

CONSULAR PROCESSING GOES GREEN IN 2009 - THE ELECTRONIC PAPERLESS ERA

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

Consular processing has undergone rapid and systemic changes during the past seven years, and the rate and scope of change does not appear to be slowing. Directly following 9/11, improving national security was at the forefront of the agenda. As a result, enhanced security checks and inter-agency data sharing – among a massive wave of other changes – made consular processing a daunting task that ensnared many unsuspecting visa applicants in problems and delays. Over the years that followed and after many growing pains, the system has begun to move towards streamlining visa processing procedures. In light of increasing familiarity and reliance on digital systems, the new trend in consular processing is “going green,” eliminating paper applications altogether in favor of a fully electronic system. Although this system may

provide opportunities for more efficient administration of visa processing, it will retain the same enhanced-security framework with more focus on internal agency data review and less on applicant participation. As recent years have taught us, it is critical to understand upcoming systemic changes to anticipate and avoid pitfalls in consular processing. However, we can only hope that going paperless will benefit both the environment and visa applicants, and will not result in making an already complex system even more opaque and inaccessible.

In the aftermath of 9/11, numerous measures designed to enhance security and streamline visa processing were implemented to identify and eliminate vulnerabilities in the visa processing system. The passage of the USA PATRIOT Act, 2001,¹ followed by the Enhanced Border Security and Visa Entry Reform Act, 2002 (Border Security Act),² and the Homeland Security Act, 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 rigorous 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 “T-

* Copyright © 2009 Bernard P. Wolfsdorf, A Professional Law Corporation/Wolfsdorf Immigration Law Group (all rights reserved). Updated from an article originally published in *Homeland Security, Business Insecurity, Immigration Practice in Uncertain Times* (AILA 2003).

Tien-Li Loke Walsh practices exclusively in the area of immigration and nationality law with the Wolfsdorf Immigration Law Group. She previously served as the Vice-Chair on the American Immigration Lawyers Association (AILA) Department of State (DOS) Liaison Committee, as well as the AILA/California Service Center (CSC) Liaison Committee. Ms. Loke Walsh is listed in the current edition of *Best Lawyers in America*, International and California editions of *Who's Who of Corporate Immigration Lawyers* and the *Southern California Super Lawyers, Rising Stars* edition. She completed undergraduate studies at the University of Sydney, Australia, and received a J.D. from Boston University School of Law. Ms. Loke Walsh can be contacted at tloke@wolfsdorf.com.

Bernard P. Wolfsdorf is the national President Elect of the AILA. He is the founding partner of the Wolfsdorf Immigration Law Group, one of the largest full-service immigration firms in the United States with offices in Santa Monica and New York City. He has been a California State bar certified specialist in immigration and nationality law for over 20 years and is featured in current editions of *Best Lawyers in America*, *Chambers World's Leading Lawyers for Business*, *California Super Lawyers*, *Martindale Hubbell's Preeminent Specialist Directory* and *The International Who's Who of Corporate Immigration Lawyers*. Mr. Wolfsdorf can be contacted at Bernard@Wolfsdorf.com.

The authors would like to thank Andrew Stevenson for his significant contributions and also to Avi Friedman for his continued insight and expertise.

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, 2002, Pub. L. No. 107-173, 116 Stat. 543 (2002) (hereinafter Border Security Act).

³ The Homeland Security Act, 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.

4” countries, (formerly the “T-7”)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.

While many of the security measures were expected after 9/11, the effects were devastating to many U.S. visa applicants, who routinely encountered completely unpredictable surprises that caused unexpected and lengthy delays in visa issuance. These initial difficulties, delays and the resulting uncertainty for visa applicants and employers adversely impacted critical U.S. economic sectors including trade, tourism, scientific research, academia, and entertainment and business generally.

Over time, the consular framework has shifted to a more balanced approach. While the focus is still on security, there is a 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, the Department of State (DOS) has now fully embraced its “Secure Borders, Open Doors”⁷ policy. Following a restrictive and frustrating period, there has been an attempt to create a balance with the application of a more rational and focused approach in consular processing.

New procedures have become more efficient as the enhanced security system infrastructure has evolved. Numerous key programs have been implemented, including the electronic Petition Information Manage-

ment System (PIMS), facial recognition analysis from photographs and digital ten-fingerprint capturing at consular interviews. This new comprehensive system has facilitated development of an interlocking network of data sharing between consular posts and the three branches of the Department of Homeland Security (DHS) that handle immigration matters: U.S. Customs and Border Patrol (CBP), U.S. Citizenship and Immigration Services (USCIS) and U.S. Immigration and Customs and Enforcement (ICE). The framework thus appears to be shifting towards a more balanced approach. Increased coordination between government agencies has led to streamlined visa application procedures with fewer false “hits” and improved security check processing times. Effectively, this has not only resulted in increased efficiency, but it has also provided practitioners, visa applicants and employers with a degree of predictability to the consular framework.

However, even as the new consular processing system becomes more transparent, the DOS is on the verge of entering yet another new era. In light of a vastly expanded and improved infrastructure to share and store electronic data, the DOS is piloting a new paperless system. This new system involves the Consular Application Center concept with the new DS-160 Smart Form, E-signatures, and inter-agency data sharing. As consular processing enters the new paperless era, the ability to share and store data has improved. However, some of the recent visa issuance procedures are more cumbersome and same day issuance is rare with most visa issuances taking at least two to five days. Nevertheless, even as the system becomes more familiar, the consular processing framework still provides numerous challenges to practitioners and visa applicants.

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 agen-

⁵ The original “T-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 “T-4 or T-4” countries, since Libya, Iraq and North Korea were removed from the list, but Libyan, Iraqi and North Korean 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 freedom 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).

cies—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).⁸

Since 9/11, DOS has made significant changes and 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, counterterrorism and high technology. In FY 2008, DOS completed more than 260,000 SAO’s.⁹ If an SAO is initiated, consular posts must now wait for an affirmative response from all appropriate government agencies prior to issuing a visa.

Since 9/11, DOS and other U.S. government agencies, including the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA) have consulted in an extensive and ongoing review of visa issuing procedures. Over 8.9 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 20 million.¹⁰ Additional name

check records from the intelligence community through TIPOFF, along with data from the U.S. Marshals Service, were also incorporated into CLASS.¹¹ 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 has been working closely with Customs and Border Protection (CBP) and their National Targeting Center to improve communications between DOS and Department of Homeland Security (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).¹² 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 driving under the influence (DUI) 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. The CCD stores fingerprints and photographs of all visa applicants in electronic form. In addition to interfacing with other

⁸ See R. Sindelar, “CHIMERA, NSEERS, Lookouts and Security Checks: The New Age,” 8 *Benders Immigr. Bull.* 105 (Jan. 15, 2003) at 107.

⁹ See “DOS Replies to AILA Liaison Questions,” (November 5, 2008) published on AILA InfoNet at Doc. No. 09022660 (posted Feb. 25, 2009). In FY 2006, DOS processed 244,558 SAOs, including 57,318 Condors and 33,388 Mantis checks See “AILA/DOS Liaison Meeting Minutes,” (October 2006) published on AILA InfoNet at Doc. No. 06101267 (posted Oct. 12, 2006). For the period between October 1, 2006 and 28 February, 2007, DOS processed over 820,000 NCIC checks, 20,205 Visas Condor and 14,384 Visas Mantis checks. See also “AILA/DOS Liaison Meeting Minutes,” (Mar. 2007), published on AILA InfoNet at Doc. No. 07041668 (posted Apr. 16, 2007). 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. 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).

