"SECURE BORDERS, OPEN DOORS": CONSULAR PROCESSING ISSUES IN 2007

by Tien-Li Loke Walsh and Bernard P. Wolfsdorf[*]

Since 9/11, numerous measures designed to enhance security and streamline visa processing have been implemented to identify and eliminate vulnerabilities in the visa processing system. The passage of the USA PATRIOT Act of 2001,[1] followed by the Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act),[2] and the Homeland Security Act of 2002,[3] accelerated these efforts by mandating increased coordination of law enforcement and intelligence agencies, inter-agency data sharing, implementation of an integrated entry and exit control system, establishment of terrorist lookout committees, foreign student monitoring, biometric collection, mandatory interviews, and intensified security check measures. These procedures created a negative, "zero-tolerance" framework, making consular practice a daunting exercise. The combination of these statutory provisions together with the steady stream of changes including the introduction of additional security clearance procedures for "List of 26" nationals from predominantly Muslim countries,[4] restrictions on the "Terrible 7" countries, (now the "Terrible 5") [5] changes to the automatic revalidation provision, increasing applicability of the Technology Alert List (TAL),[6] enforcement of export controls, and a growing scrutiny of visa violations including overstays and unauthorized employment issues, as well as minor criminal convictions, completely changed the playing field. Although some of the security measures were expected after 9/11, visa applicants, faced with an entirely new visa framework, routinely encountered completely unpredictable surprises that caused unexpected and lengthy delays in visa issuance. The inevitable problems associated with a major restructuring and the creation of new agencies were compounded by a restrictive attitude on the part of the Department of State (DOS) and U.S. Citizenship and Immigration Services (USCIS). This adversely impacted U.S. interests in business, trade, tourism, scientific research, academics, and entertainment.

Five years after 9/11, the consular framework has shifted, moving away from the "zero-tolerance" blanket approach. In recognition of the need to balance national security interests with other strategic interests, such as promoting U.S. business interests, tourism, academic and scientific education and exchange, and the overall health of the economy, DOS has now embraced its "Secure Borders, Open Doors"[7] policy. Following a restrictive and

 Updated from an article by Loke Walsh and Wolfsdorf appearing in *Homeland Security, Business Insecurity, Immigration Practice in Uncertain Times* 43 (AILA 2003).

Tien-Li Loke Walsh is a senior attorney with the Wolfsdorf Immigration Law Group, who practices exclusively in the area of immigration and nationality law. She currently serves as the vice-chair on the AILA/DOS Liaison Committee and previously served two terms on the AILA/CSC Liaison Committee. Loke Walsh is listed in the *International Who's Who of Corporate Immigration Lawyers*. She completed her undergraduate studies at the University of Sydney, Australia, and received her J.D. from Boston University School of Law. Loke Walsh can be contacted at *tloke@wolfsdorf.com.*

Bernard P. Wolfsdorf is currently the National First Vice-President of the American Immigration Lawyers Association (AILA). He is a partner in the Wolfsdorf Immigration Law Group, one of the largest in the United States with offices in Los Angeles and New York City. He is a California State Bar Certified Specialist in immigration and nationality law and is listed in Martindale Hubbell's Preeminent Specialist Directory. The firm figures prominently among the top immigration firms in the nation, with three nominees in *The International Who's Who of Corporate Immigration Lawyers*. The Chambers Global *World's Leading Lawyers for Business* guide noted Wolfsdorf's "outstanding consular law practice" and called him a "cutting-edge thinker." Wolfsdorf has written extensively on consular processing and frequently speaks on the topic. He can be contacted at *Bernard@Wolfsdorf.com.*

[1] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (hereinafter USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272 (2001).

[2] Enhanced Border Security and Visa Entry Reform Act of 2002, Pub. L. No. 107-173, 116 Stat. 543 (2002) (hereinafter Border Security Act).

[3] The Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002) (hereinafter Homeland Security Act).

[4] Although it is classified, the list of countries reportedly affected by these restrictions includes, but is not limited to, Afghanistan, Algeria, Bahrain, Bangladesh, Djibouti, Egypt, Eritrea, Indonesia, Iran, Iraq, Jordan, Kuwait, Lebanon, Libya, Malaysia, Morocco, Oman, Pakistan, Qatar, Saudi Arabia, Somalia, Sudan, Syria, Tunisia, Turkey, the United Arab Emirates, and Yemen.

[5] The original "Terrible 7" refers to countries identified as state sponsors of terrorism, which until recently were designated as Iraq, Iran, Syria, Libya, Sudan, North Korea, and Cuba. Consular officials now refer to the list as the "Terrible 5 or T-5" countries, since Libya and Iraq were removed from the list, but Libyan and Iraqi nationals still undergo extensive security checks.

[6] The TAL is discussed in detail later in this article.

[7] The concept of former Secretary Colin Powell's "Secure Borders, Open Doors," describes a "vision of an America with robust and effective measures to safeguard national security that is still able to open its doors to the exchange of people, ideas and goods that has helped to make this nation great. It is no mistake that the "secure borders" part comes first. We can have no free-

continued

frustrating period, we have seen a softening in policy and the application of a more rational and focused approach in consular processing. In the summer of 2004, DOS launched a nonimmigrant travel and business facilitation initiative that reflected this moderation of policy.[8] This policy has resulted in significant improvements to the visa application process.[9] As a result, increased coordination between government agencies, streamlined visa application procedures and improved security check processing times have increased efficiency and provided practitioners, visa applicants and employers with a degree of predictability to the consular framework. Nevertheless, this different consular processing framework still provides numerous challenges to practitioners.

MEASURES AFFECTING THE VISA APPLICATION PROCESS

What are All These Security Checks and Security Advisory Opinions (SAOs)?

Prior to 9/11, there were two basic kinds of security checks initiated by consular posts. First, Washington agency name checks involved visas that could be issued within a specific time frame if "no response" was received from Washington within a designated time period. The second type of security check, known as a Security Advisory Opinion (SAOs), was a more elaborate security check that includes a name check, but for which the visa could not be issued until an affirmative response was received from DOS authorizing issuance of the visa. The code name for Washington agency name checks and SAOs were based on animals that "walk-in" and animals that "fly-over." Name checks that traditionally did not require a DOS response were said to "fly-over" (*e.g.*, Visas Eagle) to the various police and intelligence agencies—hence the avian code names. SAOs are differentiated by animals that "walk-in," and thus, require DOS action and response (*e.g.*, Visas Donkey or Visas Bear).[10] Since 9/11, DOS has made significant changes and improvements to its system of SAOs. If an SAO is initiated, consular posts must now wait for an affirmative response from all appropriate government agencies prior to issuing a visa.

Furthermore, since 9/11, DOS and other U.S. government agencies, including the CIA, FBI, and NSA have consulted in an extensive and ongoing review of visa issuing procedures. Over eight million records from the FBI's National Crime Information Center (NCIC) have been incorporated into the Consular Lookout and Support System (CLASS) name check database, more than doubling the records on file to 18 million.[11] Additional name check records from the intelligence community through TIPOFF, along with data from the U.S. Marshals Service,

---

dom without security. While focusing on security, we have also worked to uphold our commitment to the second part of the equation—"Open Doors"—making sure that they remain open to all of those who do not intend to do us harm and who will abide by our laws." As the cable states, ultimately, success will be measured in increased numbers of visa applications, more legitimate travelers contributing to America's economy and culture, maintaining the security of the visa process. *See* "DOS Issues Cable on the Nonimmigrant Travel Initiative," *published on* AILA InfoNet at Doc. No. 04101861 (*posted* Oct. 18, 2004).

[8] As part of its "Secure Borders, Open Doors" policy, DOS launched a series of initiatives, including the July 2004 "Business Travel Initiative" to facilitate business travel in support of U.S. commerce abroad (urging posts to build relationships with local American Chambers of Commerce, establish business referral programs, provide expedited appointments, group appointments, time-block set-asides, etc.). *See* "DOS Issues Cable on New Initiative to Facilitate Business Travel," *published on* AILA InfoNet at Doc. No. 04101864 (*posted* Oct. 18, 2004) and "DOS Issues Cable on Facilitation of Business Travel," *published* on AILA InfoNet at Doc. No. 04121461 (*posted* Dec. 14, 2004); the August 2004 "Nonimmigrant Travel Initiative" ("Secure Borders, Open Doors" encouraging posts to prioritize students and medical cases, to undertake self assessments of processes and procedures to strengthen the visa process and ensure border security); *Id*; the August 2004 reminder to posts about placing key visa processing information on post websites; *see* "Follow-up to Key Visa Processing Information on Consular Post Websites," *published on* AILA InfoNet at Doc. No. 05030165 (*posted* Mar. 1, 2005); and Assistant Maura Harty's December 2004 cable to posts entitled, "We Don't Want to Lose Even One Student"; *see* "DOS Reminds Posts to Prioritize Student Visas," *published on* AILA InfoNet at Doc. No. 04121563 (*posted* Dec. 15, 2004).

[9] According to DOS, its efforts have translated into positive results. The Department of Commerce announced that there are recent positive indicators about international travel to the United States. International arrivals for June 2004 year-to-date increased 16 percent over the same period in 2003. More importantly, between January 1 through June 30, 2004, NIV applications increased 10.4 percent; visa issuances increased 9.4 percent and student visa issuances increased 11.2 percent. *See* "Improvements to Visa Processing, DOS Fact Sheet," Oct. 20, 2004, at *www.travel.state.gov/r/pa/prs/2004/37254.htm.*

[10] *See* R. Sindelar, "CHIMERA, NSEERS, Lookouts and Security Checks: The New Age," 8 *Benders Immigr. Bull.* 105 (Jan. 15, 2003) at 107. Previously, a Visas Eagle Mantis was a no-response precheck procedure that allowed posts to process a case to conclusion after a 10-calendar-day suspended period. The Visas Eagle Mantis was used primarily for U.S. government-sponsored programs with possible TAL related issues, with heavy usage for individuals from PRC China. A Visas Donkey is the SAO used for all more serious concerns, including suspected terrorists who may be inadmissible under §212(a)(3)(B), drug traffickers, suspected foreign intelligence agents, Terrible 6 country applicants, or an applicant who may have a TAL issue. *Id.* at 108.

[11] *See* Testimony of Assistant Secretary of State for Consular Affairs Maura Harty Before the National Commission on Terrorist Attacks Upon the United States, Jan. 26, 2004, available at *http://travel.state.gov/MH01262004.html.*

were also incorporated into CLASS.[12] In addition, the CLASS and TIPOFF databases interface with the Interagency Border Inspection System (IBIS), the Treasury Enforcement and Communications System (TECS II), the National Automated Immigration Lookout System (NAILS), and the Nonimmigrant Information System (NIIS). DOS is presently working closely with CBP and their National Targeting Center to improve communications between DOS and DHS on border inspection and entry issues to improve DOS access to adverse actions at the ports of entry (*e.g.*, cases in which visa holders are denied entry).[13] DOS also relies on the Terrorist Screening Center (TSC) and the Terrorist Threat Integration Center (TTIC), which integrates and maintains the terrorist watch lists and is accessible to consular officers. All of this information, which is constantly updated, includes information on terrorists and foreign warrants, but also extensive information about any criminal convictions or arrests including relatively minor offenses for DUIs or shoplifting, and provides consular officers with access to critical information during the visa interview process. Consular officers also use the Consular Consolidated Database (CCD), which includes over 75 million records of visa applications used to screen visa applicants. Since February 2001, the CCD stores photographs of all visa applicants in electronic form. Most recently, it has started to store fingerprints. In addition to interfacing with other databases, the CCD indicates the outcome of any prior visa applications.

DOS has made improvements to its system of SAOs, which require consular posts to refer selected visa cases, identified by law enforcement and intelligence information, for enhanced review. All of these SAO procedures involve close cooperation with other government agencies that are experts in law enforcement, counter-terrorism and high technology. In FY 2006, DOS processed 244, 558 SAO's, including 57, 318 Condors and 33, 388 Mantis checks; so far in FY 2007, DOS has processed over 820,000 NCIC checks.[14] In FY 2005, DOS estimated that it processed 226,083 SAO and NCIC cases, including 63,332 Condors, 24,197 Mantis and 195,758 NCIC checks; in FY2004, close to 200,000 SAOs were processed, including about 57,000 Condors and 18,000 Mantis cases. [15]

Visas Condor Security Advisory Opinions

Initiated on January 26, 2002, the Visas Condor SAO focuses on potential terrorism applicants. It is triggered primarily by information provided on the Supplemental Nonimmigrant Visa Application Form DS-157, which is submitted as part of the visa application process. The DS-157 requests information about the applicant's travel and educational history, employer information, and military service. This data is used to assess whether a visa applicant requires a Condor SAO or other security check. DOS applies a "native" standard so that additional security measures are initiated for applicants born in one of the "List of 26" or "Terrible 6 countries," and not just to citizens of those countries.[16]

After 9/11, the Condor SAOs initially resulted in long delays, often as long as four to six months, because none of the federal agencies involved in the clearing process were technically equipped to handle the volume of data that was received when the program began.

It appears that citizens or nationals from the List of 26 countries where there are few surnames or name similarity is common (*e.g.,* Patel, Mohammad Ali, Mohammad Siddiqui, etc.), create the most problems for consular posts. If there is a "hit" in the system and if there is no clarifying information such as a date-of-birth, a consular officer has no choice but to initiate a Condor security check. Additionally, any individual who has spent time, whether for short visits or extended assignments or peri-

[12] *See* "Initiatives by the Bureau of Consular Affairs to Enhance National Security," Fact Sheet, Bureau of Consular Affairs, Washington, D.C. (Sept. 5, 2002), *posted on ilw.com* (Sept. 29, 2002).

[13] According to a GAO Report many visa chiefs reported that additional guidance would be helpful regarding the interaction between DOS and DHS, as well as DHS procedures at port-of-entries, such as guidance on how to resolve cases in which visa holders have been denied entry. For example, detailed information on the reason why a visa holder was not allowed into the United States—the person was recently placed on a watch-list, for example—is not automatically transferred to CLASS. "Border Security: Strengthened Visa Process Would Benefit from Improvements in Staffing and Information Sharing," Report to Congressional Committees (Sept. 2005) by the U.S. Government Accountability Office, *published on* AILA InfoNet at Doc. No 05091372 (*posted* Sept. 13, 2005) (hereinafter "GAO Report"). According to DOS, although DHS and DOS already exchange considerable lookout records, they are working to create a link between consular and CBP databases that would allow the transfer of data, including transcripts of interviews at ports-of-entry and making I-275 records available to consular officers electronically on a real-time basis. *See* "DOS Answers to AILA's Questions," (Mar. 23, 2006), *published on* AILA InfoNet at Doc. No. 06041060 (*posted* Apr. 10, 2006).

[14] *See* "AILA/DOS Liaison Meeting Minutes," *published on* AILA InfoNet at Doc. No. 06101267 (*posted* Oct. 12, 2006). *See also* "AILA/DOS Liaison Meeting Minutes," *to be published on* AILA InfoNet.

[15] *See* "DOS Answers to AILA's Questions," (Oct. 2005), *published on* AILA InfoNet at Doc. No. 05112874 (*posted* Nov. 28, 2005); "DOS Answers to AILA's Questions," (Mar. 17, 2005), *published on* AILA InfoNet at Doc. No. 05062117 (*posted* Jun. 21, 2005).

[16] *See* "The Consul and the Visas Condor" (Dec. 4, 2002), *published on* AILA InfoNet at Doc. No. 03012240 (*posted* Jan. 22, 2003), where AILA's Department of State Liaison Committee held an informal, off-the-record conversation with a senior visa officer at a U.S. consular post abroad on December 4, 2002. Interestingly, even if an applicant who is a citizen or national of a "List of 26" or "Terrible 6" is refused a visa, consular officers will "send a Visas Condor anyway…" *Id.*

ods as a minor in a "country of concern," could be subject to a Condor SAO (a common scenario involves the children of Europeans, born in or who spent part of their childhood in former Commonwealth colonies such as Malaysia. Another scenario is where parents worked in the oil business and a child grew up in Saudi Arabia despite having European citizenship).

