protection. From the first generation PMA operating at 15,000 matches per second to those today operating at over 1,000,000 matches per second, Cogent's PMA architecture provides investment protection for the long term as your mission critical and operational needs dictate.

Flexibility

The PMA product line also affords redundancy and flexibility. The matching technology for the PMA subsystems features a multi-level comparison-elimination with multiple matching stages that are field-proven to deliver the highest levels of accuracy in the industry, as demonstrated by independent benchmark results.

Benefits:

- Linearly scalable, capacity can be added "on demand"
- Highest performance and accuracy for real-time identification
- Super-Pipeline architecture for speed
- COTS approach for lower ongoing cost
- Configurable software can meet various matching needs
- Redundant components for greater system availability
- Lower total cost of ownership
- Field programmable logic for investment protection
- Compact system footprint

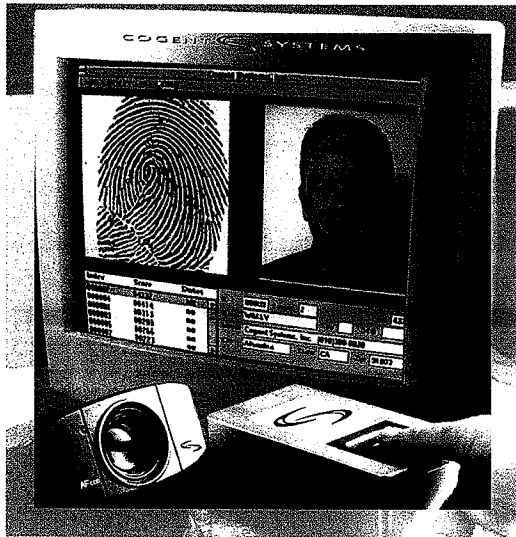
COGENT  SYSTEMS

Beyond Comparison

LiveID

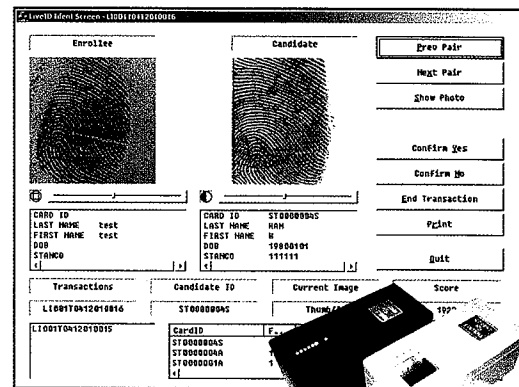
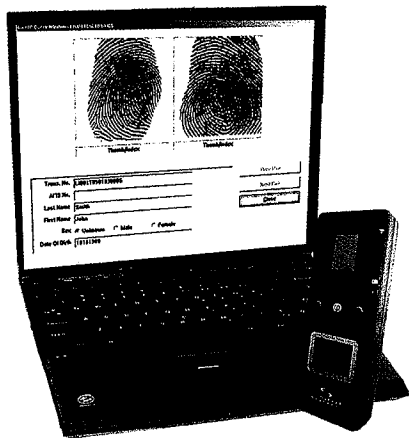
Real-Time Identification Solution

LiveID provides identity solutions for: identity authentication, securing borders, quick background checks, fraud prevention, and more. Cogent LiveID solutions provide easy-to-use systems for real-time identification where fast, positive identification of an individual is required. For government and civil sectors, LiveID is used to establish identity for people who apply for passports, driver licenses, voter registration, and for other identity document verification. Immigration control agencies use LiveID for border control identification checks. Criminal justice agencies use LiveID for the rapid identification of criminal suspects and jail management.



How LiveID Works

Cogent's LiveID provides a fast, practical method for searching and enrolling people into a database. Fingerprints are captured electronically, which means no ink, no mess, and no requirement for fingerprint expertise. Digital photographs, signatures, and demographic data can also be captured and stored. Cogent's data flow matching technology enables LiveID to accurately search entire databases ranging from a few records to millions of records in a matter of seconds. Our image fusion technology makes it possible to combine identification systems.



COGENT  SYSTEMS

Field-Proven Identity Solution

Scalable Solutions From Handheld Devices to Nationwide Networks

A LiveID system can be configured to run on handheld devices, notebook computers, stand-alone workstations, and enterprise systems serving users at thousands of sites. Systems can be implemented on platforms operating under UNIX®, Windows®, and Linux®, allowing users to submit search transactions and receive results with a standard web browser. Cogent delivered the first large-scale fingerprint identification system incorporating web technology. Cogent solutions feature the latest in data encryption and computer security techniques to protect identity information.

Cost-Effective Outsourcing Solutions for Real-Time Identification and Authentication

In addition to providing customers with turnkey LiveID solutions, Cogent also provides a fully outsourced LiveID service. Cogent works with customers to tailor solutions to their needs. Systems are housed and maintained in a secure data center at Cogent's headquarters. The data center is equipped with high-speed, fault-tolerant Cogent Programmable Matching Accelerators (PMAs) and enterprise servers that make it possible to meet each customer's specific requirements for application services, response times, and database sizing, even when a system requires processing speeds of millions of matching transactions per second and databases of millions of records.

Using LiveID to Meet Mission-Critical Business Needs

Cogent's proven image flow, data flow, and information fusion technologies have paved the way for accurate, cost-effective, and rapid identification systems that meet a wide range of needs.

In Venezuela, Cogent implemented a nationwide, fingerprint-based voter identification system to prevent voters from voting more than once. LiveID was deployed to 3,000 locations in Venezuela and relied on to submit more than 5 million fingerprint records for real-time searches in a single day.

In Ohio, an award-winning LiveID system allows over 550 schools, day care centers, hospitals, nursing homes, and other employers to perform criminal history background checks on employees via the Internet.

The Department of Homeland Security uses LiveID at over 500 border crossing points to determine if individuals apprehended illegally entering the U.S. have done so before or have been deported for criminal activity.

In Guatemala, in what the United Nations has called a "model operation," LiveID prevents applicants from obtaining driver's licenses under more than one name.



COGENT  SYSTEMS

Beyond Comparison

Cogent Systems, Inc.

209 Fair Oaks Avenue, South Pasadena, CA 91030 USA

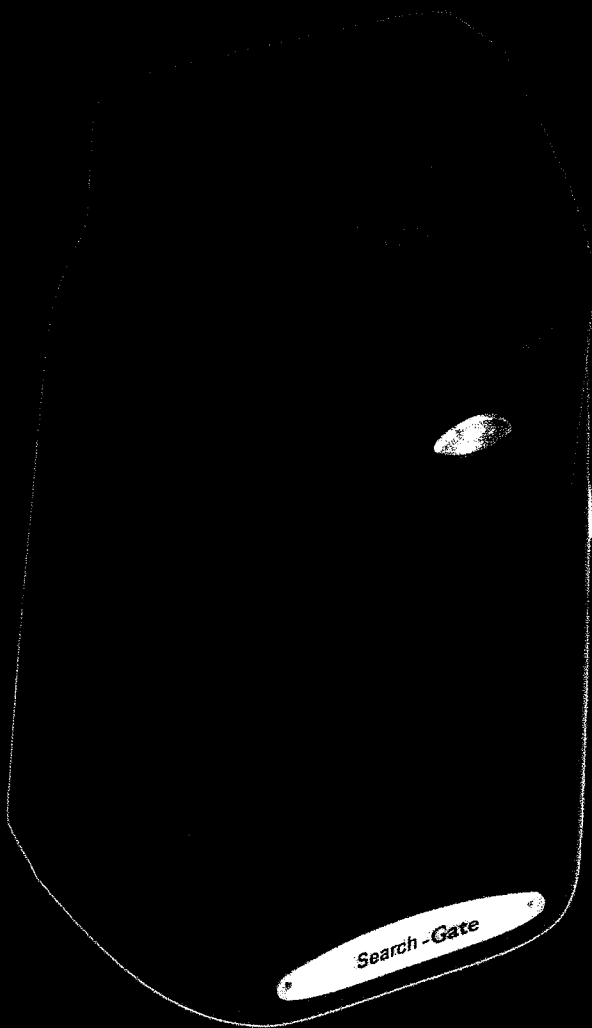
Tel: +1 626 799 8090 Fax: +1 626 799 8996

www.cogentsystems.com email: Info@cogentsystems.com



COGENT  SYSTEMS

Search-Gate™



Cogent's Search-Gate is a state-of-the-art biometric access control device supporting a wide variety of installations.

Powered by Cogent's SecurASIC chip and preeminent matching algorithm (as determined by the National Institute of Standards and Technology), Search-Gate provides the highest level of performance and accuracy available.

Search-Gate stores up to 1,200 fingerprint templates on the device and is capable of searching all 1,200 templates at a rate of 500 templates per second.

With Power over Ethernet capability and customizable Wiegand formats, biometric access control has never been easier.