¹⁰ 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>; see also Testimony of Deputy Assistant Secretary for Visa Services, Stephen A. “Tony” Edson before the U.S. House Committee on Government Reform, Subcommittee on National Security, Emerging Threats and International Relations, Sept. 13, 2005, available at http://travel.state.gov/law/legal/testimony/testimony_806.html

¹¹ 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).

¹² According to a Government Accountability Office (GAO) Report, many visa chiefs reported that additional guidance would be helpful regarding the interaction between DOS and Department of Homeland Security (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 Customs and Border Protection (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).

databases, the CCD indicates the outcome of any prior visa applications.

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 "T-4 countries," and not just to citizens of those countries.¹³

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. Prior to this guidance, any individual who had spent time, whether for short visits or extended assignments or periods as a minor in a "country of concern," was often subjected 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). Anecdotal reports indicate that applicants from some of these countries are typically not subjected to Condor SAOs and receive their visas within normal nonimmigrant visa (NIV) processing times.¹⁴

If a Condor SAO is required, DOS requires posts to wait for an affirmative response from all participating agencies prior to issuing a visa.¹⁵

The average processing times for Condor SAOs is approximately three days. To date, there is no system to expedite these security checks. However, if a Condor SAO has been pending for over 90 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*.¹⁶

NCIC Checks and "Hits" in the Database

As a result of increased database sharing between government agencies, consular posts have access to 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 a "hit" triggered upon fingerprinting an applicant. If an applicant triggers a "hit," posts will submit the applicant's fingerprints to the FBI to request more detailed information about the applicant's criminal record. In December 2006, DOS completed its worldwide deployment of the software for electronic ten-digit fingerprinting, which allows posts to submit the fingerprints directly to the FBI. The ability to capture this data electronically allows posts to request and obtain the results of the FBI fingerprint checks within a 24-hour period in most cases (and sometimes in as little as several hours).¹⁷

Attorneys are encouraged to submit copies of final court dispositions for all convictions and a legal brief arguing admissibility at the time of the initial visa application, although consular officers are still required to obtain fingerprints and verify an applicant's criminal record through electronic database checks. There

¹³ 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 "T- 7" is refused a visa, consular officers will "send a Visas Condor anyway ..." *Id.*

¹⁴ 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 9.

¹⁵ When first implemented, Visas Condor cables were sent to the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), 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,

continued

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 Department of Justice 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.

¹⁶ See "DOS Answers to AILA's Questions," (Oct. 2005) *supra* note 9.

¹⁷ See "AILA/DOS Liaison Meeting Minutes," (Mar. 2007) *supra* note 9.

is still no method to initiate the NCIC check in advance of a visa application.

Applicants with a criminal record must undergo a NCIC check with each visa application, even if a renewal and a NCIC check was performed as part of a prior visa application. However, if the applicant's criminal record is the same and the previous consular officer updated the database at the time of last visa issuance, a detailed investigation of the applicant's record by the consular post may not be necessary. Although practitioners still sporadically report problems, the transition to ten-print electronic fingerprint collection has alleviated most delays and visa processing problems.

“False hits” continue to be of concern for unsuspecting visa applicants. Anecdotal reports confirm that some false hits are still sometimes triggered if 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, so this issue may disproportionately affect applicants from Spanish-speaking countries. However, because consular officers will conduct a detailed NCIC check to confirm the applicant's identity and the existence (or non-existence) of their criminal record, applicants are not permitted to affirmatively attempt to prove that they are not the same person as that on the database.¹⁸

Visas Donkey Security Advisory Opinions

Some of the most problematic cases are with name “hits” for applicants from countries where there are few surnames or name similarity is common (*e.g.*, Patel, Mohammad Ali, Mohammad Siddiqui, Mohammad Khan, etc.). The “hit” is not based on nationality or a criminal history and since there is no clarifying information such as a date-of-birth in the system, a consular officer has no choice but to initiate a Visas Donkey security check. Unfortunately, it is virtually impossible to predict if an applicant will be subject to this SAO until the time of the interview.

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)¹⁹ to make its determinations. The TAL is also designed to specifically provide guidance for use in cases that may fall under the purview of Immigration and Nationality Act (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 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.²⁰ 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, tensions in the Middle East, and the 9/11 terrorist attacks combined to renew concern among the law enforcement and intelligence communities that controlled U.S.-origin goods and information are vulnerable.

The 2002 revised TAL consisted of two parts: a Critical Fields List (CFL)²¹ of major fields of technol-

¹⁸ 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.

¹⁹ 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.

²⁰ See “State Dept. Updates Guidance on Technology Alert Checks,” *published on* AILA InfoNet at Doc. No. 03030449 (*posted* Mar. 4, 2003).

²¹ 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 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 pathogenicity, 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

continued

(NBC) protection). In the chemical area, includes Organo-phosphate chemistry, Neurochemistry, Chemical engineering, Chemical separation technology, Pesticide production 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

continued

ogy 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 "T-4" countries.²² 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 countries designated as "state sponsors of terrorism" seeking to engage in one of the critical fields warrant special scrutiny and mandatory security advisory opinion (SAO) checks.²³

In comparison to the previous version, the 2002 TAL included a vastly expanded list of associated technologies within each critical field, which detailed virtually every potential "dual use" application, where seemingly benign technologies have potential military applications. For example, the 2002 updated TAL included chemical, biotechnology and biomedical engineering critical fields. This all-encompassing list included almost every possible associated technology or skill involving chemistry, biochemistry, immunolo-

welders), Low Energy Lasers (LEL), Semiconductor lasers, Free electron lasers, Directed Energy (DE) systems, Kinetic Energy (KE) systems, Particle beam, beam 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/VOL/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. *Id.*

²² The current designated list of state sponsors of terrorism includes Cuba, Iran, Sudan and Syria, *but see supra* note 5.

²³ See "State Dept. Updates Guidance on Technology Alert Checks," *supra* note 20.

gy, microbiology, pharmacology, genetic engineering, and chemical engineering to name a few. With such an all-inclusive list, many practitioners felt that nearly every research scientist, physician, academic scholar, or engineer involved in any of these fields in commercial research laboratories, educational institutions and universities, or private industry could be subject to a TAL security check by a post erring on the side of caution.

As further indication of the all-encompassing nature of the TAL, the updated list also added a new field to the TAL—urban planning (expertise in construction or design of systems or technologies necessary to sustain modern urban societies). This appeared to indicate 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.

According to the revised TAL, in all cases, consular officers were instructed to 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 instructed 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 urged consular officials to use their judgment, it cautioned officers to err on the side of caution if there were 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 had to submit an SAO in the form of a Visas Mantis.²⁴ If

²⁴ 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

a determination was made that the technology involved presented a security risk, the applicant could be permanently barred under §212(a)(3)(A), for which there is no waiver.

Despite this guidance, it appeared that the cable failed to provide consular posts and attorneys with clear direction²⁵ as to when an SAO is required and in fact, seemed to signal a bureaucratic shift towards initiating Visas Mantis SAO requests for all cases unless posts were absolutely sure the applicant would 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.²⁶ However, anecdotal reports confirm that posts are no longer as “trigger happy” with Mantis SAOs as in the past, although it appears that nationals of China, India and Russia, which account for the majority of Mantis SAOs, are still the most likely applicants to have Mantis SAOs initiated. Ongoing efforts by DOS to expand Mantis training also seems to have contributed to improvements in the Mantis SAO system.²⁷

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.*

²⁵ 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”). The GAO 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 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. *Id.* at 16.

²⁶ 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 was 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).