At the end of 2003, DOS provided consular posts with additional factors and guidelines to consider when faced with potential Condor situations, but the guidance remains classified. However, it appears that this guidance has proven useful to consular posts. Anecdotal reports indicate that by mid-2004, applicants from some of these countries have not been subjected to Condor SAOs and receive their visas within normal NIV processing times.[17]

If a Condor SAO is required, DOS requires posts to wait for an affirmative response from all participating agencies prior to issuing a visa.[18]

As of March 2007, DOS reported that the average processing times for Condor SAOs was approximately four days. To date, there is no system to expedite these security checks. However, if a security check has been pending for over 45 days, counsel may call the Visa Office (VO) public inquiries number at (202) 663-1225 or fax (202) 663-3899 or send an e-mail inquiry to *legalnet@state.gov*.[19]

NCIC Checks and "Hits" in the Database

As a result of increased database sharing between government agencies, consular posts have been inundated with "hits" from the millions of names added to the NCIC database, revealing criminal convictions including minor offenses such as simple DUIs and shoplifting. The NCIC check is technically not a security check and is actually integrated into the CLASS name check that is performed on every visa applicant. Since DOS is not a law enforcement agency, consular posts do not have access to detailed information explaining the reason underlying the "hit." If an applicant's name is identified as a "hit," posts will request an appearance by the applicant in order to obtain a full set of fingerprints, which are submitted for further analysis to the FBI but this check is not considered an SAO. In December 2006, DOS completed its worldwide deployment of the software for electronic fingerprinting, which allows posts to submit the fingerprints directly to the FBI. The ability to capture fingerprints electronically allows posts to provide the results of the FBI fingerprint checks within a 24-hour period in most cases.[20]

Although attorneys have attempted to be pro-active and expedite the process by submitting copies of arrest records, final court-dispositions and attorney-initiated FBI results at the initial visa application, consular officers are required to obtain fingerprints in any case of a NCIC name check "hit."[21] Once a post has received a response from the FBI via the National Visa Center (NVC), it may at the consular officer's discretion, accept documentation from the applicant that matches the extract provided by the FBI.[22] However, consular posts will not accept submission of all related documents in lieu of initiating required security checks and fingerprinting.

Applicants with a criminal record must undergo a NCIC check with each visa application, even if a renewal and a NCIC check was performed initially. Since there is no information relating to the hit in the database, even if the NCIC information had been obtained in the course of a previous application, there is no way to know if it is still timely and accurate when processing a subsequent application.

There is continuing DOS concern that there is an inability of consular officers to access key information about an applicant's criminal history records and its effects upon the efficiency of the visa processing system. DOS continues to hold discussions with the FBI to provide consular officers with immediate access to pertinent information such as criminal charges and final dispositions. DOS expects that the plans to migrate to a ten-print fingerprint collection over the next several years will likely obviate this problem and consular officers will be

[17] According to DOS, the chief of mission at a post has discretion to waive a Condor, but consular officers do not. *See* "DOS Answers to AILA's Questions," (Mar. 17, 2005), *supra* note 15.

[18] When first implemented, Visas Condor cables were sent to the FBI, CIA, the Department of Defense (DOD), and the National Security Agency (NSA). *See* "Border Security: Visa Process Should Be Strengthened as an Antiterrorism Tool," Report to the Chairman, Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform, House of Representatives (Oct. 2002) by the United States General Accounting Office at 21–22. *Published on* AILA InfoNet at Doc. No. 02110545 (*posted* Nov. 5, 2002) (hereinafter "Oct. 2002 GAO Report"). In September 2002, the FBI became the primary agency for conducting the name checks and clearing Condor cables, and the CIA started conducting name checks for selected Condor applications, rather than all of them. According to CIA and DOJ officials, under the new procedures, the FBI's Name Check Unit conducts the initial Condor name checks, which involve running the applicant's information against their databases at headquarters, and in some cases, at the Foreign Terrorism Tracking Task Force (FTTTF). If these checks result in a possible match, then the FBI sends the information on the visa applicant to DOS, which then forwards it to the CIA. *Id*. at 24.

[19] *See* "DOS Answers to AILA's Questions," (Oct. 2005) *supra* note 14.

[20] *See* "AILA/DOS Liaison Meeting Minutes," (Mar. 2007) *to be published on* AILA InfoNet.

[21] 22 CFR §41.105(b)(2); *see also* "DOS Answers to AILA Questions" (Oct. 2, 2002), *published on* AILA InfoNet at Doc. No. 02100340 (*posted* Oct. 3, 2002).

[22] *Id.*; *see also* "DOS Answers to AILA Questions" (Mar. 27, 2003), *published on* AILA InfoNet at Doc. No. 03040340 (*posted* Apr. 3, 2003).

able to access this information once the applicant's identity is confirmed through fingerprints.[23]

"False hits" continue to be of concern for unsuspecting visa applicants. Unfortunately, anecdotal reports confirm that there are still an alarming number of false hits caused by similar or identical names, especially when the applicant is from a country where there are few surnames and name similarity is quite common. Approximately half of the names in the NCIC database reflect Hispanic ethnicity and this has resulted in an alarming number of false hits for individuals with common names. Applicants with such hits are not provided with an opportunity to show that they are not the same person as that on the database.[24] To date, there is no way to initiate the security check in advance of a visa application.[25]

The Technology Alert List and Visas Mantis Security Advisory Opinions

The Visas Mantis program is an SAO procedure designed to ensure that sensitive technology is not stolen or inappropriately shared with those who would use it to harm the United States and its allies. In assessing these threats, DOS relies primarily on the Technology Alert List (TAL) [26] to make its determinations. The TAL cable

[23] *See* "DOS Answers to AILA's Questions," (Oct. 2005) *supra* note 15.

[24] Although an applicant is required to provide first, middle, and last names, maiden names, tribal names, and all names used when completing Forms DS-156 and DS-157, the provision of this information does not necessarily prevent a wary consular officer from initiating a security check on a discretionary basis.

[25] *See* "DOS Answers to AILA Questions" (Oct. 2, 2002), *supra* note 21.

[26] The TAL was originally designed to help maintain technological superiority over the Warsaw Pact and was targeted at individuals from the Soviet Union and other Communist countries. In 1996, the TAL was revised to broaden its focus and reflect more accurately current laws restricting or prohibiting the export of goods and technologies. These laws are designed to further four important security objectives: (i) Stem the proliferation of weapons of mass destruction and missile delivery systems; (ii) Restrain the development of destabilizing conventional military capabilities in certain regions of the world; (iii) Prevent the transfer of arms and sensitive dual-use items to terrorist states; and (iv) Maintain U.S. advantages in certain militarily critical technologies.

The critical fields list, which constitutes the Technology Alert List (TAL), is as follows: (A) Conventional Munitions—technologies associated with warhead and large caliber projectiles, reactive armor and warhead defeat systems, fusing, and arming systems, electronic countermeasures and systems, new or novel explosives and formulations, automated explosive detection methods and equipment; (B) Nuclear Technology—technologies associated with the production and use of nuclear material for both peaceful and military applications, including enrichment of fissile material, reprocessing irradiated nuclear fuel to recover produced plutonium, production of

continued

heavy water for moderator material, plutonium and tritium handling. Also, certain associated technologies related to nuclear physics and/or nuclear engineering, including materials, equipment or technology associated with power reactors, breeder and production reactors, fissile or special nuclear materials, uranium enrichment, including gaseous diffusion, centrifuge, aerodynamic, chemical, Electromagnetic Isotopic Separation (EMIS), Laser Isotope Separation (LIS), spent fuel reprocessing, plutonium, mixed oxide nuclear research Inertial Confinement Fusion (ICF), magnetic confinement fusion, laser fusion, high power lasers, plasma, nuclear fuel fabrication including Mixed Oxide (uranium-plutonium) fuels (MOX), heavy water production, tritium production and use, hardening technology; (C) Rocket Systems—(including ballistic missile systems, space launch vehicles and sounding rockets) and Unmanned Air Vehicles (UAV) (including cruise missiles, target drones, and reconnaissance drones)—technologies associated with rocket systems and UAV systems (the technology needed to develop a satellite launch vehicle is virtually identical to that needed to build a ballistic missile); (D) Rocket System and Unmanned Air Vehicle (UAV) Subsystems—Propulsion technologies include solid rocket motor stages, and liquid propellant engines. Other critical subsystems include re-entry vehicles, guidance sets, thrust vector controls and warhead safing, arming and fusing. Many of these technologies are dual-use and include liquid and solid rocket propulsion systems, missile propulsion and systems integration, individual rocket stages or staging/separation mechanism, aerospace thermal (such as super alloys) and high-performance structures, propulsion systems test facilities. (E) Navigation, Avionics and Flight Control Useable in Rocket Systems and Unmanned Air Vehicles (UAV)—These capabilities directly determine the delivery accuracy and lethality of both unguided and guided weapons. The long-term costs to design, build and apply these technologies have been a limiting proliferation factor. Technologies include those associated with internal navigation systems, tracking and terminal homing devices, accelerometers and gyroscopes, rocket and UAV and flight control systems and global Positioning System (GPS); (F) Chemical, Biotechnology and Biomedical Engineering—technology used to produce chemical and biological weapons is inherently dual-use. The same technologies that could be applied to develop and produce chemical and biological weapons are used widely by civilian research laboratories and industry; these technologies are relatively common in many countries. Advanced biotechnology has the potential to support biological weapons research. In the biological area, areas of interest in technologies associated with Aerobiology (study of microorganisms found in the air or in aerosol form), Biochemistry, Pharmacology, Immunology Virology Bacteriology, Mycology, Microbiology, Growth and culturing of microorganisms, Pathology (study of diseases), Toxicology, Study of toxins, Virulence factors, Genetic engineering, recombinant DNA technology, Identification of nucleic acid sequences associated with pathogenecity, Freeze-drying (lyophilization), Fermentation technology, Cross-filtration equipment, High "DOP-rated filters" (*e.g.*, HEPA filters, ULPA filters), Microencapsulation, Aerosol sprayers and technology, aerosol and aerosolization technology, Spray or drum drying technology, Milling equipment or technology intended for the production of micron-sized particles, Technology for eliminating electrostatic charges of small particles, Flight training, Crop-dusting, aerosol dissemination, Unmanned aerial vehicle (UAV) technology, Fuses, detonators, and other munitions technology, Submunitions technology, Computer modeling of dissemination or contagion, Chemical absorption (nuclear-biological-chemical (NBC) protection). In the chemical area, includes Organo-phosphate chemistry, Neurochemistry, Chemical engineering, Chemical separation technology, Pesticide production

continued

technology, Pharmaceutical production technology, Chemical separation technology, Toxicology, Pharmacology, Neurology, Immunology, Detection of toxic chemical aerosols, Chemical absorption (Nuclear-Biological-Chemical (NBC) protection), Production of glass-lined steel reactors/vessels, pipes, flanges, and other equipment, Aerosol sprayers and technology, Flight training, Crop-dusting, aerosol dissemination, Unmanned Aerial Vehicle (UAV) technology, Fuses, detonators, and other munitions technology, Submunitions technology, Computer modeling of dissemination; (G) Remote Sensing, Imaging and Reconnaissance—satellite and aircraft remote sensing technologies are inherently dual-use; increasingly sophisticated technologies can be used for civilian imagery projects or for military and intelligence reconnaissance activities. Drones and remotely piloted vehicles also augment satellite capabilities. Key-word associated technologies include, Remote sensing satellites, High resolution multi-spectral, electro-optical and radar data/imagery, Imagery instruments, cameras, optics, and synthetic aperture radar systems, Ground receiving stations and data/image processing systems, Photogrammetry, Imagery data and information products, Piloted aircraft, Unmanned Air Vehicles (UAV), Remotely-piloted vehicles; and drones; (H) Advanced Computer/Microelectronic Technology—advanced computers and software play a useful (but not necessarily critical) role in the development and deployment of missiles and missile systems, and in the development and production of nuclear weapons. Advanced computer capabilities are also used in over-the-horizon targeting airborne early warning targeting, Electronic Countermeasures (ECM) processors. These technologies are associated with Supercomputing, hybrid computing, Speech processing/recognition systems, Neural networks, Data fusion, Quantum wells, resonant tunneling, Superconductivity, Advance optoelectronics, Acoustic wave devices, Superconducting electron devices, Flash discharge type x-ray systems, Frequency synthesizers, Microcomputer compensated crystal oscillators; (I) Materials Technology—the metallic, ceramic and composite materials are primarily related to structural functions in aircraft, spacecraft, missiles, undersea vehicles, and propulsion devices. Polymers provide seals and sealants for containment of identified fluids and lubricants for various vehicles and devices. High density graphite is used in missile nosetips, jet vanes and nozzle throats. Selected specialty materials (*i.e.*, stealth and the performance of these materials) provide critical capabilities that exploit electromagnetic absorption, magnetic, or superconductivity characteristics. These technologies are associated with advanced metals and alloys, Non-composite ceramic materials, Ceramic, cermet, organic and carbon materials, Polymeric materials, Synthetics fluids, Hot isostatic, Densifications, Intermetallic, Organometals, Liquid and solid lubricant, Magnetic metals and superconductive conductors; (J) Information Security—Technologies associated with cryptography and cryptographic systems to ensure secrecy for communications, video, data and related software; (K) Laser and Directed Energy Systems Technology—Lasers have critical military applications, including incorporation in guided ordinance such as laser guided bombs and ranging devices. Directed energy technologies are used to generate electromagnetic radiation or particle beams and to project that energy on a specific target. Kinetic energy technologies are those used to impart a high velocity to a mass and direct it to a target. Directed energy and kinetic energy technologies have potential utility in countering missiles and other applications. Look for technologies associated with Atomic Vapor Laser Isotope Separation (AVLIS), Molecular Laser Isotope Separation (MLIS), High Energy Lasers (HEL) (*i.e.*, laser welders), Low Energy Lasers (LEL), Semiconductor lasers, Free electron lasers, Directed Energy (DE) systems, Kinetic Energy (KE) systems, Particle beam, beam

continued

is also designed to specifically provide guidance for use in cases that may fall under the purview of INA §212(a)(3)(A), which renders aliens inadmissible where there is reason to believe they are seeking to enter the United States to violate or evade U.S. laws prohibiting the export of goods, technology, or sensitive information from the United States. The TAL guidance cable describes the specific purpose of the Mantis program, instructs consular officers what to look for when reviewing an application that may result in a Mantis cable and provides details on what information to include in a cable.

In August 2002, DOS significantly updated the TAL and issued a cable providing updated guidance to consular posts on the use of the TAL Mantis security checks.[27] The TAL was designed to assist in the effort to prevent the transfer of sensitive technology or material, (*e.g.*, controlled nuclear or biotechnical information), from falling into the wrong hands and being used by hostile individuals. The increasing sophistication of off-the-shelf technology, dual-use technologies (technologies which have both civilian and military applications), allegations of lack of sufficient information about and controls on foreign students in the United States, recent tensions in the Middle

rider, electromagnetic guns, Optoelectronics/electro-oPtics (Europe), Optical tracking (*i.e.*, target designators), High energy density, High-speed pulse generation, pulsed power, Hypersonic and/or hypervelocity, Magnetohydrodynamics; (L) Sensors and Sensor Technology—Sensors provide real-time information and data, and could provide a significant military advantage in a conflict. Marine acoustics is critical in anti-submarine warfare; gravity meters are essential for missile launch calibration. Includes technologies associated with Marine acoustics, Optical sensors, Night vision devices, image intensification devices, Gravity meters, High speed photographic equipment, Magnetometers; (M) Marine Technology—Marine technologies are often associated with submarines and other deep submersible vessels; propulsion systems designed for undersea use and navigation and quieting systems are associated with reducing detectability and enhancing operations survivability. Includes technologies connected with Submarines and submersibles, Undersea robots, Marine propulsion systems, Signature recognition, Acoustic and non-acoustic detection, Acoustic, wake, radar and magnetic signature reduction, Magnetohydrodynamics, Stirling engines and other air independent propulsion systems; (N) Robotics—Technologies associated with Artificial intelligence, Automation, Computer-controlled machine tools, Pattern recognition technologies; and (O) Urban Planning—Expertise in construction or design of systems or technologies necessary to sustain modern urban societies. (*Please note*: Urban Planning may not fall under the purview of INA §212(a)(3)(A), U.S. technology transfer laws, or any other U.S. law or regulation. However, Urban Planning is a special interest item and posts are requested to refer such visa application requests to CA/VO/L/C for further review.) Technologies/skills include Architecture, Civil engineering, Community development, Environmental planning, Geography, Housing, Landscape architecture, Land use and comprehensive planning, and Urban design. *See* "State Dept. Updates Guidance on Technology Alert Checks," *published on* AILA InfoNet at Doc. No. 03030449 (*posted* Mar. 4, 2003).