Customizable Wiegand Setup

SecurSetup Administration Software

Power over Ethernet

Available in Rugged Aluminum Housing

Tokenless Biometric Access Control

Beyond Comparison

Beyond Comparison

Search-Gate Technical Specifications

Fingerprint Sensor	Silicon sensor (500 dpi)
Enrollment Method	Single finger, multiple enrollments
Extraction & ID Time	~1.5 seconds
FRR	FRR 0.1 % - 0.001%
FAR	FAR 0.01 % - 0.0001%
Security Level	Configurable
Allowable Finger Rotation	+/- 15°
Template Size	784 bytes
Template Storage	1,200 templates
I/O Interface	RS232, RS485
Baud Rate	9600 - 115 Kbps programmable
Ethernet	10/100
MIFARE® Cards	14443 A
Display	Customizable LCD display (16 Chars, 2 Lines)
Wiegand I/O	Programmable up to 128 bits
DC Power	6 - 12V DC standard input (12 - 48V DC jumper setup)
Power over Ethernet (PoE)	Fully 802.3af compliant, 12~60V DC (jumper setting) for Non 802.3af standard
Current	Standby: 200 ma @ 12V Operational: 280 ma @ 12V
Operating Temperature	0° to 55° C (32° to 131° F)
Physical Dimensions	(W) 3.14 in X (H) 5.42 in X (D) 2.28 in (W) 79.7 mm X (H) 137.7 mm X (D) 57.9 mm
Weight	0.9 ounces (0.3 kg)

COGENT  SYSTEMS

Cogent Systems, Inc. 209 Fair Oaks Avenue, South Pasadena, CA 91030 USA

Tel: +1 626 799 8090 Fax: +1 626 799 8996

www.cogentsystems.com email: BioGateInfo@cogentsystems.com

EXHIBIT 2

Fingerprint Retrieval Systems Providers

Producer	Headquarters	Plant Locations
123 ID, Inc.	Grand Forks, ND	Grand Forks, ND
Antheus Technology, Inc.	Boca Raton, FL	Boca Raton, FL
Avalon Biometrics* (Semantic System AG)	Madrid, SPAIN	*System integrator
Avalon Photonics	Zurich, SWITZERLAND	Switzerland
Beijing HanWang Technology Co., Ltd.	China	Beijing, CHINA
Bioscrypt	Markham, Ontario CANADA	El Segundo, CA; Buckinghamshire, UK
Changsha XingTong technology development Co., Ltd.	China	
Cogent Systems, Inc.	South Pasadena, CA	Dublin, OH; Reston, VA; Vienna, AUSTRIA; London, UK; Shenzhen, CHINA
Dermalog*	Hamburg, GERMANY	Hamburg, GERMANY; Kuala Lumpur, MALAYSIA *Have an MOU in India – no plant/office yet, however.
DATAMICRO Co., Ltd.	Taganrog, RUSSIA	Taganrog, RUSSIA
Futronic Technology Company Limited	Hong Kong, CHINA	Hong Kong, CHINA
Gevarius	Moscow, RUSSIA	Moscow, RUSSIA
Griaule	Sao Paulo, BRAZIL	San Jose, CA; Sao Paulo, BRAZIL
Eastern Golden Finger Systems	China	China
Integral Systems, Inc.	Lanham, MD	Colorado Springs, CO; El Segundo, CA; Toulouse, FRANCE
IDENCOM Germany GmbH	Berlin, GERMANY	Berlin, GERMANY; Zurich, SWITZERLAND
Identix	Minnetonka, MN	Jersey City, NJ; Ontario, CA; Miami, FL; Fairfax, VA; Springfield, IL; Wiltshire, UK; Sydney, AUSTRALIA
Miaxis Biometrics Co., Ltd	Shanghai, CHINA	Shanghai, CHINA

Producer	Headquarters	Plant Locations
Morphosoric	Brandenburg, GERMANY	Brandenburg, GERMANY
Motorola (under Government Solutions – Biometrics)	Schaumburg, IL	Research Center – Shanghai, CHINA
NEC Solutions (America), Inc., a subsidiary of NEC Corporation (Japan)	Irving, TX	Burbank, CA; Rancho Cordova, CA; Santa Clara, CA; Itasca, IL; Herndon, VA; New York, NY; Melville, NY – also have several worldwide locations
Neurotechnologija Ltd.	Vilnius, LITHUANIA	Vilnius, LITHUANIA
NITGEN Co., Ltd.	AnYang city, Gyunggi-do, KOREA	Seoul, KOREA
Nyoun	Korea	
The Phoenix Group, Inc.*	Pittsburg, KS	*Is now AFIX Technologies, Inc. – see website www.afix.net .
Raytheon (under Raytheon Biometrics C3IS)	Waltham, MA	Garland, TX
SAGEM Morpho, Inc., a subsidiary of SAGEM SA and SAFRAN Group (France)	Tacoma, WA	Alexandria, VA; Albany, NY; Austin, TX
Sonda	Miass, RUSSIA	Miass, RUSSIA
Suprema Inc.	Seongnam, SOUTH KOREA	Seongnam, SOUTH KOREA
Technoimagia Co., Ltd.	Allison Park/Pittsburgh, PA	Tokyo, JAPAN
Testech Inc.	Cheonan-Shi Chungchongnam-Do, KOREA	Have 2 research labs in South Korea – Hwaseong-shi, Gyeonggi-do, Korea

EXHIBIT 3

Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report

Summary of Results

NISTIR 7123

Charles Wilson ¹

R. Austin Hicklin ²

Mike Bone ³

Harold Korves ²

Patrick Grother ¹

Bradford Ulery ²

Ross Micheals ¹

Melissa Zoepfl ²

Steve Otto ¹

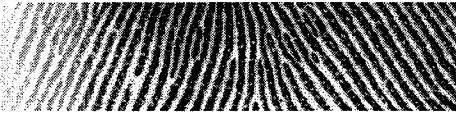
Craig Watson ¹

¹ National Institute of Standards and Technology

² Mitretek Systems

³ NAVSEA Crane Division

June 2004



FINGERPRINT VENDOR TECHNOLOGY EVALUATION 2003

SUMMARY OF RESULTS

Charles Wilson¹

R. Austin Hicklin²

Mike Bone³

Harold Korves²

Patrick Grother¹

Bradford Ulery²

Ross Micheals¹

Melissa Zoepfl²

Steve Otto¹

Craig Watson¹

¹National Institute of Standards and Technology

²Mitretek Systems

³NAVSEA Crane Division

Abstract

The Fingerprint Vendor Technology Evaluation (FpVTE) 2003 was conducted to evaluate the accuracy of fingerprint matching, identification, and verification systems. The FpVTE is one of the tests that NIST has conducted in order to fulfill part of its PATRIOT Act mandate. Additional evaluations include the testing of the FBI IAFIS system, the US-VISIT IDENT system and SDKs (Software Development Kits) from several vendors. Eighteen different companies competed in FpVTE, and 34 systems were evaluated. Different subtests measured accuracy for various numbers and types of fingerprints, using operational fingerprint data from a variety of U.S. Government sources. The most accurate systems were found to have consistently very low error rates across a variety of data sets. The variables that had the clearest effect on system accuracy were the number of fingers used and fingerprint quality. An increased number of fingers resulted in higher accuracy: the accuracy of searches using four or more fingers was better than the accuracy of two-finger searches, which was better than the accuracy of single-finger searches. The test also shows that the most accurate fingerprint systems are more accurate than the most accurate facial recognition systems, even when comparing the performance of operational quality single fingerprints to high-quality face images.

1 Introduction

1.1. Overview

The Fingerprint Vendor Technology Evaluation (FpVTE) 2003 was conducted to evaluate the accuracy of fingerprint matching, identification, and verification systems. FpVTE 2003 was conducted by the National Institute of Standards & Technology (NIST) on behalf of the Justice Management Division (JMD) of the U.S. Department of Justice. FpVTE 2003 serves as part of the NIST statutory mandate under section 403(c) of the USA PATRIOT Act to certify biometric technologies that may be used in the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program.

FpVTE 2003 was conducted at the NIST Gaithersburg, MD facilities from October through November 2003. Planning for FpVTE started in May 2003, and analysis continued through April 2004. Eighteen different companies participated, with 34 systems tested, including the NIST Verification Test Bed fingerprint benchmark system. Each test had a time limit of two or three weeks, running continuously. It is believed that FpVTE 2003 was the most comprehensive evaluation of fingerprint matching systems ever executed, particularly in terms of the number and variety of systems and fingerprints.

Participants in the FpVTE 2003 test were required to assemble, configure, and run their own hardware and software at NIST's Gaithersburg, Maryland facility. The trials began in October 2003, with each participant running over a two- or three-week period according to a predetermined and staggered schedule. Testing of all eighteen different companies was completed in November 2003.

FpVTE 2003 included operational fingerprint data from a variety of U.S. and State Government sources. The test used 48,105 sets of flat slap or rolled fingerprint sets from 25,309 individuals, with a total of 393,370 distinct fingerprint images.

The FpVTE Analysis Report concludes:

1. Of the systems tested, NEC, SAGEM, and Cogent produced the most accurate results.
2. These systems performed consistently well over a variety of image types and data sources
3. These systems produced matching accuracy results that were substantially different than the rest of the systems
4. The variables that had the largest effect on system accuracy were the number of fingers used and fingerprint quality:
 - Additional fingers greatly improve accuracy
 - Poor quality fingerprints greatly reduce accuracy
5. Capture devices alone do not determine fingerprint quality
6. Accuracy can vary dramatically based on the type of data:
 - Accuracy on controlled data was significantly higher than accuracy on operational data
 - A biometric evaluation that only uses a single type of data is limited in how it can measure or compare systems
7. Incorrect mating information is a pervasive problem for operational systems as well as evaluations, and limits the effective system accuracy
8. With current technology, the most accurate fingerprint systems are far more accurate than the most accurate face recognition systems.