²⁷ DOS provides additional training and expanded briefings on the Visas Mantis process to new consular officers at the Nation-

The TAL has now been removed from the DOS website,²⁸ but DOS confirms that it reviews the TAL each year, eliminating items which do not appear to pose a risk and adding any new areas of concern.²⁹

The Visas Mantis Process

If a Mantis SAO is required, consular posts transmit the request to the Visa Office and interested agencies.³⁰

In July 2004, the FBI, DOS, and DHS reached an agreement that fundamentally changed the FBI’s role in the Visas Mantis process.³¹ Officials from these

al 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. 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>. Country specific briefings are offered to officers en route to posts with significant Mantis volume. The Bureau of Consular Affairs, working with the Foreign Service Institute, is developing on-line consular refresher courses, including a module on the Visas Mantis process. These training modules were rolled out in early 2008 and are available worldwide. In addition to the formal training courses and briefings, DOS provides ongoing guidance to posts on Visas Mantis issues, including more than twenty-five videoconferences with dozens of posts. The Visa Office also maintains a designated Visas Mantis web page available worldwide and which contains numerous online references See Testimony of Deputy Assistant Secretary of State for Visa Services Stephen A. “Tony” Edson before the U.S. House of Representatives, Committee on Science and Technology Subcommittee on Research and Science Education, House Committee on Science and Technology, Feb. 7, 2008, available at http://travel.state.gov/law/legal/testimony/testimony_806.html.

²⁸ 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,” (Oct. 2004) published on AILA InfoNet at Doc. No. 04120760 (posted Dec. 7, 2004).

²⁹ See Testimony of Deputy Assistant Secretary of State for Visa Services Stephen A. “Tony” Edson, Feb. 7, 2008, *supra* note 27.

³⁰ See Testimony of Janice L. Jacobs, Deputy Assistant Secretary of State for Visa Services, Feb. 25, 2004, *supra* note 27.

³¹ 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,

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.³² Prior to this change in policy, DOS did not proceed with issuance of a visa until each individual government agency provided an affirmative response.³³

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.³⁴ 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.³⁵ According to DOS, waiting for highly classified reports through appropriate channels can be another reason for delay in responding to a consular post.³⁶ Once DOS receives all agency responses pertaining to the applicant, it summarizes them and prepares a response to the consular posts.³⁷ 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.³⁸

DOS reports that the average processing time for Mantis checks as of November 2008, is approximately six to eight weeks, which is significantly faster than the four to six month backlog experienced by many in the beginning, but significantly slower than the 15 days in February 2008.³⁹ Consular posts may not issue the visa until they receive an affirmative response from all participating agencies, except the FBI. However, if a Mantis security check has been pending for over 90 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*.

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.⁴⁰ This allows applicants to re-apply for visas without undergoing frequent Mantis checks, if returning to the previous program of study or professional assignment. Howev-

published on AILA InfoNet at Doc. No. 05022266 (posted Feb. 22, 2005) (hereinafter "Feb. 2005 GAO Report).

³² 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 27. 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. See Feb. 2004 GAO Report *supra* note 25 at 14.

³³ 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 commercial activities. 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. The February 2004 GAO Report found that interoperability problems among the systems that DOS and FBI use contributed to the delays in processing. Since many different agencies, bureaus, posts, and field offices are involved in processing Mantis SAOs, and each has different databases and systems, Mantis SAOs were often delayed or lost at different points in the process. 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. See Feb. 2004 GAO Report *supra* note 25 at 14.

³⁴ 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.*

³⁵ See Testimony of Janice L. Jacobs (Feb. 25, 2004), *supra* note 27.

³⁶ *Id.*

³⁷ See Feb. 2004 GAO Report *supra* note 25 at 8.

³⁸ *Id.*

³⁹ See Testimony of Deputy Assistant Secretary of State for Visa Services Stephen A. "Tony" Edson, Feb. 7, 2008, *supra* note 27. 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 31 at 2. See also "DOS Replies to AILA Questions" (Nov. 5, 2008) *supra* note 9.

⁴⁰ See "Some Visas Mantis Clearances Extended," published on AILA InfoNet at Doc. No. 05021460 (posted Feb. 14, 2005).

er, 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 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 twelve 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.⁴¹ 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 twelve months.⁴² Visas for Chinese and Russian Mantis applicants, which account for approximately 76 percent of all Mantis cases,⁴³ can only be issued as single-entry visas valid for three months.⁴⁴

⁴¹ See Feb. 2005 GAO Report, *supra* note 31 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 U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) and Student and Exchange Visitor Information System (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.

⁴² 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 9.

⁴³ 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

continued

Documents an Applicant with Potential Mantis Issues Should Bring to an Interview

Applicants involved in any activities that have potential "dual use" applications should bring the following documents to an interview: a complete resume (and if accompanying the applicant, a professional spouse's resume), a complete list of publications of the applicant (and spouse's publications), list of references in the applicant's country of birth or residence, detailed descriptions of the applicant's proposed research or work in the United States 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 and 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.⁴⁵

It also appears that many NIV applicants who are subjected to a Mantis security check are 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.

Other Security Checks: Visas Bear, Visas Eagle and Visas Merlin

There are a handful of other SAOs, including the, including Visas Bear, Visas Eagle and Visas Merlin, but it is not common for practitioners to encounter these SAOs.

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 31 at 10.

⁴⁴ See "DOS Answers to AILA Questions" (Mar. 2004), published on AILA InfoNet at Doc. No. 04042164 (posted Apr. 21, 2004).

⁴⁵ The provisions at 9 *Foreign Affairs Manual* 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," (Oct. 2004), *supra* note 28.

Visas Bear are for officials and diplomatic visa applicants. Visas Horse and Visas Pegasus are also SAOs used for official visitors.

Visas Eagle are clearances used for immigrants from certain former and current Communist countries.

Visas Merlin are security checks performed on refugee applications.

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 “T-4” 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.⁴⁶ This provision formalizes the existing procedures and screening process, known as “Falcon” security checks, for individuals from these seven countries.

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 cableless SAO process called the SAO Improvement Project (SAO IP).⁴⁷ DOS spent \$1 million providing electronic inter-agency linkage aimed at improving efficiency between interagency processing. This included the elimination of its traditional cabling system between consular posts and other federal government agencies in the SAO process.⁴⁸ The program uses real-time data sharing, allowing for seamless electronic data transmission from posts, eliminating virtually all manual manipulation of data.⁴⁹ The other agencies 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 meant to improve data integrity, accountability of responses in specific cases and statistical reporting.⁵⁰ Posts can

now 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. DOS completed worldwide implementation of the SAO IP by October 2004.⁵¹ The SAO IP operates through an interagency network known as the Open Source Information System (OSIS), which provides interoperable data transmission.⁵² Following initial interconnectivity problems between the FBI and DOS databases, the FBI is finally performing all name checks electronically through the CCD.⁵³ Full connectivity by all government agencies allow for shorter processing times and the ability to track cases and keep more accurate statistics.⁵⁴

BIOMETRIC TECHNOLOGIES

Section 303 of the Border Security Act mandated the use of biometric identifiers in all U.S. visas by October 26, 2004.⁵⁵ 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, Department of Justice (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 would consist of facial recognition (digital photographs) and fingerprint technologies.⁵⁶ 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.⁵⁷ The inclusion of biometric data in travel records will also make it easier to replace lost or stolen travel documents.

⁴⁶ See Border Security Act, *supra* note 2, §306.

⁴⁷ Testimony by Janice L. Jacobs (Feb. 25, 2004), at *supra* note 27.

⁴⁸ *Id.*

⁴⁹ *Id.*

⁵⁰ *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 31 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.*

⁵¹ See “DOS Answers AILA Questions,” (Oct. 2004) *supra* note 28; see also “DOS Answers to AILA’s Questions,” (Mar. 17, 2005), *supra* note 9.