[27] *Id.*

East, and the 9/11 terrorist attacks have combined to renew concern among the law enforcement and intelligence communities that controlled U.S.-origin goods and information are vulnerable to a variety of concerns.

The revised TAL consists of two parts: a Critical Fields List (CFL) of major fields of technology transfer concern, including those subject to export controls for nonproliferation reasons, and DOS's list of designated State Sponsors of Terrorism, also known as the "Terrible 5" countries.[28] While restrictions on the export of controlled goods and technologies applies to scientific and technical visitors from all countries, DOS instructs posts that applicants from the "Terrible 7" countries seeking to engage in one of the critical fields warrant special scrutiny and mandatory security advisory opinion (SAO) checks.[29]

In comparison to the previous version, the updated TAL includes a vastly expanded list of associated technologies within each critical field, which details virtually every potential "dual use" application, where seemingly benign technologies have potential military applications. For example, the updated TAL includes a chemical, biotechnology and biomedical engineering critical fields. It is an all-encompassing list that includes almost every possible associated technology or skill involving chemistry, biochemistry, immunology, microbiology, pharmacology, genetic engineering, and chemical engineering to name a few. With such an all-inclusive list, nearly every research scientist, physician or academic, or engineer involved in any of these fields in commercial research laboratories, educational institutions and universities, or private industry may be subject to a TAL security check by a post erring on the side of caution.[30]

As further indication of the all-encompassing nature of the TAL, the updated list also adds a new field to the TAL—urban planning (expertise in construction or design of systems or technologies necessary to sustain modern urban societies). This indicates the government's interest in skills and technologies associated with architecture, civil engineering, community development, environmental planning, geography, housing, landscape architecture, land use and comprehensive planning, and urban design.

In all cases, consular officers must determine whether an applicant proposes to engage in advanced (doctoral, postdoctoral, or research scholar) research or studies, or business activity involving any of the scientific/technical fields listed in the CFL. The cable instructs posts that information in the public domain, *i.e.*, widely available to the public and information presented in an academic course generally is not relevant for U.S. technology transfer control purposes. Although the cable urges consular officials to use their judgment, it cautions officers to err on the side of caution if there are any doubts that any of the applicant's planned activities raise questions of possible ineligibility under INA §212(a)(3)(A). If in doubt, consular officers must submit an SAO in the form of a Visas Mantis.[31] If a determination is made that the technology involved presents a security risk, the applicant may be permanently barred under §212(a)(3)(A), which there is no waiver.

Despite this guidance, it appeared that the cable failed to provide consular posts and attorneys with clear direction[32] as to when an SAO is required and in fact, seemed

[28] The current designated list of state sponsors of terrorism includes Cuba, Iran, North Korea, Sudan, and Syria, *but see supra* note 5.

[29] *See* "State Dept. Updates Guidance on Technology Alert Checks," *published on* AILA InfoNet at Doc. No. 03030449 (*posted* Mar. 4, 2003).

[30] *Id.*

[31] When an SAO is submitted in a TAL case, consular officers are instructed to gather and report as much information as possible about the applicant's background, proposed activities, and travel plans. The effectiveness of the name check (and the turnaround time) is directly related to the completeness of the information in the SAO. For example: what are the applicant's research or business interests? What is his current position and where does he work? What is the address and phone number of the company(ies) he intends to visit? Who is his point of contact? What are the specifics of his advanced (doctoral, postdoctoral or research scholar) research or studies, or business in the United States? Who is funding the travel or education? Will he be returning to work in a country that sponsors terrorism or to an entity that is under sanctions? How, and where, does the applicant plan to use the goods or knowledge acquired? Consular officers are instructed to encourage TAL applicants to provide supporting documentation from their home organizations. For example, complete résumés and complete lists of publications of the applicant and, if accompanying the applicant information concerning the spouse; project descriptions; annual reports; and letters of recommendation from a U.S. source or from abroad. This information can be useful in helping to flesh out an applicant's real motives for travel. The cable instructs posts that such documents should be described in the SAO and held until the case has been closed. DOS encourages consular officers to provide as much information and details as possible in the SAO. *Id.*

[32] *See* "Border Security: Improvements Needed to Reduce Time Taken to Adjudicate Visas for Science Students and Scholars," Report to the Chairman and Ranking Minority Member, Committee on Science, House of Representatives (Feb. 2004) by the United States General Accounting Office, at 16 (hereinafter "Feb. 2004 GAO Report") found that many consular officials expressed concern that they could be contributing to the time it takes to process Visas Mantis requests because they lacked clear guidance on determining Visas Mantis cases and feedback on whether they were applying checks appropriately and providing enough data in their Visas Mantis requests. According to the officials, additional information and feedback from Washington regarding these issues could help expedite Visas Mantis cases. Consular officials also mentioned that they would like the guidance to be simplified—for example, by expressing some scientific terms in more comprehensive language. Several officials also mentioned that they had only a limited understanding of the Visas Mantis process, including how long the process takes. They told the GAO they

continued

to signal a bureaucratic shift towards initiating TAL SAO requests for all cases unless posts are absolutely sure the applicant will not be engaged in any of the technologies or skills listed on the TAL. In response to concern and criticism about the lack of clear guidance about the TAL, DOS confirmed that the TAL guidance was significantly revised and shared with the field via cable on October 1, 2003, but it remains classified.[33] Interestingly, the TAL has now been removed from the DOS website.[34]

The Visas Mantis Process

If a Mantis SAO is required, consular posts transmit the request to the Visa Office and interested agencies.[35]

In July 2004, the FBI, DOS, and DHS reached an agreement that fundamentally changed the FBI's role in the Visas Mantis process.[36] Officials from these agencies made a determination that the FBI could fulfill its law enforcement role in the Mantis process without routinely clearing Mantis cases. Under the new "no objections" policy, DOS does not have to wait for an FBI response before processing Mantis cases, but the FBI continues to receive information on visa applicants subject to Mantis checks.[37] Prior to this change in policy, DOS did not proceed with issuance of a visa until each individual government agency provided an affirmative response.

Under the current process, the other government clearing agencies are given 10 working days to respond to SAOs, but notify the Visa Office when they need additional time to clear a specific case.[38] One of the agencies may also ask a consular post to obtain more information from an applicant, which can also take time and delay a final response to post.[39] According to DOS, waiting for highly classified reports through appropriate channels can be another reason for delay in responding to a consular post.[40] Once DOS receives all agency responses pertaining to the applicant, it summarizes them and prepares a response to the consular posts.[41] A cable is then transmitted to the post, which indicates that DOS does or does not have an objection to issuing the visa, or that more information is needed.[42]

When initially introduced, there was extensive concern because delays in Mantis checks impacted the business, academic, and scientific communities, causing significant disruptions to ongoing research and commer-

would like to have better information on how long a Visas Mantis check is taking, so that they can accurately inform the applicant of the expected wait.

[33] The classified additional guidance was issued after the GAO visited some of these posts. However, consular officials at some posts told the GAO that although it was an improvement, the updated guidance is still confusing to apply, particularly for junior officers without a scientific background. *Id.* at 17. DHS and DOS may also consider further refining the TAL. *See* K. Field, "U.S. Government Considers Extending Security Clearances for Foreign Students and Scholars," *Chronicle of Higher Education* (Aug. 30, 2004).

[34] Anecdotal reports indicate that the TAL was removed from the DOS website because of concerns that applicants used the TAL to "tailor" their CVs before interviews at posts in an attempt to avoid initiation of a Mantis SAO. When asked about the removal of the TAL from the website based on concerns that there is no current guidance on what technologies may be on the list, DOS stated that the TAL is "not produced to assist business in making plans. Making available to the public a detailed list of sensitive technologies would be invaluable to those seeking to avoid undue scrutiny of technology transfer activities." *See* "DOS Answers AILA Questions," *published on* AILA InfoNet at Doc. No. 04120760 (*posted* Dec. 7, 2004).

[35] *See* Testimony of Janice L. Jacobs, Deputy Assistant Secretary of State for Visa Services, The Conflict Between Science and Security in Visa Policy: Status and Next Steps Before the House of Representatives Science Committee, Feb. 25, 2004, at *http://travel.state.gov/testimony10.html*.

[36] *See* "Border Security: Streamlined Visas Mantis Program Has Lowered Burden on Foreign Science Students and Scholars, but Further Refinements Needed," Report to Congressional Requesters (Feb. 2005) by the U.S. General Accounting Office at 13, *published on* AILA InfoNet at Doc. No. 05022266 (*posted* Feb. 22, 2005) (hereinafter "Feb. 2005 GAO Report).

[37] Prior to this change in its role in Mantis processing, the FBI name-check unit ran the names of the subjects of SAOs through their name check system, after which the responses were uploaded onto a CD containing updated clearance information, which the VO received twice a week. The CD is a historical record of more than 500,000 responses provided to DOS by the FBI. The information from the CD was uploaded into the DOS's own FBI Response database, as well as into an automated system known as VISTA, which is the VO's tracking system for SAOs. Unfortunately, for various technological reasons, VISTA did not always capture all of the clearance information. Therefore, if analysts did not find an updated response to a case in VISTA that is due, they had to check the FBI Response database to see if in fact, the FBI had cleared the case, because DOS does not complete processing of the visa until they have the FBI response. *See* Testimony of Janice L. Jacobs (Feb. 25, 2004), *supra* note 35. This policy resulted in a backlog of almost 1,000 cases and contributed to lengthy wait times for applicants. In February 2004, it took the FBI an average of about 29 days to complete clearances on Mantis cases. In fact, FBI clearance often took longer than any other step in the Mantis process. The FBI's new role allows DOS to process Mantis cases more easily. It has also allowed DOS to clear about 1,000 Mantis cases that the FBI had maintained a "hold" for a lengthy period. *See* Feb. 2004 GAO Report *supra* note 32 at 14.

[38] Prior to this, the remaining agencies had 15 working days to respond to DOS. *Id.* at 14. As a result, the total Mantis processing time could not be less than about 20 calendar days. According to DOS, with this new timeframe, it should be able to achieve total Mantis processing times of about 15–17 days. *Id.*

[39] *See* Testimony of Janice L. Jacobs (Feb. 25, 2004), *supra* note 35.

[40] *Id.*

[41] *See* Feb. 2004 GAO Report *supra* note 32 at 8.

[42] *Id.*

cial activities.[43] A February 2004 GAO Report ("Improvements Needed to Reduce Time Taken to Adjudicate Visas for Science Students and Scholars") found that interoperability problems among the systems that DOS and FBI use contributed to the delays in processing.[44] Since many different agencies, bureaus, posts, and field offices are involved in processing Mantis SAO's, and each has different databases and systems, Mantis SAO's were often delayed or lost[45] at different points in the process.[46] In addition, feedback from officers at consular posts confirmed that they were unsure whether they were adding to the lengthy waits by not having clear guidance on when to apply the Visas Mantis process and not receiving any feedback on the amount of information they provided in their Mantis requests.

DOS acknowledged that backlogs occurred based on the overburdened system, which required extensive cooperation between multiple government agencies not yet equipped to cope with the Mantis procedures. As part of the efforts to streamline Mantis procedures, DOS created a special Mantis team of five full-time employees in the VO, exclusively dedicated to technology transfer cases.[47] In addition to creating a special Mantis team and developing an electronic system, DOS, DHS, and the FBI also took other action to improve the Mantis program, in response to the GAO's suggestions in February 2004. These steps include providing additional guidance and feedback to consular posts; clarifying the roles and responsibilities of agencies involved in the Mantis process, reiterating DOS's policy of giving students and scholars priority in scheduling of interview appointments and extensions in the validity of Mantis clearances.[48] All of these initiatives resulted in a decline in Mantis processing times.

However, according to the most recent GAO Report released in February 2005, some issues still remain.[49] Consular officers at key posts continue to have questions about how to identify applicants and apply Mantis SAOs. [50] The

[43] The GAO found that visas for science students and scholars took on average, 67 days from the date the SAO was submitted from post to the date DOS sent a response to the post. Furthermore, the GAO also found that as of October 1, 2003, 410 Visa Mantis cases submitted by seven posts in FY 2003 were still pending after more than 60 days. In the sample, the GAO found that 67 of the visa applications completed processing and approval by December 23, 2002. In addition, three of the 67 applications had processing times in excess of 180 days. Four of the 71 sample cases remained pending as of December 3, 2003—of which three had been pending for more than 150 days and one for more than 240 days. *Id.* at 10–11. Based on the 5,000 SAOs received from consular posts between April and June 2003, 2,888 pertained to science students and scholars, approximately 58 percent were from China, 20 percent from Russia and less than two percent from India. Of the 2,888 Visas Mantis cases identified during the sample time frame between April and June 2003, a total of 57 posts sent one or more Mantis SAOs to Washington D.C. China accounted for 1762 SAOs (Shanghai sent 701; Beijing sent 600; Guangzhou sent 197; Chengdu sent 74; Shenyang sent 23; and Hong Kong sent 67 requests); Russia accounted for 567 SAO's (Moscow sent 505; St. Petersburg sent 37; Yekaterinburg sent 24; and Vladivostok sent one request). *See* Feb. 2004 GAO Report *supra* note 32 at Appendix II at 31. The GAO based its report on a random sample of 71 cases from the 2,888 applications to measure the length of time taken at selected points in the visa process. *Id.*

Moreover, according to the FBI, Mantis SAOs are the most difficult to resolve because of the predominance of requests from China and commonality of Asian names.

[44] *See* Oct. 2002 GAO Report *supra* note 18 at 10.

[45] When applications are lost, the most likely reason is due to cable formatting errors and duplicate cases that are rejected from the FBI database. Posts enter visa applicant information into the State's system, which then generates a Visas Mantis cable. If the post does not format the cable according to the standard State specifications, the FBI's system will not recognize the information in the cable. The improperly formatted cables are considered an error and the FBI asks DOS to resend the cable. *Id.* at 14.

[46] According to Feb. 2004 GAO Report, a Consular Affairs official stated that in fall 2003, there were about 700 Visas Mantis cases sent from Beijing that did not reach the FBI for the security check. The official did not know how the cases got lost but told the GAO that it took Consular Affairs about a month to identify that there was a problem and provide the FBI with the cases. As a result, several hundred visa applications were delayed for another month. *See supra* note 32 at 14.

[47] *See* Feb. 2005 GAO Report, *supra* note 36 at 11.

[48] More specifically, in 2004 alone, DOS added a special presentation on Visas Mantis to the NIV portion of the Basic Consular Training course; funded a trip by Nonproliferation and Consular Affairs officials to a regional conference in China to make presentations and hold discussions with consular officers on specific Mantis issues; organized a series of video-teleconferences with posts that submit large numbers to Mantis SAOs to provide direct feedback to embassy and consular officers on the quality of their Mantis requests; began issuing reports to the field about Mantis policy and procedural issues to "help consular officers understand the Mantis program better, provide guidance on what cases should be submitted as Visas Mantis SAO requests and what information should be included in those requests, and to give feedback on the quality of those requests." The first quarterly report was issued in March 2004, followed by two or more in July and October. DOS also arranged one-on-one meetings with the CA and NP officers for new junior officers assigned to posts with high Mantis volumes; provided feedback to individual consular officers on the Mantis SAOs submitted; and established a classified webpage through the DOS's intranet for consular officers to gain access to country-specific and other useful information related to the Mantis program. *Id.* at 11–12.