1.2 Purpose

The evaluations were conducted to:

- Measure the accuracy of fingerprint matching, identification, and verification systems using operational fingerprint data
- Identify the most accurate fingerprint matching systems
- Determine the effect of a wide variety of variables on matcher accuracy
- Develop well-vetted sets of operational data from a variety of sources for use in future research

The evaluations were *not* intended:

- To measure system throughput or speed
- To evaluate scanners or other acquisition devices
- To directly measure performance against very large databases
- To take cost into consideration
- To address latent fingerprint identification

1.3 Certification

For purpose of NIST PATRIOT Act certification this test certifies the accuracy of the participating systems on the datasets used in the test. This evaluation does not certify that any of the systems tested meet the requirements of any specific government application. This would require that factors not included in this test such as image quality, dataset size, cost, and required response time be included. Certifications of deployed government systems such as the FBI's IAFIS and US-VISIT's IDENT system are covered by references [ATB] and [IDENT].

1.4 Personnel

A number of people had roles in FpVTE. Table 1 gives the name, affiliations and role of the staff that designed and executed the test.

Manager	Charles Wilson	NIST
FpVTE Liaison	Steven Otto	NIST
Lead Test Agent	Mike Bone	NAVSEA Crane Division
Test Design and Analysis Team	Austin Hicklin	
	Harold Korves	Mitretek Systems
	Brad Ulery	
	Melissa Zoepfl	
	Patrick Grother	
	Ross Micheals	NIST
	Craig Watson	

Table 1: FpVTE Personnel

2 Related Studies

NIST has or will release three related reports that provide additional information related to PATRIOT ACT certification of fingerprint systems.

2.1 Algorithmic Test Bed (ATB) Testing

NIST recently conducted a series of fingerprint matching studies using an experimental laboratory system called the Algorithmic Test Bed (ATB). The NIST ATB system is a lower capacity version of the FBI's Integrated Automated Fingerprint Identification System (IAFIS) and is being used to test the functional characteristics of IAFIS. The machine is configured with a gallery of nearly 1.2 million subjects and provides broad control over its operating modes and set points.

A NIST report on these studies [ATB] was published in April 2004. The FpVTE study includes aspects of the ATB studies – that address the matching of plain to rolled, and plain to plain, fingerprint images

2.2 Software Development Kit (SDK) Testing

NIST has conducted a series of SDK (Software Development Kit) based verification tests intended to evaluate the accuracy of the one-to-one matcher used in the US-VISIT program. Fingerprint matching systems from six vendors not currently used in US-VISIT were also evaluated to allow benchmark comparisons of the current VISIT matcher with other commercially available products. Each SDK based verifier was tested using twelve different fingerprint data sets of varying difficulty. Each set consisted of 12,000 single-finger images from 6,000 persons.

The average measured true accept rate at a false accept rate of 0.01% exceeded 98% for the two highest scoring systems with the worst always greater than 94%. The findings of the SDK tests, including documentation of the data sets and testing procedures, are detailed in a separate report [SDK].

2.3 US-VISIT IDENT Testing

A third NIST study addressed the flat-to-flat matching performance of the operational US-VISIT fingerprint matching system. Different subsystems of IDENT perform both one-to-many matches (to detect duplicate visa enrollments) and one-to-one matches (to verify the identity of visa holders). With the proper selection of an operating point, the one-to-many true accept rate for a two-finger comparison against a database of 6,000,000 subjects is 95% with a false accept rate of 0.08%. Using two fingers, the one-to-one matching accuracy is 99.5% with a false accept rate of 0.1%.

A NIST report on this test [IDENT] was published in May 2004

3 Comparison of Face and Fingerprints

The report that was sent to Congress [303a] as part of NIST's PATRIOT Act mandate [PATRIOT, BorderSecurity] included a comparison of face recognition results from the FRVT 2002 study [FRVT2002] with single-finger results from the NIST VTB fingerprint system [VTB]. The conclusions of that report should be updated in light of NIST's recent findings that the VTB fingerprint matcher is substantially less accurate than the best commercial systems, and because the DHS2 data used for the 303a report were the poorest quality in any datasets used in FpVTE. In addition, although the images used in the FRVT 2002 test are of higher quality than many of those present in operational government data sets, they all fall short of the specifications of the draft Face Image standard [ISO/IEC].

Leading contemporary fingerprint systems are substantially more accurate than the face recognition systems tested in FRVT 2002. When all these factors are combined, the comparison of face and fingerprint accuracy needs to be revised. This conclusion holds even for face and fingerprint images categorized as high quality, however, it must also be considered that any advances in face recognition technology since the FRVT tests have yet to be evaluated. Further performance benefits associated with data collected to comply with ISO/IEC 19794-5 also remain unquantified.

The following entries summarize the verification performance documented in FpVTE 2003 and FRVT 2002. The most accurate face systems:

- 71.5% true accept rate @ 0.01% false accept rate
- 90.3% true accept rate @ 1.0% false accept rate.

The most accurate fingerprint system tested (NEC MST) using operational quality single fingerprints:

- 99.4% true accept rate @ 0.01% false accept rate
- 99.9% true accept rate @ 1.0% false accept rate

When multiple face images are available, the performance of face recognition can be improved [Grother3]. With four previous images in the gallery the error rates are substantially reduced

- 89.6% true accept rate @ 0.01% false accept rate
- 97.5% true accept rate @ 1.0% false accept rate

In FpVTE 2003, when four fingerprints were used for matching, the most accurate fingerprint system tested (NEC LST) always had true accept rates in excess of 99.9% at a FAR of 0.01%.

4 Overview of Tests

FpVTE was composed of three separate tests, the Large-Scale Test (LST) the Medium-Scale Test (MST), and the Small-Scale Test (SST). Table 2 compares parameters associated with each of the three tests.

SST and MST tested matching accuracy using individual fingerprints, all of which were images from right index fingers. This contrasts with LST, which evaluated matching accuracy using sets of fingerprint images, where each set includes anywhere from one to ten fingerprints collected from an individual subject at one session. The tests were designed so that the SST is a subset of the MST. As a consequence, this allows direct comparison of SST and MST Participants. LST Participants were encouraged to participate in the MST.¹

Participants were permitted to enter more than one system in the evaluation.

¹ Eleven of the thirteen LST participants had valid MST results, but some of those had different system configurations in MST and LST.

Test	Compares	# Subtests	# Comparisons	# Systems Successfully Completed	Allowed Time
LST	Sets of 1-10 fingerprint images (Flat, Slap, and Rolled; various combinations of fingers)	31 (uses 10 datasets containing 64,000 fingerprint sets)	1.044 billion set-to-set comparisons	13	21 days
MST	Single images (Flat & Slap Right index)	1 (compares a single 10,000 image dataset against itself)	100 million single image comparisons	18	14 days
SST ²	Single images (Flat Right index) (Subset of MST)	1 (compares a single 1,000 image dataset against itself)	1 million single image comparisons	3 (SST only) 21 (as a subset of MST)	14 days

Table 2. Summary of FpVTE Tests

The size and structure of each test were designed to optimize competing analysis objectives, available data, available resources, the Participants' responses to the *System Throughput Questionnaire* (see Appendix A), and the desire to include all qualified Participants.

In particular, the sizes of MST and LST were only determined after a great deal of analysis and consideration of a variety of issues. The systems in FpVTE differed in several significant ways, for example:

- maximum throughput capacity
- the relative proportion of time spent preprocessing images and matching images
- the ability to increase throughput rates by decreasing accuracy
- the ability to increase throughput by adding additional hardware.

Designing a well-balanced test to accommodate heterogeneous system architectures was a significant challenge.

The timing analysis performed by NIST suggests that to increase the total number of comparisons made by a factor of ten (which would have been the smallest meaningful increase in measurement precision), the LST test duration would have had to increase from three weeks to *thirty* weeks. The alternative of using larger datasets and three weeks test time would have limited the test to those systems that could trade accuracy for throughput. Extending the length of the test would have placed a greater burden on the Participants for personnel and hardware. Increasing the throughput requirements without extending the length of the test would have favored one type of system, may have favored Participants with specialized hardware, and would have limited the number of participants. Although software development kit tests (see section 2.2) offer the possibility to run tests over many weeks or months, they do so by requiring vendors' applications to run on standard hardware and operating system combinations.

² Three systems competed in SST, but since SST was a subset of MST, all of the MST participants can be compared directly in SST. Hence 21 systems successfully completed this subtest.

5 Summary of Results

FpVTE analysis had three interrelated goals:

- To compare the competing systems on a variety of fingerprint data, identifying the systems that were most accurate;
- To measure the accuracy of fingerprint matching, identification, and verification systems on actual operational fingerprint data; and
- To determine the effect of a variety of variables on matcher accuracy.

As stated previously, the FpVTE analysis was not intended to take into consideration cost, throughput, equipment reliability or other factors that might be important in selecting a system for operational deployment.

5.1 Multi-Finger Performance (LST)

All of the LST systems achieved high accuracy on some of the data, especially in the ten-finger subtests. However, some of the LST systems were more consistent in their accuracy than others. Figure 1 shows the range of performance over 27 representative test partitions of operational fingerprint data. These partitions are discussed in the Analysis Report

Each line depicts a summary statistic for the systems' performance over the 27 partitions, characterizing the TAR accuracy as measured (or minimally interpolated) at FAR = 0.01%. For example, the line labeled "Average" shows for each system the average of 27 separate TAR measurements, each at FAR = 0.01%. The maximum accuracy for each system, also plotted on the graph, was quite high—100% accuracy or near-100% accuracy. Since maximum and minimum values are often outliers, the 5th highest and 5th lowest accuracies over the 27 partitions are also shown, to give a better indication of the spread of the data. Details of this subtest are discussed in Appendix D.