⁵² See Janice L. Jacobs testimony, (Feb. 25, 2004), *supra* note 27.

⁵³ See “DOS Answers to AILA’s Questions,” (Mar. 17, 2005), *supra* note 9.

⁵⁴ See “DOS Answers to AILA’s Questions,” (Mar. 23, 2006) *supra* note 12.

⁵⁵ See Border Security Act, *supra* note 2.

⁵⁶ See “DOS Answers to AILA Questions,” published on AILA InfoNet at Doc. No. 03102043 (posted Oct. 14, 2003).

⁵⁷ *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 25, at 36.

DOS completed deployment of the Biometric Visa Program ahead of schedule where all 207 NIV issuing posts were collecting biometrics for NIV and all 125 immigrant visa (IV) issuing posts for immigrant and diversity visas by October 7, 2004.⁵⁸ There are limited individual 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.⁵⁹

The inkless fingerprint scanning generally takes approximately 30 seconds.⁶⁰ 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) over a reliable, direct transmission line, which sends the results back to the CCD for relay back to the post.⁶¹ As of January 1, 2008, the fingerprints are also

screened through the FBI's IAFIS criminal database.⁶² The current turnaround time is approximately 30 minutes.⁶³

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.⁶⁴ At present, consular posts do not have access to the FBI record associated with that file number.⁶⁵ 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.⁶⁶ 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.⁶⁷ 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.⁶⁸

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.⁶⁹ DOS and DHS plan to

⁵⁸ "Completion of Biometric Deployment" Cable, Oct. 8, 2004, posted on *ilw.com*. According to DOS, it had 3,567 hits in DHS's Automated Biometric Fingerprint Identification System (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 immigrant visa (IV) system. *Id.* In May 2007, DOS estimated that it had cleared fingerprints of over 17 million visa applicants through IDENT and investigated over 35,000 IDENT matches. See Testimony of Director, Office of Fraud Prevention Programs, Andrew Simkin before the Subcommittee on Terrorism, Technology and Homeland Security, "Interrupting Terrorist Travel: Strengthening the Security of international Travel Documents," May 2, 2007 available at http://travel.state.gov/law/legal/testimony/testimony_806.html

⁵⁹ 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, 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, children 13 years and under and 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 ten fingerprints for clearance through the FBI. *Id.*

⁶⁰ 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>.

⁶¹ *Id.*

⁶² See Testimony of Deputy Assistant Secretary of State for Visa Services Stephen A. "Tony" Edson, Feb. 7, 2008, *supra* note 27.

⁶³ 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.

⁶⁴ See Testimony of Maura Harty, (Jan. 28, 2004), *supra* note 60.

⁶⁵ *Id.*

⁶⁶ *Id.*

⁶⁷ See Sept. 2004 GAO Report, *supra* note 63, at 5-6.

⁶⁸ See Testimony of Maura Harty, (Jan. 28, 2004), *supra* note 60.

⁶⁹ This information is based on comments made by Deputy Assistant Secretary of State, 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

create 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.⁷⁰ In January 2008, DOS implemented its Visa Re-issuance program, whereby posts collect ten fingerprints from visa applicants once, and expects that it would not normally re-fingerprint applicants again.⁷¹ According to DOS, once the ten prints have been collected and stored in IDENT, it is expected that DHS will collect a lesser number of fingerprints at a port-of-entry to perform identity verification.⁷² Ten prints are currently being collected at all U.S. consular posts worldwide.

The fingerprint analysis is therefore merely a first step in the biometric program. DOS also uses a facial recognition program, whereby all visa applicant photos are screened against a facial recognition database of suspected terrorists and visa violators.⁷³ 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.⁷⁴

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 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. *Id.*⁷⁰ *Id.*

⁷¹ See “AILA Liaison/DOS Q & A’s,” (Oct. 24, 2007), published on AILA InfoNet at Doc. No. 07112732 (posted Nov. 27, 2007).

⁷² *Id.*

⁷³ See Testimony of Deputy Assistant Secretary of State for Visa Services Stephen A. “Tony” Edson, Feb. 7, 2008, *supra* note 27; See “DOS Answers to AILA’s Questions,” (Mar. 17, 2005), *supra* note 9. 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 7 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 9.

⁷⁴ The posts may compare the images themselves, but only in emergency situations.

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, 2004.⁷⁵ US-VISIT is designed to collect and share information on individuals 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

⁷⁵US-VISIT has been in effect at all 115 airports and 14 seaports and at the 50 most highly trafficked land borders since January 5, 2004. The remaining 115 land borders were phased in by December 31, 2005. On December 19, 2008, DHS expanded the categories of non-U.S. citizens required to provide biometrics through US-VISIT. Effective January 18, 2009, the following additional non-U.S. citizens are required to provide biometrics when entering or re-entering the United States:

- Lawful permanent residents of the United States (LPRs);
- Persons entering the United States who seek admission on immigrant visas;
- Persons entering the United States who seek admission as refugees and asylees;
- Canadian citizens who are currently required to obtain a Form I-94 upon entry or who require a waiver of inadmissibility to enter the United States (this excludes most Canadian citizens entering the United States for tourist or business activities);
- Persons paroled into the United States; and
- Persons applying for admission under the Guan Visa Waiver Program.

See “Fact Sheet: Expansion of US-VISIT Procedures to Additional Travelers;” at www.dhs.gov/xtrvlsec/programs/gc_1231972592442

US-VISIT still does not apply to U.S. citizens, Canadian tourists and business visitors not requiring I-94 cards, diplomats, children under the age of 14 and elderly over 79 years of age. US-VISIT is separate from National Security Entry Exit Registration System (NSEERS) and SEVIS. Those requirements remain unchanged.

United States in violation of the terms of their admission to the United States.

Upon arrival in the United States, an individual who is subject to US-VISIT is inspected by CBP inspectors at a port of entry. The person's travel documents are scanned, a digital photograph and inkless fingerprints of all ten fingers are taken.⁷⁶

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.⁷⁷ If the system shows a mismatch of fingerprints or a watch list hit, the foreign national is held for further screening or processing.

The US-VISIT enrollment process takes approximately 10–15 seconds.⁷⁸ 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.⁷⁹ 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.⁸⁰

The individual's name is also checked against the IBIS database and the wants and warrants section of the NCIC database.⁸¹ 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.⁸²

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.⁸³

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.*

⁸¹ 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>.

⁸² See Statement by Kathleen Campbell Walker, *id.*

⁸³ 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

continued

⁷⁶ All ports of entry transitioned from two index finger prints to ten fingerprint collection at the end of 2008. See "DHS Begins Collecting 10 Fingerprints from International Visitors at Washington Dulles International Airport," Dec. 10, 2007 available at http://www.dhs.gov/xnews/releases/pr_1197300742984.shtm.

⁷⁷ See Testimony of Maura Harty, (Jan. 28, 2004), *supra* note 60; Comments by Catherine Barry, Acting Deputy Assistant Secretary of State for Consular Affairs, DOS/AILA meeting on Mar. 4, 2004.