[49] *Id.*

[50] Despite DOS's efforts, the GAO found that consular officers at key posts still need additional guidance. Some consular officers are still confused about how to apply the Mantis program. Officers in Beijing consistently told the GAO that they needed more clarity and guidance regarding how to use TAL. According to a key official in Beijing, because these officers do not have scientific or technical backgrounds, they often do not understand what entries on the TAL mean or whether the visa applicant has advanced knowledge about the subject he or she plans to study in the United States. They are also confused about how to apply vague, seem-

continued

GAO also found that many posts are still not fully connected to DOS's electronic tracking system. As a result, consular officers still send Mantis cases both electronically and via cable, and some agencies still provide their responses via courier, leading to unnecessary delays.[51]

Based on its findings, the GAO recommended that DOS in coordination with DHS, develop a formal timeframe to complete full connectivity between all necessary U.S. agencies and bureaus; provide additional opportunities for consular officials at key posts to interact directly with DOS officials responsible for the Visas Mantis program (including more frequent video-teleconferences, mandatory one-on-one meetings with officials knowledgeable about the program and more visits by DOS officials to consular conferences).[52] According to DOS, they now have procedures for expediting individual cases when appropriate.[53]

DOS reports that the average processing time for Mantis checks as of March 2007, is approximately 16 days, which is significantly faster than the four–six month backlog experienced by many in the past.[54] At any given moment, DOS has approximately 1,500–2,000 Mantis checks pending from the interagency review process.[55] Consular posts may not issue the visa until they receive an affirmative response from all participating agencies, except the FBI. However, if a security check has been pending for over 45 days, counsel may call the VO public inquiries number at (202) 663-1225 or fax (202) 663-3899 or send an e-mail inquiry to *legalnet@state.gov*.[56]

Validity of Visas Mantis Clearances Extended

On February 11, 2005, after extensive interagency consultation with DHS, DOS extended the maximum validity of the Visas Mantis clearances for F-1, J-1, H-1B, L-1, O-1, and B-1/B-2 visas.[57] This allows applicants to

ingly benign categories (*e.g.*, consular officers in Beijing did not know whether to continue submitting Mantis requests for all individuals that fall under the category of "communications—wireless systems, advanced," even if the visa applicant works for a foreign multinational corporation that is not a Chinese government owned telecom enterprise. Few of the consular officers that the GAO spoke to in China, Russia, and the Ukraine were familiar with the quarterly reports issued by Consular Affairs on Mantis issues. The only officer aware of the classified webpage maintained by the Consular Affairs Bureau told the GAO that he did not find it useful because it had very little information on it and because it was hard to access the classified computer, which was housed in a separate building from the consular section. The GAO also found that consular officers at the three posts did not have regular opportunities to interact with officials from the NP Bureau or the CA Bureau knowledgeable about the Mantis program. Although China accounts for more than half of the Mantis requests, only one of the six posts has held a video-teleconference. Kiev requested a video-teleconference in early 2004, but had been unable to schedule one, as of December 2004. Finally, in Beijing, only one of the officers who had attended the consular conference was still at the post.) *Id.* at 16–18.

[51] Several law enforcement, intelligence and nonintelligence agencies that receive Mantis cases, including the Departments of Commerce and Treasury, are not fully connected to DOS's electronic tracking system. These agencies thus continue to receive Mantis cases through State's traditional cabling system. For the time being, officers send Mantis cases both electronically and via cable. The agencies that are responsible for routinely clearing Mantis checks provide their responses to DOS on CDs that must be hand-carried between the agencies, leading to further delays. DOS is working to establish full connectivity with other agencies, however, it has thus far failed to set a deadline for connectivity. In July 2004, DOS stated that it expected the FBI to begin relying on the network on a regular basis by the end of July 2004. DOS and the FBI also signed a Memorandum of Understanding (MOU) in July, outlining the terms of the FBI's electronic connectivity to the system. However, it was not until December 2004 that the FBI developed the ability to gain access to DOS's electronic tracking system to test the connection and discontinue use of the cabling system. Although the FBI no longer routinely clears Mantis cases, all agencies and bureaus that receive Mantis cases, regardless of whether they routinely clear cases, must be connected electronically to the system before use of the cabling system can be eliminated. *See* Feb 2005 GAO Report, *supra* note 36 at 17–18. While DOS hoped to achieve full interconnectivity between DHS and CIA by the end of December 2005, it is now scheduled for late spring 2006. *See* "DOS Answers to AILA's Questions," (Mar. 23, 2006) *supra* note 13.

[52] *See* Feb. 2005 GAO Report, *supra* note 36 at 20.

[53] *See* Testimony of Janice L. Jacobs (Feb. 25, 2004), *supra* note 35. Prior to this testimony, DOS has always maintained that there are no procedures in place to expedite a Mantis SAO. The author is not yet aware of the specific procedures available to request an expedite.

[54] In spring 2003, it took an average of 67 days for Mantis SAO processing. Due to further restructuring of the Mantis process, as of the beginning of September 2004, 98 percent of Mantis SAOs were processed within 30 days of receipt, enabling DOS to clear a backlog of some 2,000 cases. *See* Op Ed by Assistant Secretary of State for Consular Affairs, Maura Harty, *Chronicle of Higher Education*, Vol. 51, Issue 7 at B10 (Oct. 8, 2004). *See also* Feb. 2005 GAO Report, *supra* note 36 at 2. Data also shows a significant improvement in the number of Mantis cases pending for more than 60 days. In February 2004, the GAO found that 410 Mantis cases submitted by seven posts in China, India, and Russia had been pending for more than 60 days. Recent data provided by DOS indicates that as of October 2004, only 63 cases (or nine percent of all pending Mantis cases) had been pending for more than 60 days. *Id.* at 7–8. In December 2004, only 81 cases out of more than 18,000 had been pending for more than 30 days. *See* "Student and Exchange Visa Improvements," released by DOS as part of "DOS Answers to AILA's Questions," (Mar. 17, 2005), *supra* note 15.

[55] *See* Statement of Janice L. Jacobs, Deputy Assistant Secretary for Visa Services, Department of State before the Committee on House Small Business on "The Visa Approval Backlog and its Impact on American Small Business," Jun. 4, 2003, *at www.travel.state.gov/testimony3.html*.

[56] *See* "DOS Answers to AILA's Questions," (Oct. 2005) *supra* note 15.

[57] *See* "Some Visas Mantis Clearances Extended," *published on* AILA InfoNet at Doc. No. 05021460 (*posted* Feb. 14, 2005).

re-apply for visas without undergoing frequent Mantis checks, if returning to the previous program of study or professional assignment. However, consular officers have discretion, if warranted to initiate a Mantis SAO.

The validity period for F-1 applicants is up to the length of the academic program, to a maximum of four years. However, if the student changes programs, the clearance is no longer valid and a SAO will be initiated if the applicant applies for a new visa. H-1B, J-1, and L-1 applicants are eligible for clearances valid for the duration of their approved activity to a maximum of two years. If the nature of the foreign national's activities change, the clearance ceases to be valid and a new SAO is required.

B-1/B-2 applicants can receive a Mantis clearance valid for one year, provided that that the original purpose for travel, as stated in the visa application has not changed on subsequent trips.

The new clearance validity periods do not apply to applicants from state sponsors of terrorism.

These extended validities apply to any applicants who are re-applying for a visa within 12 months of the previously issued visa. DOS estimates that this change will allow the agency to cut in half the total number of Mantis clearances processed each year.[58] As before, consular officers may issue visas to applicants who have received Mantis clearance according to the applicant's reciprocity table, but in no case for longer than 12 months.[59] Visas for Chinese and Russian Mantis applicants, which account for approximately 76 percent of all Mantis cases,[60] can only be issued as single-entry visas valid for three months.[61]

Documents an Applicant Should Bring to an Interview

Applicants involved in any activities that have potential "dual use" applications should carry a detailed letter from their employer, explaining the nature of the work, specific job duties, project descriptions and if possible, details distinguishing how the work has no possible military applications. It is also helpful to provide recommendations from U.S. sources, documentation to show that the information is in the public domain or found in academic courses (where applicable).

If a company has an export license, it is sometimes helpful to bring a copy of the license as well. However, the existence of an export license does not eliminate or replace the need for a Mantis SAO if necessary.[62]

It also appears that many NIV applicants who are subjected to a Mantis security check are now considered "persons of interest" when they arrive in the United States. There have been numerous anecdotal reports that the FBI has made follow-up visits to universities, as well as private companies to check up on such individuals to ensure that they are in full compliance with the terms of their nonimmigrant status.

DOS IMPROVEMENTS TO THE SAO PROCESS

Based on the widespread problems encountered by participating government agencies in performing the various security checks, DOS made major changes in its use of electronic processing by developing a cable-less SAO process called the SAO Improvement Project (SAO IP).[63]

---

[58] *See* Feb. 2005 GAO Report, *supra* note 36 at 16. The new validity periods are the result of negotiations between State, DHS, and the FBI. Although DOS and DHS proposed extending Mantis clearances in the summer of 2004, the FBI argued that an extension in Mantis clearances would significantly reduce its capability to track and investigate individuals subject to the Mantis program. The FBI maintained that without the same frequency of automatic Mantis notifications, it would have far less knowledge of when these individuals entered the country, where they go, and what they are supposed to do while in the United States. As a result, the FBI made its agreement conditional on receiving access to US-VISIT and SEVIS. In February 2005, the FBI and DHS reached agreement on the terms of FBI's access to these two systems, allowing the proposed extension of Mantis clearances to take effect. *Id.* at 16.

[59] *See* "Mantis Clearances Valid for 12 months," *published on* AILA InfoNet at Doc. No. 03121143 (*posted* Dec. 11, 2003); *see also* "DOS Answers to AILA's Questions," (Mar. 17, 2005), *supra* note 15.

[60] China has one of the strictest visa reciprocity schedules for students and scholars. F-1 and J-1 applicants are limited to six-month, two-entry visas. However, DOS instructions to consular officers are to give single-entry, three-month visas to applicants who undergo Mantis checks. In 2004, DOS entered negotiations with Chinese government to revise the reciprocity schedule for business travelers, tourists and students. However, in December, DOS informed the GAO that while the Chinese government agreed to extend visa validities for business travelers and tourists, it did not agree to do so for students and scholars. *See* Feb. 2005 GAO Report, *supra* note 36 at 10.

continued

[61] *See* "DOS Answers to AILA Questions" *published on* AILA InfoNet at Doc. No. 04042164 (*posted* Apr. 21, 2004).

[62] The provisions at 9 FAM §40.31 N5.1-1(2) state that "if an applicant for a visa plans to export equipment or information on [the TAL] from the United States to any country without proof that a competent U.S. governmental authority has already approved an export license, the post should suspend processing, deny the application under §221(g) and submit a SAO to the department." According to DOS, the existence of such a license does not mean that an applicant is not subject to TAL and not subject to an SAO. It is still possible that the applicant, himself, is of concern on national security grounds. *See* "DOS Answers AILA Questions," *published on* AILA InfoNet at Doc. No. 04120760 (*posted* Dec. 7, 2004).

[63] Testimony by Janice L. Jacobs (Feb. 25, 2004), at *supra* note 35. In addition, DOS has also established a quality-control procedure with the Non-Proliferation Bureau (NP Bureau) to provide VO with feedback for posts regarding the information contained in Visas Mantis cables. The NP Bureau has started identifying cables that they have found well-prepared and contain all of the pertinent information NP analysts need to make an informed recommendation on visa eligibility. The NP Bureau also points out cables that do not contain sufficient information on which to reach a recommendation.

continued

DOS spent $1 million providing electronic inter-agency linkage aimed at improving efficiency between inter-agency processing. This includes the elimination of its traditional cabling system between consular posts and other federal government agencies in the SAO process.[64] The program uses real-time data-sharing, allowing for seamless electronic data transmission from posts, eliminating virtually all manual manipulation of data.[65] The other agencies will no longer receive a telegram (which is prone to cable formatting errors and misplacement of SAO requests), but a reliable data transmission through an interoperable network that begins with the CCD, which is expected to improve data integrity, accountability of responses in specific cases and statistical reporting.[66] DOS hopes that posts will be able to forward cases to intelligence and law enforcement agencies as quickly as possible and eliminate any time period that a case awaits processing by administrative staff. As of October 2004, DOS completed worldwide implementation of the SAO IP.[67] The SAO IP will operate through an interagency network known as the Open Source Information System (OSIS), which will provide interoperable data transmission.[68] Following initial interconnectivity problems between the FBI and DOS databases, the FBI is finally performing all name checks electronically through the CCD.[69] Efforts to improve connectivity with DHS and the CIA are continuing and expect to be fully connected by late spring 2006. Full connectivity by all government agencies will allow for shorter processing times and the ability to track cases and keep more accurate statistics.[70]

VISA RESTRICTIONS FOR CITIZENS AND NATIONALS OF STATE SPONSORS OF TERRORISM

Section 306 of the Border Security Act restricts the issuance of nonimmigrant visas to aliens who are nationals of countries that are state sponsors of terrorism—the so-called "Terrible 5" countries—unless clearance is provided by the Secretary of State in consultation with the Attorney General and other relevant agencies that determine that the foreign national poses no safety or security threat to the United States.[71] This provision formalizes the existing procedures and screening process, known as "Falcon" security checks, for individuals from these seven countries.

Biometric Technologies

Section 303 of the Border Security Act mandated the use of biometric identifiers in all U.S. visas by October 26, 2004.[72] A biometric or biometric identifier is an objective measurement of a physical characteristic or personal behavior trait of an individual, which when captured in a database, can be used to verify identity or check against other entries in a database. Some examples of features that can be measured for these purposes include the face, fingerprints, hand geometry, handwriting, iris, retina, and voice.

DOS, in conjunction with DHS, DOJ, and the National Institute of Standards and Technology (NIST) studied the potential of biometric technologies in screening visa applicants and determined that the biometric identifier will consist of facial recognition (digital photographs) and fingerprint (two index fingerprints) technologies.[73]

It also calls to attention cables that have been submitted for applicants whose purpose of travel to the United States did not fall within the purview of the TAL. In all instances, NP's comments are passed on to the relevant post as a means of providing feedback and guidance to the post's officers. *See* Feb. 2004 GAO Report, *supra* note 32 at 44.

It is also providing expanded briefings on the Visas Mantis process to new consular officers at the National Foreign Affairs Training Center, including 12–15 hours of training devoted to the processing of SAOs, including Mantis. During this training, the NP Bureau, which reviews Mantis cases in the Department, briefs on the proliferation threat and the importance of the Mantis screening process. *Id.* at 25; *see also* Testimony by Janice L. Jacobs (Feb. 25, 2004), *supra* note 35.

Finally, DOS is also monitoring resource needs at posts. To alleviate staffing concerns, temporary adjudicating officers are sent to the posts as needed. DOS will also add an additional 80 officers in 2004. However, the decision to add these new officers was made before the August 2003 Personal Appearance Waiver (PAW) policy and thus it is unknown if there are enough resources for the task at hand. *See* Feb. 2004 GAO Report, *supra* note 32 at 24. Add to this the implementation of the biometric visa program by October 26, 2004, which will undoubtedly overwhelm existing consular resources.

[64] *See* Testimony by Janice L. Jacobs, (Feb. 25, 2004), *supra* note 35.

[65] *Id.*

[66] *Id.* The SAO IP allows DOS to more easily produce and track certain statistics, including the average SAO processing times; the number of SAO's submitted by each post, and the amount of time each step in the process is staking. *See* Feb. 2005 GAO Report, *supra* note 36 at 13. As an added measure, the system also has a block built into it that prevents consular officers from resubmitting SAO requests on the same visa application. *Id.*

[67] It was hoped that the cables would be phased out by December 31, 2004, but it appears that some posts still continue to use cables. *See "*DOS Answers AILA Questions," *published on* AILA InfoNet at Doc. No. 04120760 (*posted* Dec. 7, 2004); *see also* *continued*

*"*DOS Answers to AILA's Questions," (Mar. 17, 2005), *supra* note 15.

[68] *See* Janice L. Jacobs testimony, (Feb. 25, 2004), *supra* note 35.

[69] *See "*DOS Answers to AILA's Questions," (Mar. 17, 2005), *supra* note 15.

[70] *See* "DOS Answers to AILA's Questions," (Mar. 23, 2006) *supra* note 13.

[71] *See* Border Security Act, *supra* note 2, §306.

[72] *See* Border Security Act, *supra* note 2.

[73] *See* "DOS Answers to AILA Questions," *published on* AILA InfoNet at Doc. No. 03102043 (*posted* Oct. 14, 2003).

These biometric identifiers can be used to conduct background checks and confirm the identity of visa applicants, and to ensure that an applicant has not received a visa under a different name.[74] The inclusion of biometric data in travel records will also make it easier to replace lost or stolen travel documents.