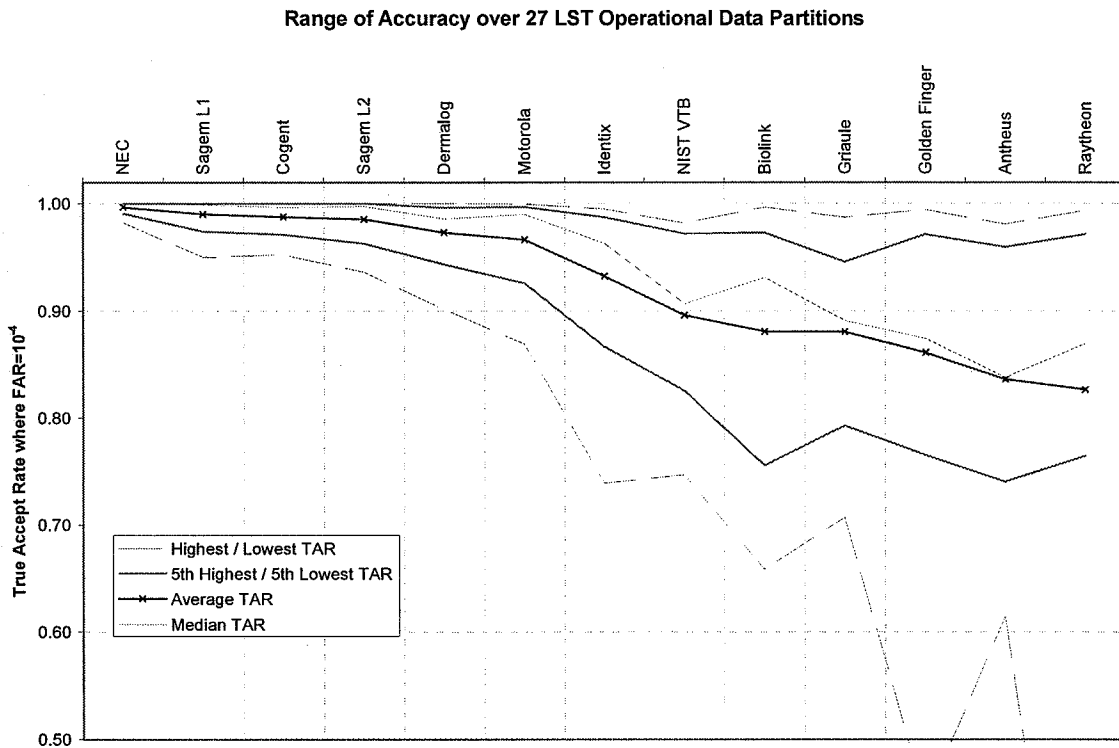


Figure 1. Range of Accuracy over 27 Operational LST Partitions. The systems are sorted by their average accuracy over the 27 partitions; note that sorting by median performance would change the order for some systems.

5.2 Single-Finger Flat and Slap Performance (MST)

In MST, the fingerprints were grouped by both source and type (as defined in the Analysis Report), yielding seven different combinations that were used to partition the data. The results for each participant for each partition were calculated and analyzed. The resulting range of accuracy on seven single-finger tests is shown in 3.

Since the highest and lowest true accept values are often outliers, the range between the second highest and second lowest is also shown. In the LST comparison, the highest TAR was often 100% with a minimal difference between the top several applicants. In MST, there was also a substantial difference between the highest and second highest values for many systems. For most systems, the highest value was achieved on the one partition that was collected under highly controlled conditions (Ohio dataset). The remaining six partitions contained only operational data, so the difference in the highest and second-highest scores are indicative of the difference between data collected via operational systems versus data collected under highly controlled conditions.

Details of this subtest are discussed in Appendix D.

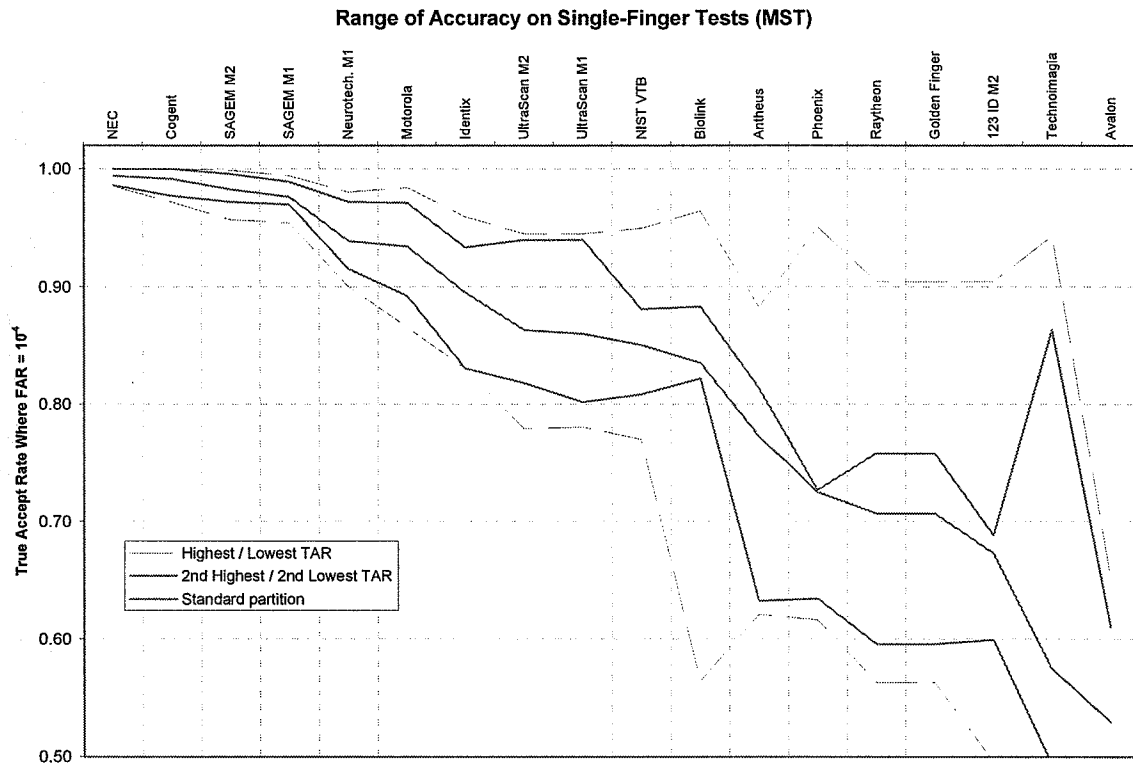


Figure 2. Range of accuracy across 7 MST partitions. These systems are sorted by the systems' performance on the standard MST, which is simply the combination of the seven partitions.³ The large difference between the highest and second highest TARs is attributable to the presence of data collected in a controlled (highest) versus operational (second highest) setting.

To facilitate comparison, all of the MST systems were ranked in order of TAR at a 0.01% FAR, for each of the seven partitions these systems are sorted by the average rank over all seven partitions.

5.3 Single-Finger Flat Performance (SST)

SST was a small test that included only a single type of data (single-finger flats), from two sources. SST was a subset of MST, so any SST partitions are (by definition) partitions of MST. The results for each SST and MST participant for each source were calculated and analyzed. The resulting range of accuracy is shown in 5. The SST systems are sorted by the systems' performance on the SST standard partition, which is simply a combination of the other two partitions.

³ Since the seven partitions differ in size, the results for the MST standard partition are not quite the same as the average of the seven partitions.

Due to the smaller size of the SST, these results are presented at a false accept rate of 0.1% and *not* 0.01% as is true for most of the other figures in this report.

Details of the SST are included in Appendix D.

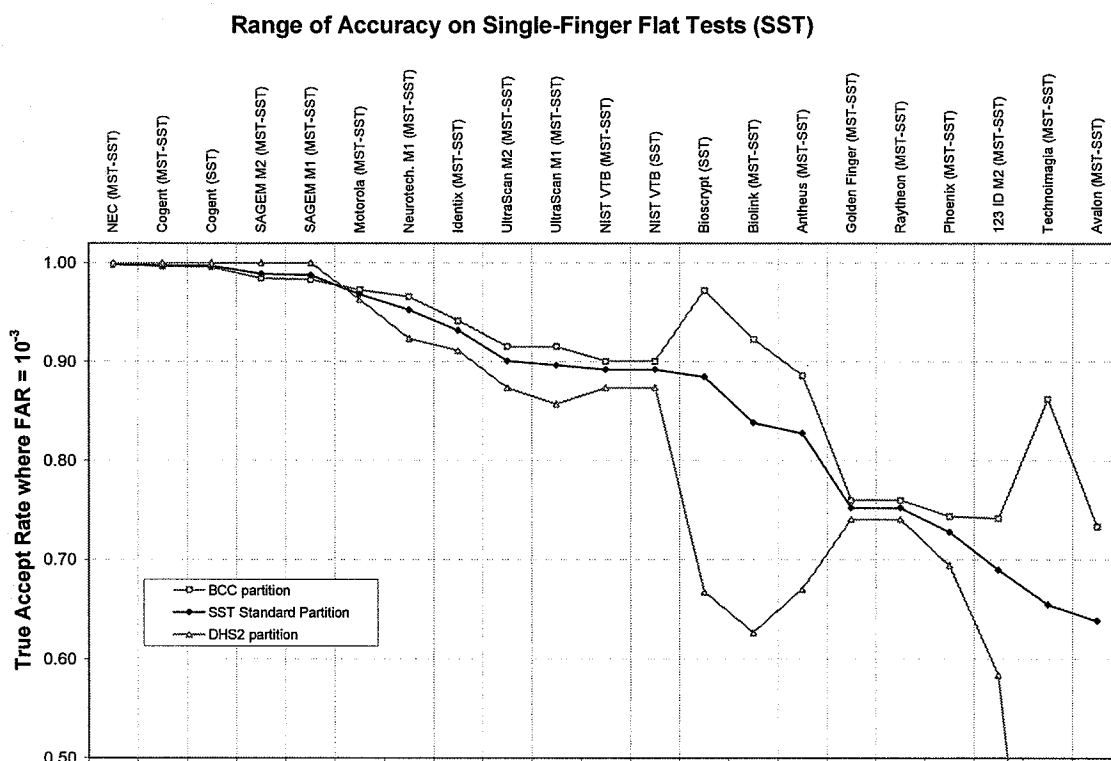


Figure 3. Range of Accuracy on Single-Finger Flats (SST). These systems are sorted by performance on the SST standard partition. Note that these results are reported at FAR=0.1%, in contrast to most of the figures in this report, which are based on FAR=0.01%.