⁷⁸ See Testimony of Maura Harty, (Jan. 28, 2004), *supra* note 60;

⁷⁹ *Id.*

⁸⁰ *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,

continued

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.⁸⁴

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 Integrated Automated Fingerprint Identification System (IAFIS)⁸⁵ 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.⁸⁶

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.⁸⁷ 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 two phases have been completed. The first phase consisted of a pilot program, known as the interim data-sharing model (iDSM). iDSM allowed for two-way sharing of biometric and biographic information, including all IAFIS wants and warrants, expedited removals and visa applicants that the DOS 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 were 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 and authorized non-criminal agencies, had fingerprint-based access to immigration history information and U.S. immigration officials had 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 expanded the categories of data shared and further enhance the infrastructure for data exchange and search capabilities between these two databases. During this phase, DHS' US-VISIT program moved from collecting two fingerprints to collecting ten fingerprints. By November 29, 2007, DHS as part of US-VISIT, started to collect ten fingerprints at the Washington Dulles International Airport. By the end of 2008, all ports-of-entry had started to collect ten fingerprints.⁸⁸ US VISIT's transition to ten-print enrollment allows for the facilitation of more efficient IAFIS and IDENT interoperability through the use of a common biometric template, which will increase the accuracy in identity verification.⁸⁹

FOC or the third phase will provide additional data and further automate many of the processes.⁹⁰

have provided only a temporary or false location as to where the alien was intending to go.

See Statement by Kathleen Campbell Walker, *id.*

⁸⁴ *Id.*

⁸⁵ Integrated Automated Fingerprint Identification System (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 10-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.

⁸⁶ See Statement by Kathleen Campbell Walker, *supra* at note 81.

⁸⁷ See "IDENT and IAFIS Interoperability Fact Sheet," *published on AILA InfoNet at Doc. No. 06110164 (posted Nov. 1, 2006).*

⁸⁸ See "DHS Begins Collecting 10 Fingerprints from International Visitors at Washington Dulles International Airport," *supra* note 76.

⁸⁹ The transition to ten prints is also in response to criticism that the system used by IDENT is based on a flat two-print. However, with consular posts starting to transition to a ten-print system based on the FBI's IAFIS, the two-print versus ten-print baseline would create problems with false matches on print checks and also because it would not interface well when the two-print IDENT print is run against the ten-print rolled IAFIS system. See K. Walker, "One If By Land, and Two If By Sea . . .," 22 *AILA's Immigration Law Today* 12 at 14 (Nov/Dec. 2003).

⁹⁰ See "IDENT and IAFIS Interoperability Fact Sheet," *supra* note 87.

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.⁹¹ With respect to the biometric identifier requirement, the International Civil Aviation Organization (ICAO)⁹² 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. Since most of the VWP countries did not have production capability in place by the original deadline, the deadline was extended to October 26, 2006.

This biometric identifier requirement coincided with a separate requirement that required VWP travelers to present a machine-readable passport (MRP) when applying for visa-free entry into the United States after October 26, 2004. It is important to note that the machine-readable passport requirement is a separate obligation to the biometric requirement. Although confusing, the passport guidelines for traveling under the Visa Waiver program are as follows:

- **Passport issued before October 26, 2005 (Machine-Readable Zones):** Older but still valid passports issued by VWP countries before October 26, 2005 must have a machine-readable zone.⁹³ If the passport is not machine-readable, the VWP traveler must obtain a nonimmigrant visa or a new passport;
- **Passports issued October 26, 2005 – October 25, 2006 (Digital Photographs):** Older, but still valid passports issued by VWP countries between October 26, 2005 and October 25, 2006, must include a digital photograph

printed on the data page, or the traveler must obtain a nonimmigrant visa.⁹⁴

- **Passports issued on or after October 26, 2006 (e-Passport):** New passports issued by VWP countries must be e-Passports, which include an integrated computer chip capable of storing biographic information from the data page as well as other biometric information, such as the required digital photograph of the holder.⁹⁵

Electronic System for Travel Authorization (ESTA)

The trend towards paperless information-sharing immigration systems has spread to other government agencies. CBP recently unveiled a new Electronic System for Travel Authorization (ESTA), participation in which is mandatory for all VWP visitors to the United States.⁹⁶ Effective January 2009, ESTA is designed to enhance security screening pursuant to post-9/11 objectives, while secondarily streamlining immigration monitoring processing through interagency data sharing. Under ESTA, all nationals and citizens of VWP countries who seek to enter the United States as temporary visitors for business or pleasure, must acquire an “electronic” approval or clearance prior to boarding an air or sea carrier to the United States. Such clearance is valid for multiple trips for two years or until the expiration of the individual’s passport, whichever occurs earlier. ESTA application information – similar to that routinely elicited on Form I-94W – must be submitted via the internet in English at least 72 hours prior to travel, and will result in a response of “Authorization Approved,” “Authorization Pending,” (to be resolved within 72 hours of submission), or “Travel not Authorized.” If travel is denied, the applicant must apply for a nonimmigrant visa at a U.S. embassy or consulate. If approved, ESTA participants will no longer be required to complete Form I-94W upon entry to the United States, and this information will be electronically collected and integrated into agency databases.

ESTA’s potential effects on the screening of VWP applicants for travel appear similar in many respects to the new paperless consular processing system. On the one hand, streamlining information collection may improve CBP efficiency in reviewing admissibility of VWP visitors; on the other hand, a fully electronic screening system provides applicants and practitioners dangerously little room for advocacy and communication with immigration authorities. In fact, in the case of ESTA, the only point of redress for aggrieved applicants will be through the DHS’s Traveler Redress Inquiry Program (DSH-TRIP), a black-hole initiative that receives information from applicants but never issues written responses. Although ESTA applicants

⁹¹ Visa-Waiver countries include Andorra, Australia, Austria, Brunei, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Lithuania, Liechtenstein, Luxembourg, Monaco, Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, and the United Kingdom.

⁹² International Civil Aviation Organization (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.

⁹³ A machine-readable passport has two lines of text as letters, numbers and chevrons (<<<) at the bottom of the personal information page, along with the bearer’s picture. See http://www.dhs.gov/xlibrary/assets/vwp_travelguide.pdf

⁹⁴ A digital photograph is one that is printed on the page, not a photo that is glued or laminated into the passport. *Id.*

⁹⁵ *Id.*

⁹⁶ See http://www.cbp.gov/xp/cgov/travel/id_visa/esta/

who are denied travel authorization may apply for nonimmigrant visas through normal consular processing channels, it is unclear whether a visa interview under the new consular application center regime will facilitate meaningful review of database errors.

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.⁹⁷ 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, was limited to a narrow category of applicants. Only visa applicants age 80 and over, and age 13 and under and diplomats are not subject to the biometric process and are eligible for the PAW.

However, in January 2008, DOS broadened the PAW policy by issuing guidance to consular posts allowing the waiver of visa interviews for certain categories of renewal applicants, who have previously provided ten fingerprints, been interviewed and received visas within twelve months of the expiration of the previous visa. Therefore, if an applicant has provided ten prints in a previous NIV application and is applying for the same category of visa at their post of usual residence and presents no national security concerns, a post may waive the interview and issue a visa without requiring that applicant to appear in person.⁹⁸

⁹⁷ Diplomatic and official visas (A, G, and NATO) will continue to be processed by the Visa Revalidation division.

⁹⁸ See Testimony of Deputy Assistant Secretary of State for Visa Services Stephen A. "Tony" Edson, Feb. 7, 2008, *supra* note 27. However, although the interview may be waived, it appears that some posts still require the applicant to make an appointment to have their biometric taken or re-taken. Some posts including Algeria, Australia, Russia and China now appear to have a system where the ten-print can be stored and re-used for subsequent

continued

DOS acknowledges that it will take some time for most posts to have a volume of applicants who have already provided ten prints, and as a result, most posts have not established "re-use" procedures. The few consular posts – Algeria, Australia, China and Russia, have announced their policies on their websites.⁹⁹

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

Consular processing at border posts in Canada and Mexico has 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 TCNs a post will accept for interview. Similarly, it is advisable to be aware of the post policy with regard to attorney representation.