DOS completed deployment of the Biometric Visa Program ahead of schedule and before the congressionally mandated deadline of October 26, 2004. As of October 7, 2004, all 207 NIV issuing posts were collecting biometrics for NIV and all 125 IV issuing posts for immigrant and diversity visas.[75] There are limited exceptions to the fingerprinting requirement, which may only be waived in the case of a person traveling to the United States for medical treatment, who, due to a medical condition, is physically unable to appear at a post. There are absolutely no other individual waivers from fingerprinting although there are limited class exemptions.[76]

The inkless fingerprint scanning generally takes approximately 30 seconds.[77] As soon as the fingerprints are enrolled, they are sent electronically, along with the digital photograph and biographic data, to the CCD in Washington D.C. The CCD relays the fingerprint files to DHS's Automated Biometric Fingerprint Identification System (IDENT) system over a reliable, direct transmission line, which sends the results back to the CCD for relay back to the post.[78] The current turnaround time is approximately 30 minutes.[79]

IDENT searches for matches, triggering a response back to the post indicating a "hit" or no existing record (N/R). A "hit" means a person is on a watch list or that the person has been previously entered into the system, either at a port-of-entry or by applying for a visa at a consular post. If the fingerprints match fingerprints provided by the FBI in the IDENT lookout database, the IDENT system returns to the post an FBI file number.[80] At present, consular posts do not have access to the FBI record associated with that file number.[81] If there is no match in the IDENT system, then the visa applicant's fingerprints are stored in IDENT and a fingerprint identification number (FIN) is returned to the post.[82] If the system cannot determine whether the applicant's prints match a set previously entered, the system sends the data to biometric experts to determine if a subject's print has a match or that there is no record in the system.[83] Until the information from IDENT is received, the visa system is locked with regard to that visa application.

Once the visa has been issued, the NIV system sends to the DHS's Interagency Border Inspection System (IBIS) the issued visa data, including the visa applicant's photo and fingerprint identification number.[84]

DOS continues to examine ways to use the fingerprint biometric more efficiently, such that both DOS and DHS would not fingerprint and enroll people every time they apply for a visa or traveled.[85] DOS and DHS plan to cre-

---

[74] *Id.*; Consular posts are already electronically capturing photos of refused visa applicants. Prior to this, the department had only required posts to capture photos of applicants who had received a visa. *See* Feb. 2004 GAO Report, *supra* note 32, at 36.

[75] "Completion of Biometric Deployment" Cable, Oct. 8, 2004, *posted on ilw.com*. According to DOS, it had 3,567 hits in DHS's IDENT watchlist since it began biometric collection, almost all of which were for wanted persons for immigration violations, or for criminal history records submitted by the FBI. Of these 3,567 IDENT watchlist hits, 1,434 did not have a corresponding CLASS category one hit and 3,324 did not exactly match the applicant's name or date of birth in the NIV or IV system. *Id.*

[76] *See* "Waivers of Fingerprinting Under the BIOVISA Program," *published on* AILA InfoNet at Doc. No. 06011870 (*posted* Jan. 18, 2006). According to the DOS cable sent to the field, there are certain classes of exemptions for applicants with no hands, paralytics, burned fingers, one hand, permanent abnormal fingers, the elderly at the age of 80 years old and above and for certain classes of diplomats. However, an applicant with a cut on an index finger or a boil or a temporary condition on an index finger must be refused under §221(g) and told to return when the condition is healed and the finger can be printed. *Id.* In cases where the post has reason to suspect that an applicant has purposely damaged both index fingers, (*e.g.*, if both index fingerprints are burned, but there are no other such burns on the hands), the applicant must submit 10 fingerprints for clearance through the FBI. *Id.*

[77] *See* Statement by Assistant Secretary of State for Consular Affairs Maura Harty, Before the House Select Committee on Homeland Security, Subcommittee on Infrastructure and Border Security, Jan. 28, 2004, *available at http://travel.state.gov/MH01282004.html.*

[78] *Id.*

[79] *See* "Border Security: State Department Rollout of Biometric Visas on Schedule, But Guidance is Lagging," Report to the Chairman, Committee on Government Reform, House of Representatives (Sept. 2004) by the U.S. Government Accountability Office, at 4 (hereinafter "Sept. 2004 GAO Report." According to DOS data gathered from February to August 2004, the total biometric visa process averaged about 30 minutes for an applicant's prints to be sent from a consular post to the CCD, then on to IDENT analysis, and then for the response to be returned to the post. However if "human analysis" is required, DHS has up to 24 hours to provide a response back to the post. *Id.* at 7.

[80] *See* Testimony of Maura Harty, (Jan. 28, 2004), *supra* note 77.

[81] *Id.*

[82] *Id.*

[83] *See* Sept. 2004 GAO Report, *supra* note 79, at 5–6.

[84] *See* Testimony of Maura Harty, (Jan. 28, 2004), *supra* note 77.

[85] This information is based on comments made by Deputy Assistant Secretary Tony Edson at the October 2005 AILA/DOS Liaison meeting. However, it appears that this is what Secretary of State, Condoleezza Rice and Secretary of Homeland Security, Michael Chertoff in their Joint Vision statement, called the Global Enrollment Network—where DHS and DOS will align travel document application processes so that data need only be captured once from an applicant, whether the person is encountered first by DOS or DHS. This data could then be viewed by

continued

ate a Global Enrollment Network to achieve this, allowing DOS and DHS to verify a traveler's identity, citizenship and other information that helps to facilitate the admission process at the border.[86]

However, the fingerprint analysis is only the first step in the biometric program. DOS has now launched the initial phase of its facial recognition program, beginning with high-fraud posts. Facial recognition is being used for applicants who are currently not subject to biometric collection (*i.e.*, those under 14 years and over 79 years of age and diplomats), and also to any applicants from "Terrible 6" countries.[87] If there is a "hit," these checks will be performed by analysts at the Kentucky Consular Center (KCC), which is staffed to complete these checks within a 24-hour period. However, this has signaled the end of same-day processing for most posts, except in limited emergency situations.[88]

US-VISIT

The Biometric Visa Program, which is designed to deny U.S. visas to questionable travelers to prevent entry to the United States and to verify the identity of legitimate travelers who use visas to enter the United States, commences with consular posts abroad and complements and reinforces DHS' automated entry/exit system—the United States Visitor and Immigrant Status Indicator Technology program (US-VISIT), which was launched on January 5, 2004.[89] US-VISIT is designed to collect and share information on foreign nationals traveling to the United States, providing the government with capability to record the entry and exit of non–U.S. citizens into and out of the United States. Although the idea of the entry-exit program was introduced in 1996, the 9/11 terrorist acts accelerated its implementation and also introduced the concept of biometrics as the technology standard that would be used in the US-VISIT system. The overall implementation of US-VISIT calls for the collection of personal data, photos and fingerprints at consular posts abroad and at ports-of-entry, as well as extensive database and information sharing. It also provides officials with information about persons who are in the United States in violation of the terms of their admission to the United States.

Upon arrival in the United States, a foreign national who is subject to US-VISIT is inspected by Customs and Border Protection (CBP) inspectors at a port-of-entry. The individual's travel documents are scanned, a digital photograph and inkless fingerprints of both index fingers are taken.

If a foreign national has received a NIV from a post collecting biometrics, CBP inspectors will have access to three windows through the database. The first contains the same digital photograph that was taken as part of the initial visa application at a consular post and the CBP inspector is able to tell if the traveler has altered the photo on the visa. If the visa is a complete counterfeit, nothing will appear on the CBP inspector's screen. The second screen contains the biographic data and the third reflects if there is a fingerprint on file. If the applicant has been fingerprinted as part of the visa application process at a post abroad, the CBP officer will use the FIN to match the visa in the file with IDENT and will compare the visa holder's fingerprints with those on file. This one-to-one fingerprint comparison is designed to ensure that the person presenting the visa at the port-of-entry is the same person to whom the visa was issued. If there are no fingerprints in the database, the foreign national is enrolled in US-VISIT.[90] If the system shows a mismatch of fingerprints or a watch list hit, the foreign national is held for further screening or processing.

---

both DHS and DOS as appropriate, to verify a traveler's identity, citizenship, and other information that will help facilitate the admission process at the border. *See* Joint DOS/DHS Announcement on the Rice-Chertoff Joint Vision, *published on* AILA InfoNet at Doc. No. 06011860 (*posted* Jan. 18, 2006) (hereinafter "Rice-Chertoff Joint Vision: Secure Borders and Open Doors in the Information Age"). The Joint Vision statement has three main pillars which seek to: (1) use new information technology to renew America's welcome, making it as easy as possible for foreign visitors to travel to the United States and to do so securely and safely; (2) create travel documents for the 21st century, documents that can protect personal identity and expedite secure travel; and (3) to conduct smarter screening in every place that we encounter travelers, whether at a consulate abroad or at a port of entry into the United States. *See* "Chertoff/Rice Briefing on Secure Borders and Open Doors in the Information Age," *published on* AILA InfoNet at Doc. No. 06011861 (*posted* Jan. 18, 2006).

[86] *Id.*

[87] *See* "DOS Answers to AILA's Questions," (Mar. 17, 2005), *supra* note 15. The facial recognition program has been a great success in the DV lottery program context, where it has improved the DOS' ability to catch duplicate submissions and fraudulent entries. Over seven percent of "winning" entries were eliminated in the DV-2006 program through the use of facial recognition technology. *See* "DOS Answers to AILA's Questions," (Oct. 2005), *supra* note 15.

[88] Posts may compare the images themselves, but only in emergency situations.

[89] Effective January 5, 2004, US-VISIT is in effect at 115 airports and 14 seaports, and the 50 most highly trafficked land borders. The remaining 115 land borders were phased in by December 31, 2005. US-VISIT currently does not apply to U.S. citizens, lawful permanent residents, most Canadians, diplomats, children under the age of 14 and elderly over 79 years of age. Beginning September 30, 2004, visitors traveling from Visa Waiver Program countries will also be subject to US-VISIT at air and sea ports-of-entry. US-VISIT is separate from NSEERS and SEVIS. Those requirements remain unchanged.

[90] *See* Testimony of Maura Harty, (Jan. 28, 2004), *supra* note 77; Comments by Catherine Barry, Acting Deputy Assistant Secretary of State for Consular Affairs, DOS/AILA meeting on Mar. 4, 2004.

The US-VISIT enrollment process takes approximately 10–15 seconds.[91] The speed of this process is attributed to the fact that CBP officers only run a text-based name check at the time of admission. The IDENT security check, which is interfaced with the applicable biometric database, only occurs after the foreign national is admitted to the United States.[92] If CBP ran the IDENT checks during the admissions process, it would add approximately five minutes to every US-VISIT enrollment, which would wreak havoc at any port-of-entry.[93]

The individual's name is also checked against the IBIS database and the wants and warrants section of the NCIC database.[94] IBIS contains certain terrorist watch list information from the TIPOFF system maintained by DOS. Both the IBIS and NCIC checks are text-based checks and not biometric checks.[95]

DHS expects that US-VISIT will assist in combating fraud and protecting the integrity of the U.S. visa. However, questions remain regarding whether US-VISIT will really enhance the nation's security.[96] There are also several other concerns about how the US-VISIT program will operate. First, since the information for applicants enrolled under US-VISIT with no criminal record or apprehension record with USCIS or DHS are contained in the same database as the individuals for whom DHS is on the lookout, it will cause confusion for CBP inspectors who have to determine which individuals in IDENT are inadmissible to the United States and which have merely been enrolled in US-VISIT.[97]

There are additional concerns about the interoperability of the database systems. The notion of a comprehensive watch list database system is thoroughly dependent on the accuracy of the information in the database. The goal of IDENT and IAFIS interoperability is to allow the real-time exchange of biometric and biographic information between agencies that is complete, accurate and timely. Interoperability will ensure that federal, state and local law enforcement, authorized non-criminal justice agencies and immigration officials will have better information with which they can use to make decisions. Currently, the separate databases from the three immigration bureaus have not been fully integrated into US-VISIT.[98] Moreover, the system used by IDENT is based on a flat two-print. However, over the next few years, consular posts are required to go to a 10-print system based on the FBI's Integrated Automated Fingerprint Identification System (IAFIS),[99] which is based on a rolled 10-print

---

[91] *Id.*

[92] *Id.*

[93] *Id*; Each time a foreign national enters the United States, they still have to be "re-VISITed" upon each entry. Ideally, future travelers will be able to swipe their biometric passport or visa, provide index fingerprints and photograph, and have their identity checked against the US-VISIT database without any delays. The system would rely on US-VISIT to identify the individual and process the usual text-based IBIS database check. However, this procedure will not provide for a rapid biometric check against any criminal or other biometric watch list database. *Id.*

[94] *See also* Statement of Kathleen Campbell Walker on behalf of the American Immigration Lawyers Association and the Foreign Trade Association, Inc. of the Paso del Norte Region, "Integrity and Security at the Border: The US-VISIT Program" Before the Subcommittee on Infrastructure and Border Security of the Select Committee on Homeland Security on Jan. 28, 2004, *published on* AILA InfoNet at Doc. No. 04012940 (*posted* Jan. 29, 2004). CBP inspectors also have access to over 75 million visa records from the CCD allowing them to view the electronic files of every visaed individual entering the United States. The CCD permits examination of detailed information in near-real time on all visas issued, including the photographs of NIV applicants. The CCD is also shared with the National Targeting Center, a 24/7 operation of CBP. *See* Testimony of Assistant Secretary of State for Consular Affairs Maura Harty Before the National Commission on Terrorist Attacks Upon the United States, Jan. 26, 2004, *available at http://travel.state.gov/MH01262004.html.*

[95] *See* Statement by Kathleen Campbell Walker, *supra* note 94.

[96] A June 1998 Senate Judiciary Committee Report (Senate Judiciary Report 105-197 on S. 1360, Border Improvement and Immigration Act of 1997, June 1, 1998) had serious concerns about the utility of an entry-exit control system, commenting:

> The Committee is keenly aware that implementing an automated entry/exit control system has absolutely nothing to do with countering drug trafficking, and halting the entry of terrorists into the United States, or with any other illegal activity near the borders. An automated entry/exit system will at best provide information only on those who have overstayed their visas. Even if a vast database of millions of visa overstayers could be developed, this database will in no way provide information as to which individuals might be engaging in other unlawful activity. It will accordingly provide no assistance identifying terrorists, drug traffickers, or other criminals.

The report further states the following about tracking individuals who have overstayed:

> Even if a list of names and passport numbers of visa overstayers would be available, there would be no information as to where the individuals could be located. Even if there was information at the time of entry as to where an alien was expecting to go in the United States, it cannot be expected that six or more months later the alien would be at the same location. Particularly, if an alien were intending to overstay, it is likely that the alien would have provided only a temporary or false location as to where the alien was intending to go.

See Statement by Kathleen Campbell Walker, *supra* at note 94.

[97] *Id.*

[98] *Id.*

[99] IAFIS is the FBI's biometric database and it is maintained by the FBI's Criminal Justice Information Services (CJIS) division. The IAFIS is a ten-rolled fingerprint identification system that was deployed in 1999 and is used by federal, state and local law enforcement and authorized non-criminal justice agencies to identify subjects with a criminal history. It is the world's largest database with 400 million fingerprints, but takes approximately two hours to review electronically-submitted prints.

continued

fingerprint. Unfortunately, the two-versus 10-print baseline creates problems with false matches on print checks and does not interface well when the two-print IDENT print is run against the 10-print rolled IAFIS system.[100] Although behind schedule, the database integration program efforts continue between DHS and the FBI. In September 2006, DHS and the FBI made technology enhancements to these databases which provided immediate tangible benefits to federal, state and local law enforcement, non-criminal justice agencies, as well as consular officers and immigration officials. These technology enhancements represent the first in a series of three phases to achieve full interoperability between IDENT and IAFIS; an interim solution, initial operating capability (IOC) and full operating capability (FOC). These technology enhancements will further improve fingerprint-based access and sharing of criminal history information among immigration officials and will, for the first time, allow fingerprint-based access to immigration history information to state and local law enforcement and an authorized non-criminal justice agency.

The first phase consists of a pilot program, known as the interim data sharing model (iDSM). IDSM allows for two-way sharing of biometric and biographic information, including all IAFIS wants and warrants, expedited removals and visa applicants that the DOS has determined to be a substantial risk to enter the country and has denied issuance of a visa to that applicant (Category One refusals). The three agencies selected to pilot iDSM are the Boston Police Department, the Dallas County Sheriff's Department and the Office of Personnel Management. During the pilot, federal, state and local law enforcement, an authorized non-criminal agency will have fingerprint-based access to immigration history information and U.S. immigration officials will have fingerprint-based access to criminal history information in real time to make timelier and more informed decisions.