5.4 Effect of Fingerprint Quality on Matcher Accuracy

It is well known that poor quality fingerprints are universally difficult to match. The effects of fingerprint quality are clear and dramatic, as shown in Figure : without exception, accuracy on good quality images was much higher than accuracy on poor quality images. This finding is important for several reasons:

- Operational procedures can be used to control fingerprint quality to a large extent;
- System designers can model the effect of different distributions of fingerprint quality on matcher accuracy to predict system cost and performance;
- Systems can use fingerprint quality to predict search reliability (low quality leads to false non-matches);
- The relevance of tests is limited if the distribution of fingerprint quality is not known in the test sets;
- The outcome of tests can vary significantly if fingerprint quality is not controlled.

Note that the sample sizes for the poorer quality images are very small, but the results are as expected and consistent across systems. Figure also shows that some systems are extremely sensitive to image quality.

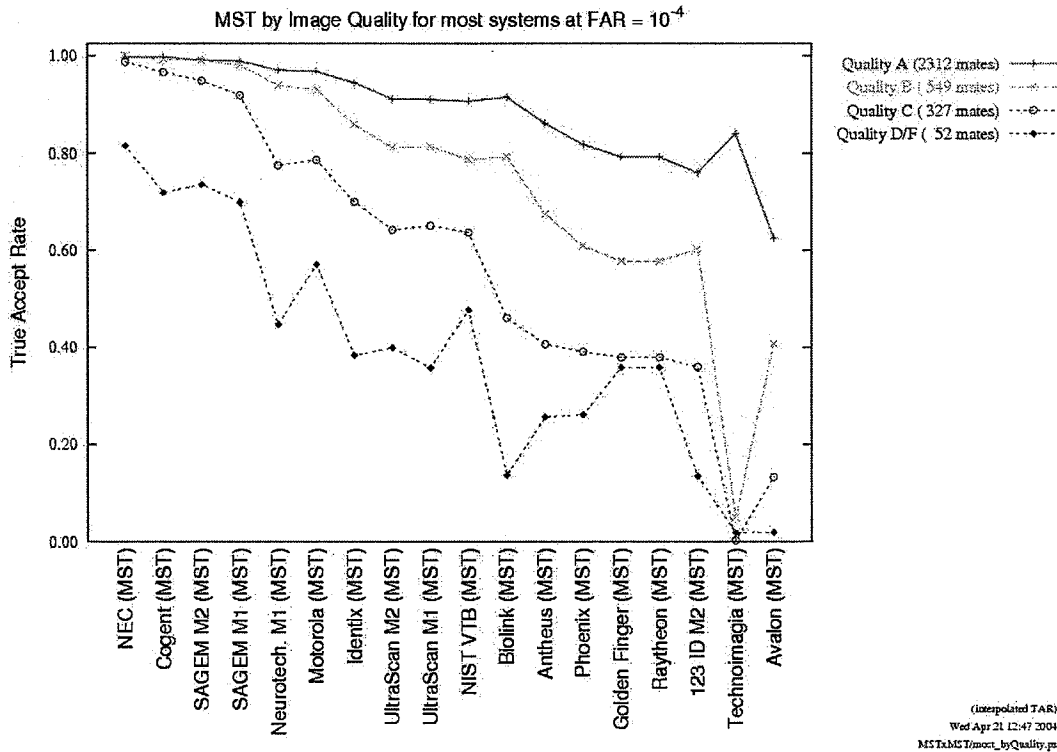


Figure 4. Effect of Image Quality (MST)

The image quality metrics used are discussed in Section 5.1 of the Analysis Report.

5.5 Effect of Number of Fingers

System accuracy was *highly* sensitive to the number of fingers compared. This can be seen clearly in Figure 4, which shows false reject rates at a fixed false accept rate of 0.01%. This figure compares different numbers of both plain and rolled fingerprints from both livescan and paper. Different colors are used to represent the number of fingers, while the letters denote rolled (R) and slap (S) fingerprints from paper (P) and livescan (L). Thus, the last aqua/grey curve as listed in the legend applies to the comparison of ten rolled paper prints with ten rolled paper prints (10RP vs. 10RP).

The error rates for each vendor typically vary by a factor of 100. The first vendor, NEC, falsely rejects 1 in 100 of the most difficult single fingers but fewer than one in ten thousand of the easiest ten finger sets. The last entry, Antheus, falsely rejects 40% of the hardest single fingerprints and 1% of the easiest multi-finger sets.

Figure 5 clearly shows that single finger matching is less accurate than two-finger matching, that two-finger matching is less accurate four-finger matching, and that four-finger matching is less accurate than eight-finger matching. The test sample size is not large enough to separate the eight and ten finger results. Thus the major conclusion from the figure is that each doubling of the number of fingers produces a fixed factor reduction in false rejection errors. For NEC, the error rates are 1% 1%, 0.2%, 0.05% and 0.01% for one, two, four and eight fingers respectively. Therefore, the errors reduce by approximately a factor of five as the number of fingers is doubled. Similar ratios of accuracy apply to the other vendors on the left side of the graph.

The figure also shows that there is great variability within the data for a given number of fingers. Much of this variability can be attributed to variations in data source, quality, and type.

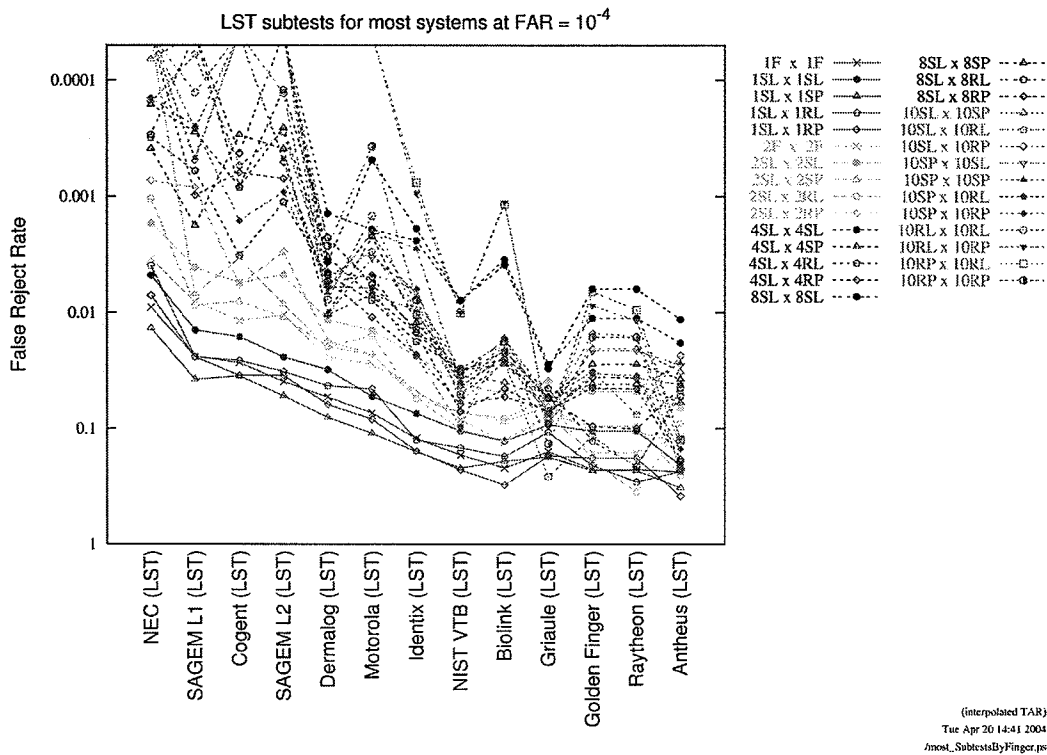


Figure 4. Effect of Fingerprint Number and Other Variables in LST. The Y scale is the log of False Reject Rate, which is 1 - TAR. Note that the single-finger searches (red) are clearly separated from the two-finger searches (green), but the four, eight, and ten-finger searches are intermingled. At the test sizes used, accuracy of four, eight, and ten-finger searches is difficult to differentiate and depends, to some extent, on the type of fingerprints used. The lines off of the top of the chart are for TAR=100% (no false rejects), which cannot be represented in log scale.

In order to minimize the effects of confounding variables, data source and image type were controlled in additional analyses. These analyses involved slap livescan probes compared to four different gallery types (slap livescan, slap paper, rolled livescan, and rolled paper), with data from four distinct sources. In general, the results showed that for most systems accuracy clearly improves as the number of fingers increases.