Processing for "List of 26" and "T-4" nationals

Since 9/11, border posts generally do not accept applications from "List of 26" or what was known as the "T-4" countries, but some Canadian consular posts have accepted certain "List of 26" and former "T-4" applicants. However, such applicants cannot re-enter the United States until the security checks, if required, are complete and the visa is issued.¹⁰⁰ 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 legally enter and exit Canada or Mexico, during the entire duration of the processing period.¹⁰¹ Thus, it appears that

visa applications. See "DOS Replies to AILA Liaison Questions," (Nov. 5, 2008) *supra* note 9.

⁹⁹ See "DOS Replies to AILA Liaison Questions," (Nov. 5, 2008) *supra* note 98.

¹⁰⁰ Some Canadian posts have previously exercised discretion to issue a two-entry visa if an applicant can demonstrate that his or her travels are "part of a single journey" and that on both entries the applicant would be "seeking admission for the same principal purpose." See 9 FAM 41.113 N5.1. For example, an Iranian physician could apply as a third country national applicant in Canada, return to the United States after issuance of the visa in transit 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.

¹⁰¹ *Id.*

border posts may accept visa applications from “List of 26” and former “T-4” 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 aliens¹⁰² returning from short visits to contiguous territories¹⁰³ or adjacent islands.¹⁰⁴ 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 Code of Federal Regulations (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 from countries designated as “state sponsors of terrorism,” 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 pro-

vided the applicant does not apply for a new visa, and is not a national from one of the “T-4” 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 (E, F, H, J, L, 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.¹⁰⁵ Given the current focus on security measures, it is unlikely that CBP will permit re-admission in visitor classification except in limited circumstances.

DOS continues to work with USCIS to ensure effective enforcement at all ports of entry. When initially amended, the DOS cable to all diplomatic and consular posts announcing these changes provided de-

¹⁰² 68 Fed. Reg. 49351 (Aug. 18, 2003).

¹⁰³ The term “contiguous territories” refers to Canada and Mexico.

¹⁰⁴ 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.

¹⁰⁵ 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); see also 9 FAM 41.121.

tailed 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 automatic revalidation provision.¹⁰⁶ However, these procedures were further revised in January 2007, with the discontinuance of the “Application Received” stamp traditionally placed in the back of an applicant’s passport when refused a visa.¹⁰⁷

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

¹⁰⁶ At the time, DOS similarly revised 9 FAM 41.212(d) Note 4 to detail the precise procedures to be followed in the event of a visa refusal. These revisions included 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.

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, the cable instructed consular officers 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 had to be turned over to that office. In other cases, the form had to 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 was unable to retrieve the I-94 because the applicant claimed it is lost or stolen or turned in to USCIS, the consular officer was 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 was in addition to the stamp placed in the back of the passport as is required for all visa refusals. In cases where an applicant possessed a valid visa, consular officers were 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.*

¹⁰⁷ See Elimination of the “Application Received” Stamp,” *published on AILA InfoNet at Doc. No. 07050461* (posted May 4, 2007). The DOS cable eliminating the “Application Received” stamp is discussed further in the article under the “Other Developments in Consular Processing” section.

country of nationality must file his or her NIV applications at a post designated by DOS.¹⁰⁸

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.

As part of its ongoing efforts, in February 2007, DOS also established a worldwide customer service standard by which every nonimmigrant visa applicant at any post should be scheduled for an appointment within thirty days.¹⁰⁹ The customer service standard for students and U.S.-interest business visas is fifteen days or less. In addition, all applicants found eligible for a visa and who do not require additional security-related processing should expect the visa to be issued within three-days of the interview. DOS’s goal is that by the end of 2008, 100 per cent of posts will be able to meet this thirty-day appointment benchmark.¹¹⁰

¹⁰⁸ 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); Iranians in Abu Dhabi (United Arab Emirates), Ankara (Turkey), Frankfurt, Germany (family-based applicants only), Vienna (Austria), or Naples (Italy); Iraqis in Amman (Jordan), Casablanca (Morocco), Ankara (Turkey) or Cairo (Egypt); Libyans in Tunis (Tunisia); Somalis in Nairobi (Kenya (nonimmigrant visa applications)), 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. At the moment, Cairo is issuing and printing Khartoum’s visas. However, an officer goes to Khartoum periodically to conduct interviews).

¹⁰⁹ See Testimony of Deputy Assistant Secretary of State for Visa Services, Stephen A. “Tony” Edson before the U.S. Senate Committee on Commerce, Trade and Tourism, Subcommittee on Interstate Commerce, Trade and Tourism, Mar. 20, 2007 available at http://travel.state.gov/law/legal/testimony/testimony_806.html; Testimony of Deputy Assistant Secretary of State for Visa Services Stephen A. “Tony” Edson, Feb. 7, 2008, *supra* note 27.

¹¹⁰ See Testimony of Deputy Assistant Secretary of State for Visa Services, Stephen A. “Tony” Edson, Mar. 20, 2007, *supra* note 109.

The Consular Electronic Application Center Introduces A Paperless Visa Processing System

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 reports that the use of the electronic version has improved processing and issuance times. These improvements are paving the way for an entirely paperless visa processing system.

The Future: the New Fully Electronic DS-160

The new Consular Electronic Application Center concept starts with an online application that also collects the fee, schedules the appointment, and most importantly allows a post to have an earlier look at the application.

Information entered by visa applicants will automatically upload into the NIV database system. The plan is that this mechanism will allow DOS to conduct fraud and other checks in advance of the applicant's visa interview.¹¹¹ It will also allow DOS to verify an applicant's U.S. contacts and company and petitioner information ahead of the interview. DOS expects that these checks could also include corroboration of applicant data, searches of relevant DHS records and searches in U.S. visa records to identify issues that require closer examination.¹¹²

All of this will be accomplished through the new Form DS-160, which combines the current DS-156, DS-157 & DS-158 forms. The Form DS-160 will also eventually integrate information from the DS-156E, 156K and 156V forms. The new Form DS-160 is lengthy. The OMB estimates 75 minutes to complete the form but anecdotal evidence indicates that it can take 2-3 hours. The roll-out is gradual, but it is currently being piloted in Mexico (Nuevo Laredo, Ciudad Juarez, Monterrey and Matamoros), Canada (Vancouver and Montreal), Hong Kong S.A.R., Ireland (Dublin) and Japan. The Mexican posts are also testing off-site biometric collection through DOS maintained Application Support Centers. This new framework sets up a rules-based analysis of applications which can differentiate clearly approvable cases, including cases with prior visa issuance, and it also allows the DOS to

¹¹¹ See "AILA/DOS Liaison Meeting Minutes," (Mar. 2007), *supra* note 9.

¹¹² See Testimony of Deputy Assistant Secretary of State for Visa Services Stephen A. "Tony" Edson, Feb. 7, 2008, *supra* note 27.

plan ahead regarding its caseload. Hopefully, this will allow posts to handle workload assignments and reduce lengthy wait times at some posts.