During the second phase of enhancements called IOC, DHS and the FBI plan to expand the categories of data shared and further enhance the infrastructure for data exchange and search capabilities between these two databases. During this phase in 2008, DHS' US-VISIT program will move from collecting two fingerprints to collecting 10 fingerprints, which will increase the accuracy in identity verification and will complement the IAFIS database. FOC or the third phase will provide additional data and further automate many of the processes.[101]

Moreover, DOS is planning 10-print pilots in San Salvador, London and Riyadh in FY 2006. DOS expects some deployment of 10-print capability to posts in the second half of FY 2007, depending on the ability of the DHS IDENT fingerprint system to be able to make effective use of 10-prints.[102]

Visa Waiver Country Applicants

Section 303(c) of the Border Security Act also contained a separate provision requiring the use of biometric identifiers for passports of applicants from Visa Waiver Program (VWP) countries. This biometric identifier requirement coincided with a second requirement that requires VWP travelers to present a machine-readable passport (MRP) when applying for visa-free entry into the United States after October 26, 2004.[103] It is important to note that the machine-readable passport requirement is a separate obligation to the biometric requirement.[104] Under the MRP requirement, a passport issued on or before October 25, 2004, will be valid for VWP entry to the United States after October 26, 2004, as long as it is machine-readable. If it is not machine-readable, the VWP traveler must obtain a nonimmigrant visa.[105]

With respect to the biometric identifier requirement, the International Civil Aviation Organization (ICAO)[106] determined that facial recognition, in the form of a facial image stored in a contactless chip embedded in passports as the preferred biometric identifier. The original deadline of October 26, 2004, mandated that VWP countries establish a program to issue ICAO-compliant passports by that date, such that travelers from VWP countries, whose passports are issued on or after October 26, 2004, must present a machine-readable passport with the appropriate biometric identifier or must otherwise apply for a NIV at a consular post in order to enter the United States after October 26, 2004. Although all VWP countries made varying degrees

[100] *See* K. Walker, "One If By Land, and Two If By Sea …," in 22 *Immigration Law Today* 12 (Nov/Dec. 2003) at 14.

[101] *See* " IDENT and IAFIS Interoperability Fact Sheet," *published* on AILA InfoNet at Doc. No. 06110164 (Nov. 1, 2006).

[102] *See* "DOS Answers to AILA's Questions," (Mar. 23 2006), *supra* note 13.

[103] After October 26, 2004, travelers from visa waiver program countries must present a tamper-resistant machine-readable passport at a U.S. port-of-entry to be admitted under the VWP program. These include Andorra, Australia, Austria, Brunei, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Japan, Liechtenstein, Luxembourg, Monaco, Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom.

[104] A machine-readable passport is one that can be "read" mechanically when swiped through a passport reader. It contains two lines of text on the bottom of the data page which, when read, populate the bio-data fields for consular officers or CBP officers. *See* "DOS Instructs on Machine-Readable and Biometric Requirements," *published on* AILA InfoNet at Doc. No. 04033166 (*posted* Mar. 31, 2004).

[105] After October 26, 2004, children who are included on parent's passports will not be permitted to enter the United States under the visa waiver program and must possess their own machine-readable passport to gain visa-free entry to the United States.

[106] ICAO is a specialized agency of the United Nations, founded to secure international cooperation and the highest possible degree of uniformity in regulations and standards, procedures, and organization regarding civil aviation matters.

of progress toward compliance with the requirement to have a program in place to issue biometric passports, only one or two countries would have had production capability in place by October 26, 2004.[107] Based on the continuing technical difficulties, legislation was signed to extend the deadline to October 26, 2005, to comply with the biometric identifier mandate. Therefore, machine-readable passports issued between October 26, 2005, and October 25, 2006, must contain a digital photograph printed on the biographical data page of the passport or an integrated chip with information from the data page. Machine-readable passports issued on or after October 26, 2006, must be e-passports (*i.e.*, have an integrated chip with information from the biographical data page).[108] Again, travelers who obtained machine-readable passports prior to October 26, 2005, are not required to have the digital photograph or contactless chip and may continue to use it until the passport expires.

WHERE CAN VISA APPLICANTS APPLY: ARE THE OPTIONS STILL THE SAME?

In the period since 9/11, DOS and many consular posts have streamlined the visa application process to accommodate enhanced security measures. The "zero-tolerance" attitude has softened somewhat, in part due to the enormous concerns of business, scientific and academic groups, and as a result of DOS's embracement of its "Secure Borders, Open Doors" policy.

Visa Revalidation through DOS

The requirement for use of biometric identifiers in visas by October 26, 2004, ultimately ended the visa revalidation program for E, H, L, I, O, and P applicants.[109] Thus, one of the most desirable options for foreign nationals previously issued certain NIV is no longer available.

Visa Applications in Applicant's Home Country—Mandatory Interviews Required

The October 2004 worldwide deployment of the Biometric Visa Program requires the physical presence of virtually all applicants at consular posts to comply with the fingerprinting and photo requirement. Thus, the Personal Appearance Waiver (PAW) policy introduced in July 2003 is no longer be applicable, except in limited circumstances.[110]

Third-Country National (TCN) Processing at Border Posts in Mexico and Canada

Consular processing at border posts in Canada and Mexico have undergone significant changes since 9/11. For now, TCN processing still remains a desirable avenue because of the proximity, speed, and the opportunity (depending on post policy) to have counsel present at interviews to explain complex elements of a case and to clarify issues that could otherwise result in a visa denial or even a petition revocation. The prevailing attitude in adjudications at both USCIS and DOS increases the need for attorney representation at the visa interview. Explanation and documentation of complex issues are important to avoid inconsistent decisions and random denials. Practitioners are advised to check this book and the individual border post's website to verify which categories of TCN's a post will accept for interview. Similarly, it is advisable to be aware of the post policy with regard to attorney representation.

The End of Same-Day Issuance?

With the implementation of the Biometric Visa program, particularly with the introduction of the facial recognition phase, border posts in Mexico and Canada are no longer able to provide same-day visa issuance.

Processing for "List of 26" and "T-5" nationals

Since 9/11, border posts generally do not accept applications from "List of 26" or "Terrible 5" countries, but some Canadian consular posts have accepted certain "List of 26" and "Terrible 6" applicants. However, such applicants cannot re-enter the United States until the security checks, if required, are complete and the visa is issued.[111] If granted an appointment to apply for a NIV in Canada or Mexico, the applicant must have permission to remain lawfully in Canada or Mexico, or have permission to le-

[107] None of the larger countries (Japan, the United Kingdom, France, Germany, Ireland, Italy, or Spain) would have been able to issue passports with the ICAO biometric by October 26, 2004. Japan and the United Kingdom anticipated that they could not begin until late 2005; others not until 2006. Most of these countries simply could not overcome the hard-technology hurdles of designing, testing, and rolling out biometric passports on a large scale. *See* Testimony of Maura Harty, (Jan. 28, 2004), *supra* note 77. Australia and New Zealand may make the October 26, 2004 deadline. Some countries have indicated that implementing a biometric program may have been possible by the deadline, but they are putting on the brakes because of questions of interoperability (can a U.S. POE scanner read a Danish biometric chip?) that remain unresolved. *See* "DOS Instructs on Machine-Readable and Biometric Requirements," *supra* note 103.

[108] *See www.travel.state.gov* for further information.

[109] Diplomatic and official visas (A, G, and NATO) will continue to be processed by the Visa Revalidation division.

[110] Visa applicants age 80 and over, and age 13 and under and diplomats are not subject to the biometric process and thus are still eligible for the PAW.

[111] Moreover, the Canadian posts have discretion to issue a two-entry visa if an applicant can demonstrate that his or her travels are part of a continuous transit. A two-entry visa allows the applicant to return to the United States after issuance of the NIV, depart the United States for the designated reason, and then return to the United States. For example, an Iranian physician could apply as a TCN applicant in Canada, return to the United States after issuance of the visa, depart the United States to attend a conference in Italy, and return to the United States after the conference. Comments of Leslie Gerson, Minister of Consular Affairs for Canada, ILW Teleconference, Consular Processing on Dec. 17, 2002.

gally enter and exit Canada or Mexico, during the entire duration of the processing period.[112] Thus, it appears that border posts may accept visa applications from "List of 26" and "Terrible 5" country applicants on a discretionary basis and have the ability to initiate all required security checks.

DOS Amendments to the Automatic Revalidation Provision of 22 CFR §42.112(d)

Effective April 1, 2002, DOS amended the provision for automatic revalidation of expired visas for nonimmigrant aliens[113] returning from short visits to contiguous territories[114] or adjacent islands.[115] Commonly referred to as the "contiguous territory" rule, the automatic revalidation provision allowed aliens who traveled outside of the United States for fewer than 30 days in a contiguous territory to re-enter the United States with an unexpired I-94 Arrival/Departure card. Therefore, an applicant with a USCIS approved extension of stay or change of status to another nonimmigrant visa category (except E-1/E-2), such as H-1B, L-1, or O-1, could be eligible for re-entry to the United States under the contiguous territory rule without having to obtain a new visa. Section 42.112(d) of 22 CFR also provided automatic revalidation to Fs and Js if they traveled to either a contiguous territory or an adjacent island, except Cuba.

In an effort to enhance security screening of visa applicants, DOS amended the automatic revalidation provision in two key ways. First, the automatic revalidation provision is no longer applicable to aliens who apply for *new* visas and are *refused* during visits to contiguous territories or adjacent islands. This change requires denied TCN visa applicants to depart directly to their home country or designated post to obtain a visa. Second, the ability to re-enter the United States without a valid visa is no longer available to aliens who are nationals of the "Terrible 6" countries, regardless of whether they apply for a NIV at a border post. These changes are designed to prevent these aliens from re-entering the United States prior to the completion of security checks.

The automatic revalidation provision may still be used by aliens to re-enter the United States after they travel to contiguous territories or adjacent islands provided the applicant does not apply for a new visa, and is not a national from one of the "Terrible 6" countries. However, based on anecdotal reports, aliens traveling to contiguous territories sometimes encounter problems. It appears that many airlines have been instructed by DHS officials to "lift" an alien's I-94 card, even if only traveling to Canada or Mexico. Practitioners should warn their clients that ensuring a safe return to the United States under the automatic revalidation rule requires that the alien retain the I-94 card. Unfortunately, some airlines will not permit a passenger to board a flight unless they turn over the original I-94 card. Some practitioners have been successful in providing photocopies to airlines while keeping the original. Unfortunately, the incidence of aliens who have turned over the valid I-94 and thus have been unable to take advantage of the automatic revalidation provision is on the rise.

The amendment to 22 CFR §41.112(d) severely impacted TCN processing by removing the "safety net" which allowed applicants to re-enter the United States even if unsuccessful in applying for a nonimmigrant visa at U.S. border posts in Canada and Mexico. This change to the automatic revalidation provision necessitates careful screening before applying for a visa at a border post. Unsuccessful TCN visa applicants at a border post must now depart directly from Mexico or Canada to their home countries. If the visa is not issued, such applicants are not permitted to re-enter the United States using an I-94 Arrival/Departure record from a USCIS change- or extension-of-status approval under the automatic revalidation provision. In limited cases where an applicant is applying for a "visa renewal" in the same category (H, L, E, O, or P), the applicant may re-enter the United States if there is time remaining on the existing NIV. In such cases, it may be prudent to apply for a visa prior to the expiration of the existing visa. Alternatively, if an applicant possesses a valid and unexpired visitor visa or is from a visa-waiver country, it may be possible to apply for re-admission at the discretion of the CBP port of entry.[116] During the "war" on terrorism it is unlikely that CBP will permit re-admission in visitor classification except in limited circumstances.

Since the rule came into effect, DOS has worked with USCIS to ensure effective enforcement at all ports of entry. The DOS cable to all diplomatic and consular posts announcing these changes provided detailed guidance regarding the handling of visa applications from aliens previously entitled to re-enter the United States from contiguous territories or adjacent islands based upon the

[112] *Id.*

[113] 68 Fed. Reg. 49351 (Aug. 18, 2003).

[114] The term "contiguous territories" refers to Canada and Mexico.

[115] The term "adjacent islands" refers to Anguilla, Antigua, Aruba, Bahamas, Barbados, Bermuda, Bonaire, British Virgin Islands, Cayman Islands, Cuba, Curacao, Dominica, Dominican Republic, Grenada, Guadeloupe, Haiti, Jamaica, Marie-Galante, Martinique, Miquelon, Montserrat, Saba, Saint-Barthelemy, Saint Christopher, Saint Eustatius, Saint Kitts-Nevis, Saint Lucia, Saint Maarten, Saint Martin, Saint Pierre, Saint Vincent and Grenadines, Trinidad and Tobago, Turks and Caicos Islands, and other British, French, and Netherlands territory or possessions bordering on the Caribbean Sea.

[116] However, if the consular officer determines that the alien is no longer entitled to the visa classification indicated on the visa (for example, based on INA §214(b)), and places an "application received" stamp next to the valid unexpired visa, USCIS will not permit re-admission. *See* "Further Instructions on Change to 41.112(d) Regarding Automatic Extension of Visas," *published on* AILA InfoNet at Doc. No. 02061947 (*posted* Jun. 19, 2002).

automatic revalidation provision. The DOS cable[117] urges posts to carefully follow procedural guidelines as outlined by 9 FAM §41.121 (requiring that passports are stamped with an "application received" notation when a visa is applied for but not immediately issued for any reason). As clarification, DOS similarly revised Note 4 to §41.112(d) to detail the precise procedures to be followed in the event of a visa refusal. These revisions include procedures that must be used to indicate refusals in passports—use of the "application received" stamp, where to place the stamp, and what details must be included within the stamp.[118] These measures are designed to ensure that inspectors can easily identify visa applicants who have been refused issuance of a nonimmigrant visa.

Therefore, while some border posts have limited the kinds of TCN applications they will accept, it still remains a valid option for many applicants.

Processing for Homeless Applicants

"Homeless" nonimmigrant visa applicants who have no U.S. embassy or consulate in their home country of nationality must file his or her NIV applications at a post designated by DOS.[119]

OTHER DEVELOPMENTS IN CONSULAR PROCESSING

Improved Dissemination of Information to the Public

In 2004, DOS redesigned its website at *www.travel.state.gov* as part of a concerted "user friendliness" outreach effort to make information about visas and processing times more accessible to the public. Posts individual websites are at *www.usembassy.state.gov,* while visa appointment waiting times and processing times can be found at *www.travel.state.gov/visa/tempvisitors_wait.php.* Based on ongoing problems with delays in scheduling timely visa appointment interviews, DOS has instructed all consular posts to post its criteria on obtaining emergency appointments on their respective websites.

The Future: A Paperless Visa Processing System

i) Electronic DS-156

Since November 2006, all applicants must complete the electronic version of the Form DS-156 (EVAF) when applying for a nonimmigrant visa. The EVAF generates a bar code on the application and is available at *https://evisaforms.state.gov/ds156.asp*, as well as on all post websites. The barcode allows posts to scan the information straight into the system, rather than manually inputting the 40+ data fields into the system, thereby reducing the risk of errors created by manual manipulation of the information into the system. DOS anticipates that the use of the electronic version will improve processing and issuance times. These improvements are supposed to pave the way for a "paperless visa processing" system.

ii) Online NIV Applications

DOS is currently exploring ways to make the NIV application entirely interactive - a "paperless" visa system where applicants can apply online and DOS can even perform SAO's ahead of time. DOS hopes to pilot a fully online NIV application this summer, whereby information entered by visa applicants will automatically upload into the NIV system. The hope is that this mechanism will allow DOS to conduct fraud checks and even SAO's in advance of the applicant's visa interview. However, this is in the very early stages of development and implementation. Online IV applications are expected to be more difficult as it requires coordination with USCIS.[120]

---

[117] *Id*.

[118] In order to prevent refused applicants (including those subject to mandatory waiting periods, SAO checks, etc.) from attempting to reenter the United States under the automatic revalidation provision, and in order to alert USCIS to such an attempt, consular officers have been instructed to collect any valid I-94, mark the back of the I-94 with the date and post name using the "application received" stamp, and return the I-94 to USCIS. If there is a USCIS office at the post, the I-94 must be turned over to that office. In other cases, the form must be sent to ACS-USCIS, P.O. Box 7125, London, KY 40753 when using the U.S. mail or pouch or to ACS-USCIS, 1084 South Laurel Road, London, KY 40744 when using another delivery method.