The following two charts show examples of the effect of number of fingers, where data source and type of fingerprint are held constant. Figure 5 shows results for the FBI's 12k⁴, slap livescan vs. rolled livescan data set, which most systems match with high accuracy. Note that for the more accurate systems the results provide no evidence that more fingers improve accuracy on a dataset such as this, because TAR is already at or near 100% for a single finger.

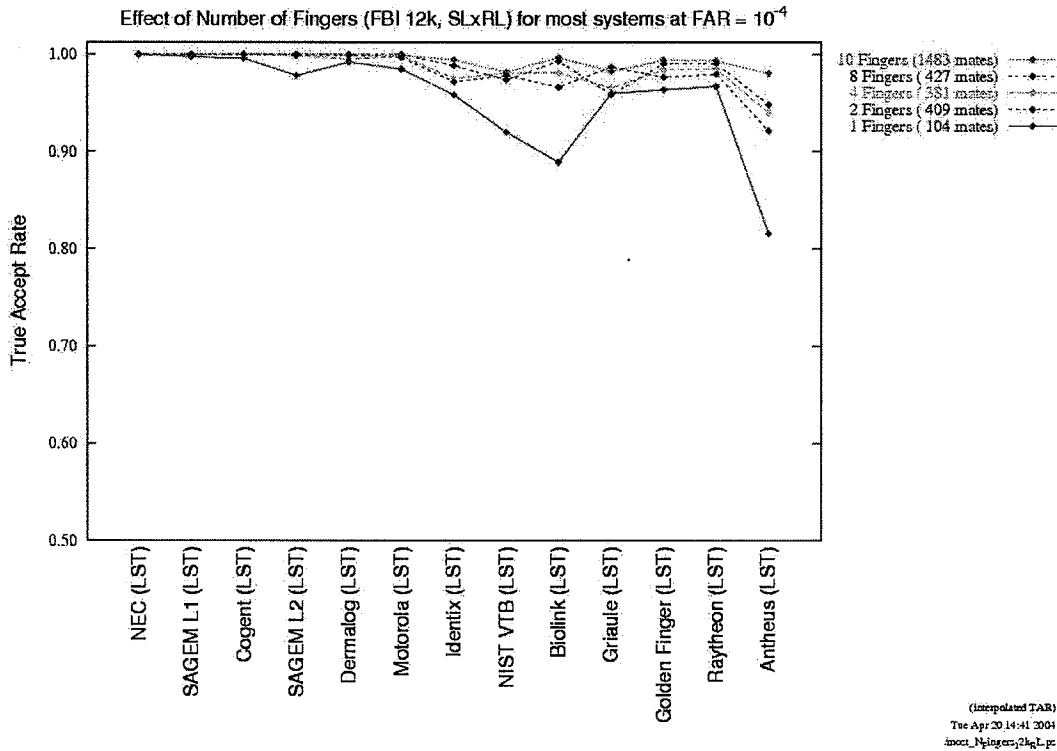


Figure 5. Effect of number of fingers on FBI 12k (slap livescan vs. rolled livescan). The effect is not measurable when the one-finger TAR approaches 100%.

⁴ The "FBI 12k" data is described in more detail in the analysis report, with others.

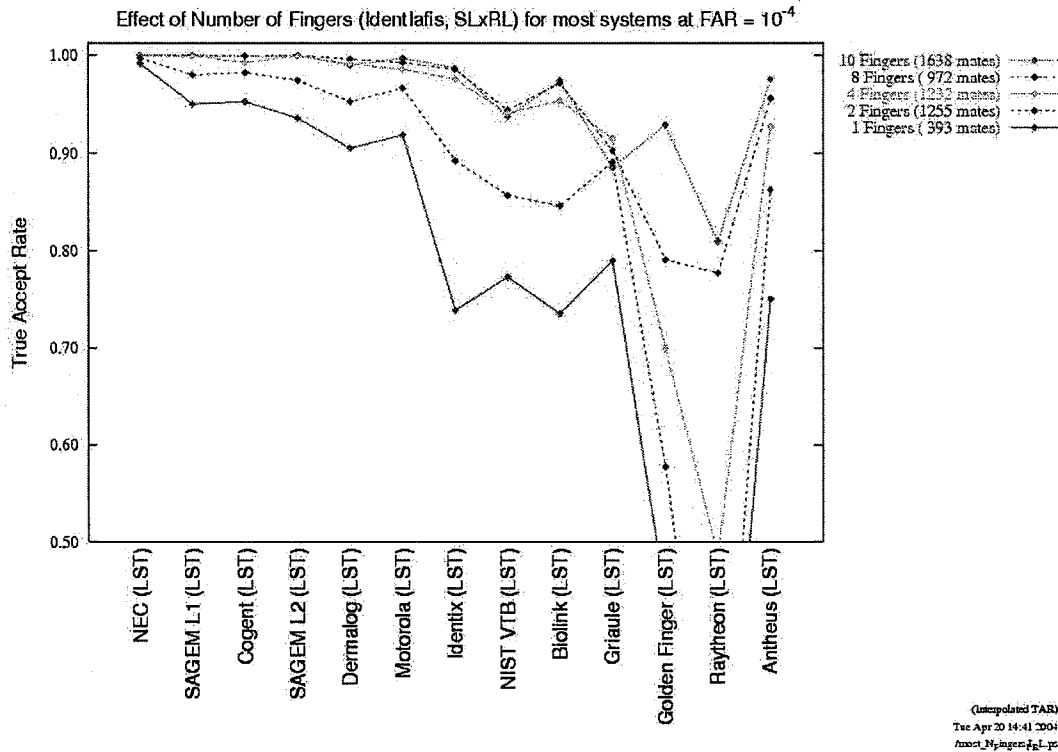


Figure 6. Effect of number of fingers on IDENT-IAFIS (slap livescan vs. rolled livescan). This data clearly shows the significant benefit when comparisons are done with more than two fingers.

Even for some of the more accurate systems, a difference in performance can be seen between two- and four-finger comparisons on the IDENT-IAFIS data (slap livescan vs. rolled livescan). Since NEC and SAGEM L1 achieved TARs of 100% with 4 fingers, they cannot be expected to differentiate at this level.

5.6 Other Results

Other important results discussed in the Analysis Report include:

- Accuracy on controlled data was significantly higher than accuracy on operational data.
- Some systems were highly sensitive to the sources or types of fingerprints, but this was not true of all systems.
- Accuracy dropped as subject age at time of capture increased, especially for subjects over 50 years of age. This effect may be due largely to image quality, which is known to vary by age.
- The choice of finger was not found to have a substantial effect on accuracy, except that segmented slap little fingers performed poorly.
- The following variables were not found to have a substantial effect on accuracy - gender, or criminal vs. civil records.

- In any operational government database, the performance attributable to source, fingerprint type (rolled, flat or slap images) and livescan vs. paper cannot be fully separated.

5.7 Implications for Operational Systems

When discussing the implications of the FpVTE results for operational systems, several issues need to be emphasized:

- Real world operational results for a system may be better or worse than the results reported here. Differences may arise from factors such as the operational environment, sources and types of fingerprint data, capture devices, operators and their training, hardware and software architecture and implementations, throughput requirements, and gallery size. One important conclusion of FpVTE is that such factors have a clear but complex effect on the performance of fingerprint systems.
- Operational systems are likely to use different operating points than are cited here, with correspondingly different error rates.
- Operational systems can be tuned to maximize performance given a particular concept of operations.
- Many systems have the ability to trade off accuracy for throughput: different throughput requirements will result in different levels of accuracy. Very high throughput requirements may be attained through a drop in accuracy.
- System cost, which was not addressed in FpVTE, must always be considered for operational systems.
- The error rates associated with slap segmentation were not addressed in FpVTE.

6 Conclusions

Overall, FpVTE makes six major conclusions regarding state-of-the-art, COTS and GOTS fingerprint systems.

1. The systems were that performed most accurately developed by NEC, SAGEM, and Cogent

In single and multi-finger tests (LST), NEC was the most accurate system (or tied for most accurate) in 42 out of 44 distinct combinations of data, including tests of mixed image type, and those from a variety of operational and controlled sources. The SAGEM and Cogent systems were the next most accurate LST systems.

In single-finger tests (MST), NEC was the most accurate system (or tied for most accurate) in 6 out of 7 distinct combinations of data, from both operational and controlled sources. The Cogent and SAGEM systems were the next most accurate MST systems.

Following the tier of the most accurate systems tested, the most accurate of the other systems tested were developed by Dermalog and Motorola, which had comparable performance.

Similarly, in the MST, the most accurate of the other systems were developed by Neurotechnologija and Motorola, which had comparable performance.

The SST results corresponded to the MST results.

2. The most accurate systems were highly accurate

On 44 test partitions defined by fingerprint type, number, and source, the most accurate LST system (NEC) was capable of identifying more than 98% of the mates in *every* subtest, with a false accept rate of 0.01%.

Given a false accept rate of 0.01% the results for NEC LST system showed that:

- Every single-finger subtest had a true accept rate higher than 98.6%
- Every two-finger subtest had a true accept rate higher than 99.6%
- Every four, eight, or ten-finger subtest had a true accept rate higher than 99.9%

SAGEM L1 and Cogent had true accept rates in excess of 95% on all single and multi-finger LST tests, at a false accept rate of 0.01%.

2a. The most accurate systems performed consistently well over a variety of image types and data sources

The most accurate systems maintained high accuracy even on data on which other systems performed with significantly less accuracy.