Form DS-260 will eventually replace the DS-230 forms for immigrant visas. Online immigrant applications are expected to be more difficult as it requires coordination with USCIS.¹¹³

Petition Information Management Service (PIMS)

Since November 2007, consular posts have been using the Petition Information Management Service ("PIMS"), which allows posts to access the details of an approved nonimmigrant visa petition through the CCD.¹¹⁴ The Kentucky Consular Center (KCC) no longer emails and scans copies of approved petitions to consular posts.¹¹⁵ USCIS typically sends the duplicate petition and approval information via Federal Express to KCC. KCC then enters key data from an I-129 petition into PIMS and scans in key documents such as the I-129 form, employer support letter and identification documents of the beneficiary.¹¹⁶ In urgent cases, (typically Os and Ps), USCIS will fax the documents to KCC, but these cases are typically uploaded into PIMS by KCC within 12 hours of receipt from USCIS. Hs and Ls are usually uploaded within 48 hours, and change-of-status petitions and extensions are uploaded within 120 hours. KCC also conducts some database checks looking for evidence of fraud, criminal background, immigration status violations or other adverse history and records (including from SEVIS) and records its findings in PIMS.¹¹⁷

¹¹³ See "AILA/DOS Liaison Meeting Minutes," (Mar. 2007), *supra* note 9; see also "DOS Replies to AILA Liaison Questions," (Nov. 5, 2008) *supra* note 9.

¹¹⁴ See "Accessing NIV Petition Information Via the CCD," published on AILA InfoNet at Doc. No. 07112560 (posted Nov. 25, 2007); "Update: New PIMS System," published on AILA InfoNet at Doc. No. 07121072 (posted Dec. 10, 2007).

¹¹⁵ Previously, 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. KCC scanned the petition and transmitted it electronically to post (in the form of an adobe Acrobat document) See "USCIS Sending I-129s to Kentucky Consular Center Rather Than to Posts," published on AILA InfoNet at Doc. No. 04071264 (posted July 12, 2004).

¹¹⁶ Data is not electronically transferred from USCIS to KCC. The Service Centers mail and fax information to KCC, which then data enters and scans the material into PIMS. See "DOS Answers AILA Questions on PIMS," published on AILA InfoNet at Doc. No. 07112960 (posted Nov. 29, 2007).

¹¹⁷ See "Update: New PIMS System," *supra* note 114. See also "PIMS Update" published on AILA InfoNet at Doc. No. 08081564 (posted Aug. 15, 2008). The PIMS petition report contains a record of all petitioners recorded by the KCC as hav-

continued

The electronic PIMS record created by KCC is now the primary source of evidence to be used in verifying the approval of an I-129 petition. Before a post can issue a nonimmigrant visa, it must confirm the petition in PIMS.¹¹⁸ It is not possible for a petitioner or beneficiary to send a petition directly to KCC for entry into PIMS, or to contact KCC directly to verify the existence of a positive approval record before an interview.¹¹⁹ If a post cannot find a petition in PIMS, it must email KCC, which unlike posts, has access to the USCIS CLAIMS 3 system where USCIS records petition approvals. KCC will research approval of the petition and if able to confirm its approval, make the details available through the CCD in two working days.¹²⁰

Initially USCIS only sent petitions designated for consular processing petitions to KCC and did not send change-of-status petitions or extensions to KCC. As a result, this caused unexpected problems for applicants applying for nonimmigrant visas after USCIS has already granted an extension or change-of-status. Based on these "teething" problems, USCIS and DOS recently agreed to a process that facilitates the entry of this information for cases filed after March 2008 into the PIMS system. If a change, extension of stay or amendment is requested, and if a duplicate petition with original signatures is provided to USCIS, it will send the duplicate copy to KCC for data entry into PIMS.¹²¹

It is anticipated that PIMS will result in less reliance on original I-797 approval notices, as the petition approval has to be verified electronically in all cases. As a practical matter, policies requiring the original I-797 still vary from post to post, although DOS has indicated that it con-

ing approved petitions since 2004. In addition, many of the records contain information from KCC's Fraud Prevention Unit. Each new, approved petition is linked to a base petitioner record, allowing DOS to track each NIV petitioner and petition information. See "Accessing NIV Petition Information Via the CCD," *supra* note 114.

¹¹⁸ See "Update: New PIMS System," *supra* note 114; "Accessing NIV Petition Information Via the CCD," *supra* note 114.

¹¹⁹ See "PIMS Update" *supra* note 117.

¹²⁰ See "Update: New PIMS System," *supra* note 114; "Accessing NIV Petition Information Via the CCD," *supra* note 114. KCC tries to complete processing of requests from posts within 24 hours (1 working day) and generally succeeds. According to DOS, if there is an emergency outside of KCC hours, posts can contact the Visa Office duty officer for assistance. See "DOS Answers AILA Questions on PIMS," *supra* note 116. Providing DOS with access to CLAIMS 3 would involve substantial technological and training challenges. As a result, DOS chose to limit CLAIMS 3 access to KCC. Both USCIS and DOS have indicated that they are actively seeking a solution that involves some kind of interim data exchange, but nothing is concrete as of yet. See "PIMS Update" *supra* note 117.

¹²¹ See "PIMS Processing Update," *published on AILA InfoNet at Doc. No. 08032132 (posted Mar. 21, 2008).*

tinues to remind posts that the original is not required. In addition, DOS apparently instructed all posts to implement procedures by which PIMS is checked for H, L, O, P and Q visas before the visa applicant's interview. Many posts have used their interview scheduling procedures to gather the petition receipt number before the visa interview. As resources are available, posts use the information to check PIMS before the interview, and at least begin steps to increase the chances that verification of petition approval will be available at the time of interview.¹²²

As a practical matter, while an original I-797 approval notice is not required for visa issuance, it may be required by CBP when applying for admission at a port of entry.

Fingerprint Collection

All consular posts completed the transition to ten-fingerprint collection in December 2007. According to DOS, two fingerprint scans provide a limited amount of data and also yield a large number of "false positive" results. Ten fingerprints provide a greater number of data points allowing more complete checks against criminal history fingerprint records and much more accurate responses.¹²³ In addition, since January 2008, under the Visa Re-issuance program, DOS will only collect an applicant's ten fingerprints with their first visa application. DOS will not normally fingerprint applicants again for future applications. Based on this program, DOS has expanded the PAW program for certain applicants.¹²⁴ Moreover, after ten prints have been collected and stored in IDENT, it is expected that DHS will collect a lesser number of fingerprints at a port-of-entry to perform identity verification.¹²⁵

DOS is also 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.¹²⁶ DOS is piloting the collection of ten-prints offsite at a secure facility in conjunction with its pilot of the online NIV application in Mexico.¹²⁷

¹²² See "PIMS Update" *supra* note 117.

¹²³ See Testimony of Director, Office of Fraud Prevention Programs, Andrew Simkin, May 2, 2007, *supra* note 58. See also Testimony of Deputy Assistant Secretary of State for Visa Services, Stephen A. "Tony" Edson, Mar. 20, 2007, *supra* note 109.

¹²⁴ Details of the Visa Re-issuance program are found earlier in the article under the section, "Where Can Visa Applicants Apply: Are the Options Still the Same?"

¹²⁵ See "AILA Liaison/DOS Q & A's," (Oct. 24, 2007), *supra* note 71.

¹²⁶ See "AILA/DOS Liaison Meeting Minutes," (Mar. 2007), *supra* note 9.

¹²⁷ See Testimony of Deputy Assistant Secretary of State for Visa Services Stephen A. "Tony" Edson, Feb. 7, 2008, *supra* note 27.

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.¹²⁸

End of an Era: Elimination of the “Application Received” Stamp

In 2007, after 25 years of use, DOS instructed consular posts to discontinue the use of the “Application Received” refusal stamp. With issuance and refusal data now available to all posts through the CCD, it is no longer necessary to alert interviewing officers to previous refusals by stamping the back of the passport. In addition, CCD information is now available at port-of-entry in secondary and to other DHS officers. The DOS cable did however; also remind posts in Canada and Mexico to ensure compliance with the procedures in refusing applicants who are no longer eligible for automatic visa revalidation.¹²⁹

Practitioners who have long relied on the “telltale” “Application Received” stamp in the back of an alien’s passport to determine prior visa refusals, must now be additionally cautious and probe further regarding an applicant’s previous visa refusals as it will no longer be readily apparent.