If the consular officer is unable to retrieve the I-94 because the applicant claims it is lost or stolen or turned in to USCIS, the consular officer is required to place the "application received" stamp next to the expired visa, or in the case of a prior change of status, next to the unexpired visa in the different category that might otherwise be erroneously converted and revalidated if the USCIS officer were unaware of the alien's intervening visa application. This stamp is in addition to the stamp that is placed in the back of the passport as is required for all visa refusals. In cases where an applicant possesses a valid visa, consular officers have been instructed that the visa should not be revoked unless the consular officer determines either that the alien is no longer entitled to the visa classification indicated on the visa (this would include aliens in possession of valid B visas who are no longer qualified under §214(b), or that alien is ineligible under §212(a)) or some other legal ground of visa ineligibility. *Id.*

[119] Currently, the designated consular posts for homeless applicants who have no embassy/consulate in their home country are as follows: Afghanis must apply in Islamabad (Pakistan); Bosnians in Sarajevo (Bosnia-Herzegovina); Iranians in Abu Dhabi (United Arab Emirates), Ankara (Turkey), Frankfurt, Germany (family-based applicants only), Vienna (Austria), or Naples (Italy); Iraqis *continued* in Amman (Jordan) or Casablanca (Morocco); Lebanese in Abu Dhabi (United Arab Emirates), Damascus (Syria), Nicosia (Cyprus), Tel Aviv (Israel), or Beirut (Lebanon) (for revalidations and special cases); Libyans in Tunis (Tunisia); Somalis in Nairobi (Kenya), Dar Es Salaam (Tanzania),or Djibouti (Djibouti); and Sudanese in Cairo (Egypt) (although this is expected to be a temporary designation for Sudanese until the U.S. Embassy in Khartoum resumes to normal operation).

[120] *See* "AILA/DOS Liaison Meeting Minutes," (Mar. 2007) *to be published on* AILA InfoNet.

iii) Implementation of Worldwide Web-Based Appointment System

DOS is currently working on piloting a web-based appointment system that would be available for global use through a single Internet portal. It expects to pilot the program with the embassy in Kingston, Jamaica in April 2006. If successful, it will migrate at the remaining posts currently being supported by Hong Kong. At the same time, all other posts will be invited to begin using the centrally hosted appointment system.[121]

iv) Video Conferencing Technology

DOS is testing a digital videoconferencing project to see how it can make the visa interview process easier for those who currently need to travel great distances for a visa interview. In some countries, bottlenecks may arise from the need for applicants to go the only, or one of the few, consular posts in their country for the visa interview. A pilot program will be conducted between Belfast and London in the third quarter of 2006.[122]

v) Fingerprint Collection

In FY 2006, DOS tested several methods to remotely collect fingerprints and capture data for the NIV form from applicants with special needs. DOS piloted a method whereby an officer can collect fingerprints offsite using a laptop. However, DOS determined that such applicants would have to pay an additional fee. Until DOS can establish the cost of that service, it will not be made available for group processing. Even once a fee is established, it would be limited to pre-select groups of applicants, not available on a single case request basis and only on referral from DOS.[123]

Finally, DOS is planning to require all posts to collect ten fingerprints from visa applicants by the end of FY 2007. As part of this process, it is currently exploring whether the ten prints can be collected by a third party, such as a bank and then verified by a consular officer at the post.[124]

DOS/DHS Advisory Board in Partnership with the Private Sector

DOS and DHS plan to have an enhanced partnership with the private sector by creating an advisory board to provide regular, institutional outreach with tourism, business and academic communities to consider their views and to identify "best practices" when developing travel policies. The goal is to have the advisory board provide feedback on specific initiatives and serve as a reliable sounding board for innovative travel facilitation and security-related programs.[125]

Interagency Panel on Advanced Science and Security

The White House Office of Science and Technology Policy (OSTP) has been working on implementing an enhanced mechanism for visa review in sensitive areas of science and technology, to be conducted by the Interagency Panel on Advanced Science and Security (IPASS). The IPASS process is designed to increase the involvement of U.S. government scientific experts to work with the intelligence, counterintelligence and law enforcement representatives to advise DOS of science-related visa applications. Once IPASS is formally established, it will determine what constitutes "uniquely available sensitive scientific research and technology development" and put in place procedures for reviewing and issuing advisory opinions on applicable F and J visa applications that fall within these categories. The IPASS proposal has been under review by the DHS.

Student and Scholar Visa Applications Given a Priority

In response to serious concerns by academic and scientific groups that U.S. policies have discouraged foreign students and exchange visitors from choosing the United States to study or conduct research, DOS has made student and scholar visa applications a priority every year.[126]

---

[121] *See* "DOS Answers to AILA's Questions," (Mar. 23, 2006), *supra* note 13.

[122] During this pilot, participation of visa applicants will be voluntary and visas will not be adjudicated over videoconferencing. Rather, test visa interviews will be conducted on visa applicants in Belfast whose visas have already been adjudicated. The interviews will be conducted by consular officers in London via videoconferencing in order to test the possibilities of using this technology in real visa interviews. *See "*DOS Answers to AILA's Questions," (Mar. 23, 2006), *supra* note 13 and *see also* "Rice-Chertoff Joint Vision: Secure Borders and Open Doors in the Information Age," *supra* note 85.

[123] *See* "AILA/DOS Liaison Meeting Minutes,"(Mar. 2007) *to be published on* AILA InfoNet

[124] *Id.*

[125] *Id.*

[126] Foreign students contribute $13 billion annually to the U.S. economy, but numerous reports confirm that American universities are facing intense competition. Some of the decline is in part due to aggressive recruitment efforts by competing countries such as Australia, the United Kingdom, Ireland, New Zealand, and Canada. However, many blame the decline to post-9/11 delays in visa processing. Foreign applications to U.S. graduate schools declined 28 percent in 2004, while actual foreign graduate student enrollments dropped 6 percent. Enrollments of all foreign students, in undergraduate, graduate and postdoctoral programs fell for the first time since 1972. Chinese and Indian students represent the largest proportion of students in the United States (in 2004, about 80,000 Indian students and 62,000 Chinese students). Yet, statistics show that Indian graduate school applications were down 28 percent, while Chinese graduate school applications declined by 45 percent in 2004. *See* Dillon, S., "U.S. Slips in Attracting the World's Best Students," *The New York Times*, Dec. 21, 2004; "The United States Earns More From International Student Fees Than From Weapons

continued

Since 2003, each spring, DOS sends a cable reminding posts that they should give priority scheduling to F, J and M visa applicants by having clear, well-publicized procedures in place for obtaining priority appointments.[127] DOS has successfully implemented this requirement in different ways, such that 97 percent of student visa applications are processed in one or two days.[128]

Kentucky Consular Center

As of July 6, 2004, USCIS began sending all approved I-129 petitions (except I-129F petitions) to the Kentucky Consular Center (KCC), rather than sending them directly to the overseas visa processing post.[129] Initially, KCC will scan the petition and transmit it electronically to post (in the form of an adobe acrobat document) Eventually, the I-129 petition information will be made accessible to posts via the CCD and DOS hopes that centralizing processing at KCC will bring uniformity and consistency to the visa application process.[130] KCC will only transmit approved I-129 petitions. Other documentation associated with the case will be scanned and sent to post on an "as-needed" basis, per request from post. It is hoped that once DHS is able to electronically share petition data through the CCD, all posts will begin to issue a NIV without requiring an original I-797 Approval Notice.

The Homeland Security Act of 2002 and the Memorandum of Understanding (MOU)

The passage of the Homeland Security Act of 2002[131] radically altered U.S. visa operations by transferring the function from DOS to DHS, effectively stripping DOS of most of its visa issuing functions.

The Memorandum of Understanding (MOU), the agreement between DOS and DHS governing the implementation of Section 428, was released and became effective on September 30, 2003.[132] As expected, the MOU transfers virtually all of the visa functions from DOS to DHS, with some limited exceptions. According to the MOU, DHS will establish visa policy and review implementation of that policy. While DOS may propose and issue visa guidance, it is subject to DHS consultation and final approval. Of particular interest to DHS is the final responsibility over visa guidance (as it relates to regulations, FAM, cables implementing the provisions of the INA or other immigration and nationality laws as it pertains to visas) concerning eligibility for nonimmigrant and immigrant classification, grounds of inadmissibility, waivers, determinations as to where aliens may apply for visas, personal appearance waivers, visa denials and persons from state sponsors of terrorism.

DHS also has the exclusive authority to administer, enforce, and issue regulations relating to functions of consular officers in the granting or refusal of visas. DHS is authorized to assign DHS employees to consular posts where visas are issued.[133] DHS employees may recommend to a consular officer that a visa be refused or revoked if it is deemed necessary or advisable in the foreign policy or security interests of the United States. However, if a supervisory consular officer or the chief of section does not agree that a visa should be refused or revoked, the post must initiate a request for a security or other advisory opinion.[134]

Additionally, section 429 of the Homeland Security Act requires that whenever a consular officer denies a visa to an applicant, the fact of the denial, the basis for such denial, and the name of the applicant are entered into the interagency electronic data system implemented under section 202 of the Border Security Act.[135] Under this provision, once a person is denied a visa, no subsequent visa

---

Exports," Progressive Policy Institute Trade Fact of the Week, Feb. 22, 2005.

[127] For the latest cable, *see* "DOS Reminds Posts to Prioritize Student Visas," *published on* AILA InfoNet at Doc. No. 04121563 (*posted* Dec. 15, 2004).

[128] *Id.*

[129] "USCIS Sending I-129s to Kentucky Consular Center Rather Than to Posts," *published on* AILA InfoNet at Doc. No. 04071264 (*posted* July 12, 2004).

[130] *Id.* A Fraud Prevention Unit will start up at KCC in the fall under the direction of an experienced consular officer. This unit will identify fraud indicators that posts will be able to investigate further during the visa adjudication process. Posts are encouraged to establish a dedicated e-mail address to receive NIV petitions in order to ensure efficient transmission of data. All posts, whether establishing a dedicated e-mail address or not, are requested to send to KCC an e-mail address where they would like petitions to be sent. *Id.*

[131] *See* Homeland Security Act, *supra* note 3.

[132] 68 Fed. Reg. 56519 (Sept. 30, 2003); "U.S. Department of State, Homeland Security Reach Agreement on Visa Oversight Rules," *published on* AILA InfoNet at Doc. No. 0309012 (*posted* Sept. 30, 2003).

[133] Employees of DHS who are assigned overseas shall perform the following functions: (A) Provide expert advice and training to consular officers regarding specific security threats relating to the adjudication of individual visa applications or classes of applications; (B) Review any such applications, either on the initiative of the employee of the Department or upon request by a consular officer or other person charged with adjudicating such application; and (C) Conduct investigations with respect to consular matters under the jurisdiction of the Secretary of Homeland Defense. *See* Homeland Security Act, *supra* note 3; "U.S. Departments of State, Homeland Security Reach Agreement on Visa Oversight Rules," *supra* note 130. DHS officials have been in place at posts in Jeddah and Riyadh, Saudi Arabia since August 31, where they review *all* nonimmigrant and immigrant visa applications. DHS expects to place additional officials in regional hubs, including at posts in Casablanca, Morocco; Jakarta, Indonesia; Abu Dhabi, United Arab Emirates; Cairo, Egypt; and Singapore.

[134] *Id.*

[135] *See* Homeland Security Act, *supra* note 3.

may be issued to the person unless the consular officer considering it has reviewed the information concerning the person placed in the interoperable data system, has indicated on the person's application that the information has been reviewed, and has stated for the record why the visa is being issued or a waiver of visa ineligibility recommended in spite of that information.[136] The person may not be admitted to the United States without a visa issued in accordance with these procedures.[137]

As a practical matter, while DOS and DHS have consulted on some regulations, including the free-trade agreements visas for Chile, Singapore and Australia the effects of this restructuring are yet to be seen.

Enforcement of Export Control Regulations

As government agencies continue to implement increasingly sophisticated security measures to address national security concerns, enforcement to abate the unlawful transfer of sensitive technologies will undoubtedly increase. Already, government agencies are focusing on the activities of foreign nationals and consequently so-called "deemed exports."

When a company releases controlled technology to a foreign national during the course of employment, a "deemed export" occurs. The "deemed export" rule presumes that any technology released to a foreign national in the United States will be exported to a foreign national's home country. The reasoning behind the rule is that the uncontrolled release of technology to a foreign national in the United States could ultimately result in the dissemination of sensitive technologies and information to risky foreign governments, terrorist organizations or any other entities involved in activities contrary to our security and national interests. Once the technology is released, there is no way to "take it back."[138]

Therefore, when an applicant applies for a nonimmigrant visa at a consular post, in addition to a TAL Mantis check, the post may also initiate (or request the Department of Commerce to initiate) further checks to determine if an employer or alien is liable for an illegal technology transfer or failed to obtain the appropriate export-control license. Many are simply unaware of these "deemed export" requirements or the heavy penalties that are associated with such violations, which include civil, criminal and administrative penalties. Although export controls and immigration appear to be two distinct areas of law, the company which is investigated and sanctioned as a result of its failure to comply with export licensing provisions for its foreign nationals may not be aware of the overlapping issues. Therefore, it is critical to advise your client of the potential export control issues and refer them to an export control specialist to ensure compliance.

In fact, anecdotal reports have already surfaced from virtually every industry from businesses to academic institutions concerning monitoring and requests for information on H-1B foreign nationals, inquiries about particular projects on which the individuals are working, spot checks of worksites, including interviews with employers and licensing checks and an increase in audits by a host of government agencies including USCIS, CBP, FBI, and the Bureau of Industry and Security (BIS), to name a few. These developments signal a shift in government priorities and immigration practitioners can be sure that these issues will affect their practice, particularly as statistics show that the number of U.S. students graduating in technology, engineering, and scientific fields continues to decline. This will only increase the reliance of U.S. companies and universities to focus on hiring foreign nationals in the workforce.

Moreover, the GAO performed a review of export controls and how the Department of Commerce controls transfers of technology to foreign nationals. This report is likely to serve as an additional impetus for increasing scrutiny of existing procedures and implementation of new procedures. The GAO report on export controls found several vulnerabilities in the Department of Commerce's deemed export control system, including the lack of a screening process for change-of-status applications submitted to USCIS from foreign nationals already in the United States, and the lack of an effective monitoring system.

The GAO report made specific recommendations that would include the use of all existing immigration data by the Commerce Department to identify foreign nationals who could be subject to deemed export licensing requirements; as well as coordination between USCIS and the Commerce Department to refer change-of-status applications involving employment that might result in access to sensitive technology.[139]

---

[136] *Id.*

[137] *Id.*

[138] It is critical to understand that although counterintuitive, export controls that relate to a physical export of the technology to a foreign country would also apply to the release of the technology *in* the United States to a foreign national of that country, because it is considered an "export" under applicable regulations.

[139] In 1999, Legacy INS extended the D/S period for F-1 and J-1 students (and their derivatives) who applied for change-of-status to H-1B but were subject to the H-1B cap and whose status expired prior to October 1. This became part of 8 CFR §214.2(f)(5)(vi) and §214.2(j)(1)(vi), but is discretionary. The extension allowed F's and J's to legally stay in the United States until October 1 without accruing unlawful presence, but did not allow the individual to commence employment for the H-1B employer until October 1. *See* Practice Advisory: Extension of Status for Certain F/J Students, *published on* AILA InfoNet at Doc. No. 04072362 (*posted* July 23, 2004). This discretionary provision was exercised again in 2000, but not in 2004, when the H-1B quota was reduced back to 65,000. According to USCIS officials at the AILA National Conference in Salt Lake City in June 2005, this provision was not invoked again in 2004 or 2005 because of concerns from the White House about the

continued

Based on the generally negative assessment of visa operations and export control vulnerabilities, DOS, DHS, and other federal agencies will undoubtedly continue to accelerate their efforts to streamline, develop and implement new polices and procedures that will enhance the effectiveness of the visa process against the backdrop of heightened security threats.