2b. There was a substantial difference in accuracy between the most accurate systems and the rest of the systems

The most accurate systems were more accurate than the rest of the systems for almost every metric examined.

On single-finger tests (MST and LST), accuracies below 80% were typical among the lower third (by rank) of participating systems. This corresponds to a False Reject Rate much more than ten times that of the high-accuracy systems. This ratio was even greater for multi-finger tests.

3. The variables that had the largest effect on system accuracy were the number of fingers used and fingerprint quality

3a. Additional fingers greatly improve accuracy

All systems achieve greater accuracy when multiple fingers are provided for comparison than when only one finger is provided. The improvement is both large and consistent. Although the actual benefits were found to vary by dataset and by system, the general trend was quite consistent. The accuracy of searches using four or more fingers was higher than the accuracy of two finger searches, which was higher than the accuracy of single-finger searches.

As a rough rule of thumb, at a fixed false accept rate the false reject rate was found to decrease by up to an order of magnitude when using two fingers rather than one, and again when using ten fingers rather than two. Actual differences varied by dataset and by system, but the general trend was quite consistent.

It should be acknowledged, however, that given accurate systems and a relatively limited number of images, a *precise* quantification of the benefit of using of four, eight, and ten-finger sets was not possible in FpVTE 2003. The utility of using an increased number of prints (four or more) is in suppressing false accepts when either a large one-to-many search is needed or when aggregate image quality is reduced.

3b. Poor quality fingerprints greatly reduce accuracy

For all systems, accuracy on high-quality images was much higher than accuracy on low-quality images. Some systems were particularly sensitive to low image quality. For example, at the standard false accept rate of 0.01% the Technomagia MST accuracy of 82% for the highest-quality fingerprints dropped to 2% for the lowest quality fingerprints⁵. NEC MST achieved an accuracy of 99.8% for the highest-quality fingerprints, which dropped to 84% for the lowest quality fingerprints.

4. Capture devices alone do not determine fingerprint quality

Different operational fingerprint sources can use the same type of collection hardware *and* software and yet result in substantially different performance. The State Department Border Crossing Card (BCC) data and the DHS Recidivist (DHS2) data used the same scanners and software, but are substantially different in overall quality. Using the FpVTE image-quality metric (see Analysis Report), 80% of BCC is high quality, but only 45% of DHS2. Consequently, for most systems, there is a clear difference in accuracy between the two datasets.

Therefore, the subject populations, collection environment, staff training, and equipment maintenance are some of the other factors that are believed to have a substantial impact on fingerprint quality.

5. Accuracy can vary dramatically based on the characteristics, or type, of the data

Performance on one type of data is not necessarily similar to performance on another type of data. The False Reject Rate (one minus the TAR) for a system often varied by a factor of two or more between different datasets.

Some systems showed an unusually high sensitivity to the sources or types of fingerprints; the most accurate systems did not. For example, in SST Cogent had a true accept rate of 99.6% for BCC data and 100% for DHS2, at a false accept rate of 0.1%. At the same false accept rate Bioscrypt had a true accept rate of 97.2% for BCC data and 66.8% for DHS2.

⁵ Quality D and F combined. Performing with near-zero errors on low quality prints may indicate a system has an effective mechanism for electing not process such images. If revealed such events are included in a failure to acquire rate. FpVTE ignores FTA by demanding systems return a result no matter what. This yields system level performance.

Any predictions of operational accuracy must account for this important source of variability. Projections from measurements on one type of data to operational performance on another type of data are questionable.

5a. Accuracy on controlled data was significantly higher than accuracy on operational data

All systems were more accurate on the controlled Ohio fingerprints, which were of distinctly higher quality than the operational fingerprints.

5b. Biometric evaluations that only use a single type of data are limited in how systems can be measured or compared

An evaluation that uses a single type of data can measure the accuracy only on that type of data, and may give a misleading impression of overall performance. Likewise, it is not safe to assume that operational performance will closely resemble performance on test data.

In addition, the relative performance of different systems varies by the type of data, so a comparison of systems using one type of data may be very different from a comparison using different data. Rank order among systems was sometimes sensitive to which dataset was selected for comparisons; for this reason, comparisons were based on an aggregate of results.

6. Incorrect mating information is a pervasive problem for operational systems as well as evaluations, and limits the effective system accuracy

The *effective* accuracy of a system is bounded by the mating error rate of the underlying ground truth data. Mating errors were found by trained examiners in every source used in FpVTE. The initial mating errors in most of the datasets used in this evaluation exceeded the matching error rates for the most accurate systems. These ground truth errors were corrected before formal scoring.

Minimizing mating errors in evaluation data is essential to correctly evaluating the accuracy of systems, especially at very low false accept rates or very high true accept rates.

For example, the number of consolidations (cases in which the same person has fingerprint sets under different names or IDs) found and removed in FpVTE was 0.49%. If these had not been found and corrected, then FAR could not have been measured below 0.5%.

References

- [303a] "Use of Technology Standards and Interoperable Databases with Machine-Readable, Tamper-Resistant Travel Documents – Appendix A," PDF document at <http://www.itl.nist.gov/iaui/894.03/fing/fing.html>; November 2002.
- [ATB] Stephen S. Wood and Charles L. Wilson, "Studies of Plain-to-Rolled Fingerprint Matching Using the NIST Algorithmic Test Bed (ATB)" NIST IR7112, April 2004; National Institute of Standards & Technology, Gaithersburg Maryland.
- [BorderSecurity] Public Law 107-173 (Enhanced Border Security and Visa Entry Reform Act of 2002); 107th United States Congress, Washington, D.C.; 14 May 2002.
- [FpVTE2003] C. Wilson, R. A. Hicklin, H. Korves, B. Ulery, M. Zoepfl, M. Bone, P. Grother, R. Micheals, S. Otto, C. Watson, Fingerprint Vendor Technology Evaluation 2003 Analysis Report.
- [FRVT2002] P. J. Phillips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and M. Bone, 'Face recognition vendor test 2002, NIST IR 6965, National Institute of Standards & Technology, Gaithersburg Maryland, March 2003
- [Grother] Patrick Grother, *Face Recognition Vendor Test 2002 Supplemental Report*. February 2004. NIST IR 7083.
- [IDENT] C. L. Wilson, M. D. Garris, and C. A. Watson, "Matching Performance for the US-VISIT IDENT System Using Flat Fingerprints," DRAFT NISTIR; National Institute of Standards & Technology, Gaithersburg Maryland.
- [PATRIOT] Public Law 107-56 (USA PATRIOT ACT); 107th United States Congress, Washington, D.C.; 26 October 2001.
- [SDK] Craig Watson, Charles Wilson, Karen Marshall, Mike Indovina, and Rob Snelick, "Studies of One-to-One Fingerprint Matching with Vendor SDK Matchers," DRAFT NISTIR; National Institute of Standards & Technology, Gaithersburg Maryland .
- [VTB] Wilson, Watson, Reedy, Hicklin. *Studies of Fingerprint Matching Using the NIST Verification Test Bed (VTB)*; NISTIR 7020; 7 July 2003.
(ftp://sequoyah.nist.gov/pub/nist_internal_reports/ir_7020.pdf).

EXHIBIT 4

Biometrics in China

— A National Activity Report

China National Body
ISO/IEC JTC 1/SC 37 Biometrics
London. July 10, 2006

China's Participation in SC37

- Joined SC37 in 2004
- Participated 2005 (South Africa)
- Participating 2006 (London)

Outline

- Biometrics in China
 - Background
 - R & D
 - Applications and Markets
- Standardization Efforts
 - Organization
 - Current Activities

Background

Nation's Facts (1)

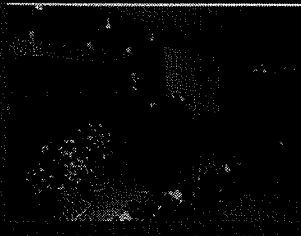
- Country of the largest population
 - Population 1.3B
 - Floating Population 140M
- Economy growth, rapid increase in the use of computer and Internet users
 - 100+ M Internet users
 - 4,500 billion USD e-bank transactions in 2005
- Government – Supportive
- Acceptance of biometric applications

Nation's Facts (2)

- Biometrics R&D started in early 1980s,
- Commercial systems appeared in 1993
- Industry: 200+ companies
- Academia: 100+ research teams
- R&D Areas: Face, iris, fingerprint, palmprint, hand, voice, gait, signature, vein, etc
- Compelling technologies developed

Biometrics Meetings in China

- Chinese Biometrics Forum since 2003
- Annual Sino-biometrics Conference since 2000 (merged to ICB since 2006)
- Asian Biometrics Forum, 2006



R & D

Leading R&D Teams

- Center for Biometrics and Security Research (CBSR)
Institute of Automation, Chinese Academy of Sciences (CASIA)
- Joint Research & Development Laboratory for Advanced Computer and Communication Technologies (JDL)
Institute of Computing Technology, Chinese Academy of Sciences (CASICT)
- Electric Engineering Dept, Tsinghua University
- Center for Information Research, Perking University
- Biometric Research Center, Hong Kong Polytechnic University
- Center of Forensic Sciences, Beijing Genomics Institute

Center for Biometrics and Security Research (CBSR)

Institute of Automation, Chinese Academy of Sciences (CASIA)