Implementation of Worldwide Web-Based Appointment System

DOS has been working on piloting a web-based appointment system that would be available for global use through a single Internet portal. It piloted 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.¹³⁰

Remote Data Collection, Video Conferencing Technology, Remote Adjudication and Other Initiatives

DOS has been exploring technological developments such as remote data collection and visa adjudication and interview via digital videoconference.

Pilot tests of remote data collection at several locations in the United Kingdom, Japan and Samoa demonstrated that the technology is not fully mature and DOS must still address technical issues concerning data transmission and security, as well as legal issues before it can incorporate remote adjudication into a workable visa system.¹³¹

DOS also successfully piloted a digital videoconferencing project between London and Belfast to see how it could 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 to the only, or one of the few, consular posts in their country for the visa interview. DOS has some concerns regarding technical and security issues that must be resolved before considering wider application of this technology, including ensuring that the video image on the screen and the fingerprint data sent in remotely belong to the same applicant.¹³²

DOS continues to put new systems in place designed to improve efficiency. It is currently developing a Consolidated Visa System that will incorporate all of its current NIV and IV processing systems into one.¹³³ DOS is also moving towards all-electronic correspondence, similar to what NVC does with the majority of communication with IV petitioners and applicants. DOS expects to make all correspondence for the Diversity Visa Lottery (DV) program fully electronic by 2009.¹³⁴

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

¹²⁸ *Id.*

¹²⁹ “Elimination of the “Application Received Stamp,” *supra* note 107. DOS has also amended 9 FAM 41.121, instructing posts to collect any valid corresponding I-94 card from the applicant. In addition, in order to alert DHS, posts must also mark the back of the I-94 card with the date and post name and return the I-94 to DHS. *Id.*

¹³⁰ See “DOS Answers to AILA’s Questions,” (Mar. 23, 2006), *supra* note 12.

¹³¹ See Testimony of Deputy Assistant Secretary of State for Visa Services, Stephen A. “Tony” Edson, Mar. 20, 2007, *supra* note 109.

¹³² See Testimony of Deputy Assistant Secretary of State for Visa Services Stephen A. “Tony” Edson, Feb. 7, 2008, *supra* note 27.

¹³³ *Id.*

¹³⁴ *Id.*

and serve as a reliable sounding board for innovative travel facilitation and security-related programs.¹³⁵

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

The passage of the Homeland Security Act of 2002¹³⁶ 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, 2003.¹³⁷ 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.¹³⁸ 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.¹³⁹

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.¹⁴⁰ Under this provision, once a person is denied a visa, no subsequent visa 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.¹⁴¹ The person may not be admitted to the United States without a visa issued in accordance with these procedures.¹⁴²

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

¹³⁵ *Id.*

¹³⁶ See Homeland Security Act, *supra* note 3.

¹³⁷ 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).

¹³⁸ Employees of DHS who are assigned overseas shall perform the following functions: (1) Provide expert advice and training to consular officers regarding specific security threats relating to the adjudication of individual visa applications or classes of applications; (2) 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 (3) 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 137. 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

continued

Casablanca, Morocco; Jakarta, Indonesia; Abu Dhabi, United Arab Emirates; Cairo, Egypt; and Singapore.

¹³⁹ *Id.*

¹⁴⁰ See Homeland Security Act, *supra* note 3.

¹⁴¹ *Id.*

¹⁴² *Id.*

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.”¹⁴³

Therefore, when an applicant applies for a non-immigrant 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.¹⁴⁴

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 policies 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. 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 complexity of consular practice. Knowledge of immigration petition filing procedures is not sufficient to ensure visa issuance at consular posts abroad. 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. The practice of immigration law now requires 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. The government now has access to far more data, and moreover this data is stored eternally. This data is also being shared with other government

¹⁴³ 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.

¹⁴⁴ 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 lack of domestic security checks for sensitive technology transfers on change-of-status applications filed with USCIS.

agencies. Visa practice now goes beyond mere work authorization and travel issues. The focus on foreign nationals and their activities has also 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, the government’s attempt to balance national security concerns with legitimate travel needs still leaves many visa applicants facing unpredictable delays and a myriad of potential pitfalls. Attorneys and visa applicants are therefore advised to plan ahead, research the requirements of the consular post and be ready to present documentation and explanations regarding the purpose of their proposed travel, and explanations relating to their past activities. With the primary goal of enhancing security, the consular framework has changed dramatically over the past few years. The new rules, regulations, and procedures, together with increased scrutiny and the enhanced use of biometrics and security advisory opinions, together with increased database sharing between DOS, USCIS, and intelligence agencies has changed the playing field. These new developments, when combined with unpredictable differences between consular posts, has dramatically changed the consular visa issuance 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).¹⁴⁵ 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.¹⁴⁶ 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.¹⁴⁷ 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 completed.¹⁴⁸ 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.¹⁴⁹ Generally, visa refusals fall into two

¹⁴⁵ Enhanced Border Security and Visa Entry Reform Act of 2002, Pub. L. No. 107-173, 116 Stat. 543 (2002).

¹⁴⁶ Border Security Act §§202 and 203 relate to CHIMERA, while §201 includes the provision requiring database sharing between government agencies.

¹⁴⁷ 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).

¹⁴⁸ 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.

¹⁴⁹ *See* “Visa Process Should Be Strengthened as an Antiterrorism Tool,” (GAO Report Oct. 2002) *supra* note 15.

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).¹⁵⁰

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 and is generally updated on a daily basis.¹⁵¹ 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.¹⁵² 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.¹⁵³ 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.¹⁵⁴ 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 began 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.¹⁵⁵

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.

¹⁵⁰ See W. Rosner and M. Ritter, "How to Find Out What Government Records Contain About Your Client," 1 *Immigration & Nationality Law Handbook* 47 (1998–99 Ed.).

¹⁵¹ 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>.

¹⁵² See M. Lawler, "Security Checks Conducted by DHS/INS and DOS," in *Professionals: A Matter of Degree*, Fourth Ed. 60 (AILA 2003).

¹⁵³ *Id.*

¹⁵⁴ 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,

continued

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).

¹⁵⁵ See GAO Report (Sept. 2004) *supra* note 63.

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, Sudan, and Syria ("T-4" 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.

"T-4" countries: The "T-4" countries are those identified as state sponsors of terrorism – originally Iran, Iraq, Syria, Libya, Sudan, North Korea and Sudan. Iraq, Libya and North Korea have been removed from the list, leaving the "T-7" as the "T-4."

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.¹⁵⁶

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.

¹⁵⁶ See Testimony of Assistant Secretary of State for Consular Affairs Maura Harty, Jan. 26, 2004, *supra* note 11.

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 screened or stopped anywhere in the federal system. TSC receives 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 provides TSC with information about purely domestic terrorism. TSC consolidates this information into an unclassified terrorist screening database (Terrorist Screening Database (TSDB)) and makes it available to queries for federal, state, and local agencies for a variety of screening purposes. TSC, through the participation of DHS, DOJ, DOS, and intelligence community representatives determines which information in the database will be available for which types of screening. 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 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 Bear: SAO for officials and diplomatic visa applicants.

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 T-4 country.

Visas Donkey: is an SAO triggered by a name hit that is not based on nationality or a criminal history.

Visas Eagle: SAO used for immigrants from certain former and current Communist countries.

Visas Horse: SAO used for official visitors.

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

Visas Merlin: SAO performed for refugee applications.

Visas Pegasus: SAO used for official visitors.

VVP (Visas Viper Program): VVP 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.