CONCLUSION

Security concerns are pivotal as the United States grapples with the dilemma of balancing legitimate international travel needs with the ever-present security risks facing the nation in the "war against terrorism." While globalization has increased the frequency and necessity of travel to the United States by foreign nationals, the minefield of immigration practice is now complicated by the increasing perils and complexity of consular practice. Knowledge of USCIS procedures is no longer sufficient to ensure visa issuance. Involvement with a visa case merely starts with the filing of a petition with USCIS and the issuance of an I-797 Notice of Action approval. Practicing immigration law now requires integral involvement and a thorough analysis of an alien's entire employment and immigration history all the way through to the final stages of the visa application process. To further complicate matters, the focus on foreign nationals and their activities has generated significant government investigation and enforcement of export control violations. Complete familiarity with nonimmigrant consular processing procedures and an in-depth understanding of the maze of security measures and related issues is vital to assisting clients in navigating the complex consular process. While DOS has softened its approach from a "zero-tolerance" policy to a more open, "Secure Borders, Open Doors" policy, its attempts to balance national security concerns against legitimate travel needs still leaves visa applicants facing unpredictable delays and myriad dangers. While aimed at enhancing security, the rules, regulations, and procedures, increased scrutiny and the use of biometric collection and SAOs, the continuing commitment to database sharing between DOS, USCIS, and intelligence databases, and the unpredictable differences between consular posts, have dramatically changed the consular framework.

GLOSSARY OF TERMS

APIS (Advanced Passenger Information System): Biographical data from individuals' passports, visas, or other travel documents is collected by airlines and submitted electronically to U.S. Customs and Border Patrol (CBP) prior to an aircraft's arrival in the United States. The APIS also includes data on U.S. citizens, permanent residents, and Canadians. The information is checked against databases for information on criminal activity, terrorism, visa denials, and overstays. Although APIS commenced in 1989, the mandatory reporting requirement was implemented as part of the Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act).[140] The information that is transmitted through APIS feeds into the Arrival Departure Information System (ADIS) and supplements NIIS, which relies on matching I-94s and I-94Ws for overstays.

CCD (Consular Consolidated Database): This DOS database contains over 75 million visa applications, including information about applicants and indicates the outcome of any prior visa applications. Since February 2001, the CCD also stores photographs of applicants in electronic form and most recently, has started to store fingerprints. The CCD is available at ports-of-entry, allowing CBP to determine if passports or visas have been tampered with and modified. The CCD is also the mechanism through which government agencies, such as the FBI and CIA, perform SAOs. However, the FBI is currently the only agency that is connected to the CCD, although DOS is working on establishing connectivity with the remaining government agencies that are involved in the SAO process.

CHIMERA: The Border Security Act mandated that DHS integrate all its data systems into one system—an interoperable interagency system to be known as CHIMERA.[141] CHIMERA ties together DOS, intelligence agencies, the FBI, and local and state law enforcement databases. This system includes electronic sharing of visa files, including personal information, the applicant's home address, date of birth, passport number, and relatives' names; an integrated entry-exit system; machine-readable and tamper-proof visas and other travel documents; use of sophisticated technologies to run name checks using algorithms to account for variant spellings and the establishment of standard biometric identifiers for visa applicants.[142] CHIMERA also requires that airlines commence electronic transmission of passenger manifests to DHS, *i.e.*, APIS.

CLASS (Consular Lookout and Support System): The CLASS database is the principal lookout database used by DOS to check names and visa eligibility of applicants. A CLASS check is automatically performed on every visa applicant and a visa cannot be issued without the approving consular officer's confirmation that the name check is

lack of domestic security checks for sensitive technology transfers on change-of-status applications filed with USCIS.

[140] Enhanced Border Security and Visa Entry Reform Act of 2002, Pub. L. No. 107-173, 116 Stat. 543 (2002).

[141] Border Security Act §§202 and 203 relate to CHIMERA, while §201 includes the provision requiring database sharing between government agencies.

[142] There are three required biometric identifiers—fingerprints, face recognition, and a third yet to be chosen method. *See* R. Sindelar, "CHIMERA, NSEERS, Lookouts, and Security Checks: The New Age," 8 *Benders Immigr. Bull.* 105 (Jan. 15, 2003).

completed.[143] An individual's name in CLASS indicates that information exists that may be relevant to the application, *e.g.*, previous visa refusals. Records in CLASS are presented with name, date of birth, country of birth, nationality, and a code corresponding to the reason it was entered, including, among others, previous visa refusals, immigration violations, lost or stolen passports or visas, and terrorism.[144] Generally, visa refusals fall into two categories. A Category I refusal is one based on INA §§212(a)(1), (2), (3), (6), or (8), and a Category II refusal is one that can be overcome by additional evidence. A category I refusal must be entered in CLASS, as must any refusals under INA §214(b).[145]

The majority of information (61 percent) now in CLASS is derived from other agencies, including DOS, DHS, CIA, FBI, DEA, DOJ, Interpol, Customs, and other U.S. intelligence community sources.[146] DOS's CLASS and TIPOFF databases also interface with IBIS, TECS II, NAILS, and NIIS.

CLASS uses language algorithms, including Arabic and Russian/Slavic names to help increase the likelihood that the name check will find a person's name if it is in the database. In addition, DOS has an algorithm for Hispanic names, which is in the final stages of development, and DOS is considering the development of an East Asian algorithm.

IAFIS (Interagency Fingerprint Identification System): This FBI database was implemented in 1999. It is an automated 10-fingerprint matching system that contains in its Criminal Master File over 43 million sets of 10-print fingerprint records. IAFIS records can be electronically compared against submitted fingerprints, taking approximately two hours to review. When the FBI checks the criminal history of the individual, the fingerprints and results must be less than 15 months old.[147] The database may have local and state law enforcement information, and unless the CIA has a record of criminal history abroad, the check will not provide information relating to international criminal history.[148] IAFIS is the system through which consular posts electronically send the FBI 10-fingerprints when the system shows a NCIC hit.

IBIS (Interagency Border Inspection System): This DHS database is linked to the NCIC, CLASS, Bureau of Alcohol, Tobacco and Firearms database, Customs, NAILS, and TECS. IBIS checks are performed on all nonimmigrant and immigrant applications filed at USCIS service centers and are valid for 90 calendar days.[149] This means that an IBIS check need not be repeated as long as adjudication of the application or petition occurs within 90 days of the prior IBIS check. However, if at the time of adjudication, the record does not contain evidence of an IBIS check conducted within the preceding 90 days, a check must be completed and incorporated in the record.

IDENT (Automated Biometric Fingerprint Identification System): This is DHS's automated fingerprint system, which begin operating in 1994 and is separate from the FBI's automated fingerprint identification system—IAFIS. IDENT is the US-VISIT database that contains the biometric information of international travelers to the United States who are enrolled through DHS' US-VISIT program. To enroll an alien in IDENT, an alien's right and left index fingerprints are taken with a fingerprint scanner; a photograph is taken with the IDENT camera; and the alien's biographical information is input into the computer. IDENT then electronically compares the alien's fingerprints to fingerprints in two IDENT databases: (1) a "watchlist" fingerprints database that contains fingerprints and photographs of approximately one million aliens including immigration violators and a subset of the FBI's fingerprint database containing records of all known and suspected terrorists; selected wanted persons (foreign-born, unknown place of birth, individuals with felony convictions or previous criminal histories for high risk countries); DHS's ICE information on deported felons and sexual registrants; and DHS information on previous criminal histories; and (2) a "recidivist" database that contains fingerprints and photographs of persons entered into the system either at a port-of-entry or by applying for a visa at a consular post, including approximately six million illegal aliens who have been apprehended by DHS and enrolled in IDENT since it was deployed.[150]

---

[143] This is known as the Visa Lookout Accountability (VLA), which requires consular officers to certify in writing that they have checked the database prior to issuance of a visa.

[144] *See* "Visa Process Should be Strengthened as an Antiterrorism Tool," *supra* note 18.

[145] *See* W. Rosner & M. Ritter, "How To Find Out What Government Records Contain About Your Client," *Immigration & Nationality Law Handbook: Advanced* 47 (1998–99 ed.).

[146] *See* Testimony by Deputy Assistant Secretary of State for Consular Affairs, Janice L. Jacobs, Before the Senate Foreign Relations Committee, Oct. 23, 2003 at *http://travel.state.gov/testimony9.html*.

[147] *See* M. Lawler, "Security Checks Conducted by DHS/INS and DOS," in *Professionals: A Matter of Degree,* Fourth Ed. 60 (AILA 2003).

[148] *Id.*

[149] Prior to January 20, 2004, IBIS checks were valid for 35 calendar days. USCIS conducted a study to determine whether the validity period of IBIS checks could be extended to 60 days, 90 days, six months, or nine months, while maintaining the integrity of the checks and ensuring public safety and national security. Based on the results of that study, it was determined that the IBIS check validity period be increased to 90 days. *See* "IBIS Checks Valid for 90 Days," *published on* AILA InfoNet at Doc. No. 04063071 (*posted* June 30, 2004).

[150] *See* "State Department Rollout of Biometric Visas," *supra* note 79.

The IDENT database is supposed to interface with the FBI's IAFIS database, but has continued to encounter delays in implementation of the database integration program that will make IDENT and IAFIS interoperable.

"List of 26" countries: Although it is classified, the list of countries reportedly includes, but is not limited to, Afghanistan, Algeria, Bahrain, Bangladesh, Djibouti, Egypt, Eritrea, Indonesia, Iran, Iraq, Jordan, Kuwait, Lebanon, Libya, Malaysia, Morocco, Oman, Pakistan, Qatar, Saudi Arabia, Somalia, Sudan, Syria, Tunisia, Turkey, the United Arab Emirates, and Yemen.

NAILS II (National Automated Immigration Lookout System II): This is a DHS database and serves as the primary lookout database used during primary inspection at ports of entry. It also contains the NIIS, the Deportable Alien Control System (DACS) lookout records from the Detention and Deportation Branch, records from the ADIT Lost and Stolen Alien Registration Card Facility (ICF), lookout records for Visa Waiver Program aliens that are confirmed overstays or refusals, and lookout records from CLASS and TIPOFF. Much of the lookout information from NAILS II is also shared with IBIS, TECS, and CLASS.

NCIC (National Crime Information Center): Created by the FBI in 1967, the NCIC was initially a national database of information on wanted individuals and stolen articles, vehicles, guns, and license plates. The NCIC and its sister system, the National Law Enforcement Telecommunications System (NLETS) contain a multitude of criminal history information and outstanding warrants submitted by participating federal, state, and local law enforcement agencies ranging from relatively minor shoplifting incidents to more serious offenses in the wants and warrants database. Criminal history is maintained in the Interstate Identification Index (III). Fingerprint information is maintained in IAFIS. Information in III can be accessed by name or FBI number through an NCIC terminal. The same information in III can also be accessed via fingerprint submission to IAFIS.

NIIS (Nonimmigrant Information System): NIIS is a system of nonimmigrant denials and overstays collected from matching of entry and departure I-94s and I-94Ws.

NSEERS (National Security Entry Exit Registration System): This is a registration system, which requires fingerprinting and photographing of arriving aliens from designated countries. It is registered in NCIC, and also requires periodic registration with DHS to ensure compliance with nonimmigrant status.

SAO (Security Advisory Opinion): Certain factors identified by law enforcement and intelligence agencies require consular posts to refer selected visa cases to various government agencies, as well as DOS, for enhanced review and are known as security advisory opinion requests.

SEVIS (Student and Exchange Visitor Information System): DOS, DHS, and FBI have the ability to track data (including contact information), visa issuance, and maintenance of status of all F-1, J-1, and M-1 aliens and accompanying family members in F-2, J-2, and M-2 status through SEVIS. Under SEVIS, F, J, and M institutions (universities, colleges, vocational schools, and program designated sponsors) must report when the alien commences a full course of study; drops below a full course of study; transfers schools; extends stay; is reinstated to student status; engages in off-campus employment, curricular practical training, or optional practical training; and completes the program. SEVIS also requires educational institutions and J-1 program sponsors to report aliens who fail to register or show up for school or the J-1 program.

TAL (Technology Alert List): Maintained by DOS, the TAL is a list of sensitive technologies that have been identified as "dual-purpose" technologies, *i.e.*, technologies with both civilian and military applications. The TAL was designed to assist in the effort to prevent the transfer of such sensitive technologies or material from falling into the wrong hands. The TAL specifically provides guidance for use in cases that may fall under the purview of INA §212(a)(3)(A), which renders aliens inadmissible where there is reason to believe they are seeking to enter the United States to violate or evade U.S. laws prohibiting the export of goods, technology, or sensitive information from the United States.

The TAL also includes DOS' list of designated state sponsors of terrorism, which consists of Cuba, Iran, Libya, North Korea, Sudan, and Syria ("Terrible 6" countries).

TECS (Treasury Enforcement and Communications System): Maintained by the U.S. Customs Service, TECS is the information and communication system for not only the U.S. Customs Service, but also for the Bureau of Alcohol, Tobacco and Firearms, IRS Intelligence and Inspection Divisions, and the U.S. National Central Bureau of INTERPOL. TECS is also accessible to DEA, DOS, and the Coast Guard. It is available at all ports of entry and provides agencies with information on suspect individuals, businesses, vehicles, aircraft, and sea vessels. It also functions as an automated index to Customs enforcement files, Bureau of Alcohol, Tobacco and Firearms records on fugitives, stolen weapons and explosives, and other information on pilots in private aircraft, commercial aircraft, smuggling techniques, and private and commercial sea vessels. TECS also provides access to NCIC and the Service Lookout Book. Moreover, DHS findings of ineligibility are entered into the TECS system, and these entries are electronically fed into CLASS.

"Terrible 5" countries: The "Terrible 6" refers to countries identified as state sponsors of terrorism—currently designated as Cuba, Iran, North Korea, Sudan, and Syria. Iraq was removed from the list in October 2004, since

Iraq is under "U.S. control," but Iraqi nationals still undergo extensive security checks. Libya was also recently removed from the list, leaving the "Terrible 6" to the "Terrible 5."

TIPOFF: Maintained by DOS's Bureau of Intelligence and Research, TIPOFF is another classified database of approximately 120,000 records and includes the names of suspected terrorists.[151]

TSC (Terrorist Screening Center): Created in September 2003 to consolidate terrorist watchlists and provide 24/7 operational support for thousands of federal screeners across the United States and throughout the world. The TSC is supposed to ensure that government screeners are working from the same unified set of antiterrorist information and comprehensive antiterrorist lists when a suspected terrorist is screened or stopped anywhere in the federal system. The TSC will receive the vast majority of its information about known and suspected international terrorists from the TTIC, after the TTIC has assembled and analyzed that information from a wide range of sources. In addition, the FBI will provide the TSC with information about purely domestic terrorism. The TSC will consolidate this information into an unclassified terrorist screening database and make it available to queries for federal, state, and local agencies for a variety of screening purposes. The TSC, through the participation of DHS, DOJ, DOS, and intelligence community representatives will determine which information in the database will be available for which types of screening. The TSC does not collect any information independently—it only receives information provided by the TTIC and the FBI. Based on its technical experience in watchlist integration, the FBI is in charge of administering the TSC, with DHS, DOS, and others coordinating and assigning operational and staff support to TSC.

TTIC (Terrorist Threat Integration Center): Is an interagency body intended to provide a comprehensive, all-source based picture of potential terrorist threats to U.S. interests. Analysts from every intelligence agency receive and review a steady stream of threat information developed by their agency agents and sources, and furnish their finished analyses to the TSC to some 2,600 specialists at every major federal agency and department involved in counterterrorism activities. In December 2004, the TTIC was superseded by the National Counterterrorism Center (NCTC).

US-VISIT (United States Visitor and Immigrant Status Indicator Technology): US-VISIT is a DHS program that collects biographic and biometric information – digital fingerprints and photographs – from travelers when they enter and leave the United States through U.S. airports, seaports and land border ports of entry, and when they apply for a visa at a U.S. consular post. This program provides the government with capability to record the entry and exit of non–U.S. citizens into and out of the United States.

Visas Condor: Is an SAO generally triggered by a male national or citizen between the ages of 16 and 45 years of age from a predominantly Muslim country, *i.e.*, a List of 26 or Terrible 6 country.

[151] *See* Testimony of Assistant Secretary of State for Consular Affairs Maura Harty Before the National Commission on Terrorist Attacks Upon the United States, *supra* note 94.

Visas Mantis: Is an SAO triggered by the TAL designed to prevent the transfer of sensitive, dual-purpose technologies.

VVP (Visas Viper Program): Is not a security check, but is actually an interagency committee of officers at consular posts who are tasked to share data from local sources and coordinate and decide who constitutes a threat. A Visas Viper message is the cable that consular posts use to report information about suspected terrorists who may not be applying for visas at the time, but need to be identified in databases in the event that they apply at a later date.