- Largest Biometrics Team in China
 - 10 Researchers, 3 Advisors, 30 Ph.D Students, 30 Master Students, 10 Engineers, 3 Admin Staff
 - Face, Iris, Fingerprint, Palmprint, Signature, Gait, Voice
- Advocate of Nation-wide Biometric Activities
- Biometrics Books:
 - Handbook of Face Recognition. S.Z. Li and A.K. Jain (Ed), Springer, 2005
 - Human Identification based on Gait. M. Nixon, T.N. Tan, R. Chellappa. Springer, 2005
 - Encyclopedia of Biometrics. Editor-in-Chief: S.Z. Li. Springer, 2008.
 - 250 A-Z entries, 1000 pages, covering all aspects of biometrics. XML version updated annually
 - "Harmonized Biometric Vocabulary" will be adopted as much as possible
 - Contributions of entries from SC37 participants are welcome

Advanced Technologies

- Face (Visible Light & Near Infrared)
 - CASIA
 - Institute of Computing Tech, CAS
 - Tsinghua University
- Fingerprint
 - CASIA
 - Peking University
 - Many Companies
- Iris
 - CASIA
- Palmprint
 - Hong Kong Polytech Univ
 - CASIA

Algorithm Competition Winners

- Face -- ICPR 2004 (Banca database)
 - No.1 in all tests (Tsinghua Univ.)
- Face -- ICB 2006 (XM2VTS database)
 - No.1 in all tests (Institute of Comp. Tech, CAS)
- Fingerprint -- FVC 2004
 - 3rd on the open category, 7th on the light category (CASIA)

Biometric Databases

- CASIA Iris Database
 - Used by 1600 organizations from 70 countries/regions
- CAS-PEAL Face Database
 - Used by 95 organizations from 30 countries/regions

Applications & Markets

Significant Biometric Applications

- Governmental
 - Self-Service Border-crossing (deployed)
 - ShenZhen – Hong Kong Boarder since June 2005
 - Zhuhai – Macau Boarder since April 2006
 - Biometric E-Passport (on-going)
- Enterprise: Time attendance and access control
 - Finger, Face, Iris, Hand
- Consumer products
 - Face Logon – on notebook PC
 - Finger Logon – on mobile phone
 - Finger Lock

Biometric Border-Crossing: ShenZhen – HongKong

- 400,000 border-crossings every day
- Two scenarios: Passengers & Vehicle Drivers
- 100+ gates deployed by now
- Two Modalities: Face & Fingerprint
- 1,600,000 people enrolled.
- Verification Speed: 6 sec / crossing
- 35,000,000 crossings since June 2005



Market: Biometric Sales

Modality	Sales (units)	Revenue (m)	Mkt share
Fingerprint	165,000	462.0	95.2%
Palm	500	15.5	3.2%
Face	(licenses)	5.1	1.1%
Iris	100	2.2	0.5%
	Total	484.8	100%

Market: Application Sectors

Applications	Mkt share
Time Attendance	42.2%
Access Control	27.6%
Lock	14.3%
Government	4.1%
Information Security	0.97%
Police AFIS	7.58%
Others	3.25%
Total	100%

Standardization

Standardization and Testing: Organizations

- Standardization Administration of China (SAC)
 - National Standardization Technical Committee for Information Technology (TC28) ↔ ISO/IEC JTC1
 - <http://www.nits.gov.cn>
 - TC28 secretariat: China Electronics Standardization Institute (<http://www.cesi.ac.cn>)
- Related Organizations
 - TC100 ↔ IEC TC79
 - www.tc100.org.cn
 - TC100 secretariat: Ministry of Public Security
 - Center for Biometric Product Testing
 - A Branch of Center for Information Security Product Testing
 - Host: CBSR (www.cbsr.la.ac.cn)

Ongoing Works: National Standards

- SAC/TC28 (\leftrightarrow ISO/IEC JTC1)
 - Developing product standards (Eg: Technical specification for iris authentication systems)
 - To absorb SC37 standards as national standards (2007 projects)

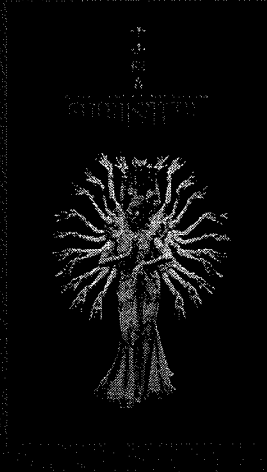
Ongoing Works: Product Standards

- SAC/TC100 (\leftrightarrow IEC TC79)
 - For Public Security Related Applications
 - Developing Standards for
 - Fingerprint, Face, Iris, and Hand Geometry

Future Perspectives

1. China to become a great market for biometrics (currently very small)
2. China to become a provider of biometric technologies and systems (visible now)
3. China to contribute to SC37 (We will do our best)

Thank You



Thank You



Contact:
Prof. Stan Z. Li
Center for Biometrics and Security Research
Institute of Automation, Chinese Academy of Sciences
szli@nlpr.ia.ac.cn

EXHIBIT 5



- [Home](#)
- [Markets](#)
- [Products & Services](#)
- [Partners](#)
- [Support](#)
- [About NECAM](#)
- [Press Room](#)

- [Servers](#)
- [Storage Arrays](#)
- [Thin Client](#)
- [AFIS Fingerprint / Palmprint ID](#)
 - [21st Century ID Technology](#)
 - [Highest Standards](#)
 - [Worldwide Deployment](#)
 - [Integrated Networks](#)
 - [AFIS User Group](#)
- [Identity Management](#)
- [Enterprise Software](#)
- [Cinema](#)
- [IT Consulting and Managed Services](#)
- [Retail Applications](#)
- [Enterprise Content Management](#)
- [Optical Networking](#)
- [Carrier Professional Services](#)
- [Removable Storage](#)
- [Visual Displays](#)
- [Printer Supplies](#)

[Home](#) >> [Products & Services](#) >> [AFIS Fingerprint/Palmprint ID Solution](#)

AFIS FINGERPRINT/PALMPRINT ID

Quickly and accurately match fingerprints and palmprints while the suspect is still in custody! NEC's Automated Fingerprint Identification System (AFIS) is considered one of the best biometric identification solutions in the world today.

21st Century Identification Technology

NEC's AFIS identification technology leads the industry because of its proven technology, superior accuracy, open system platform, integrated solutions and high capacity.

Highest Standards

NEC's AFIS meets and exceeds the highest current state and federal government standards in identification technology.

Worldwide Deployment

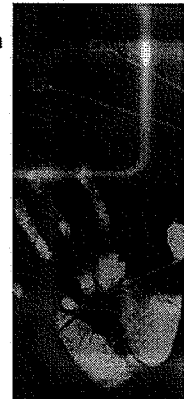
NEC AFIS collectively store over 60 million records and process more than 500,000 transactions daily helping solve more crimes from latent prints than all other systems combined.

Integrated Networks

NEC has successfully implemented statewide and inter-state AFIS networks with interfaces to different Computerized Criminal History systems. NEC's AFIS is based on an open-system platform that satisfies current interface needs for live scan and other record systems, ready for new interfaces in the future with minimal upgrade costs.

Active AFIS User Group

Current customers remain a valuable resource for Research and Development on how to improve AFIS design and operation. NEC has never failed to meet customer requirements for capacity, throughput, or response time.



Related Informa

- [Events](#)
- [In the News](#)
- [Press Releas](#)
- [Collateral Do](#)
- [Request More](#)

I found what I needed. disagree agree

I found it quickly. disagree agree





[SITE INDEX](#) [CONTACT NEC](#) [GL](#)

- [Home](#)
- [Markets](#)
- [Products & Services](#)
- [Partners](#)
- [Support](#)
- [About NECAM](#)
- [Press Room](#)

- [Servers](#)
- [Storage Arrays](#)
- [Thin Client](#)
- [AFIS Fingerprint / Palmprint ID](#)
 - [21st Century ID Technology](#)
 - [Highest Standards](#)
 - [Worldwide Deployment](#)
 - [Integrated Networks](#)
 - [AFIS User Group](#)
- [Identity Management](#)
- [Enterprise Software](#)
- [Cinema](#)
- [IT Consulting and Managed Services](#)
- [Retail Applications](#)
- [Enterprise Content Management](#)
- [Optical Networking](#)
- [Carrier Professional Services](#)
- [Removable Storage](#)
- [Visual Displays](#)
- [Printer Supplies](#)

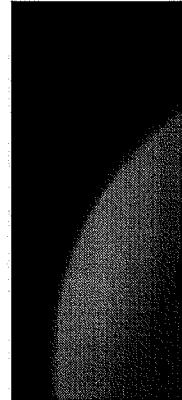
[Home](#) >> [Products & Services](#) >> [AFIS Fingerprint/Palmprint ID Solution](#)
>> [AFIS: Worldwide Deployment](#)

AFIS: WORLDWIDE DEPLOYMENT

More than 65 percent of the world's fingerprints are stored on NEC's AFIS, helping solve more crimes from latent prints than all other systems combined.

NEC's AFIS is currently in use in the following countries:

Country	Number of Installations
Japan	49
North America	37
China	5
Taiwan	4
Spain	3
Macau	2
Singapore	2
Argentina	1
Chile	1
El Salvador	1
Grenada	1
Indonesia	1
Namibia	1
New Zealand	1
Philippines	1
South Africa	1
Thailand	1
Turkey	1



Related Informa

- [Events](#)
- [In the News](#)
- [Press Releas](#)
- [Collateral Do](#)
- [Request More](#)

I found what I needed. disagree agree

I found it quickly. disagree agree

www.necam.com
© 2006 NEC Corporation of America
Terms of Use Privacy Policy

