THE LAND OF CLASS, TIPOFF, MANTIS, CONDORS, AND DONKEYS

DEMYSTIFYING SECURITY ADVISORY OPINIONS, BIOMETRICS, AND GOVERNMENT DATABASES INVOLVED IN THE CONSULAR PROCESSING FRAMEWORK

by Tien-Li Loke Walsh[*]

Since 9/11, numerous measures designed to enhance security and streamline visa processing have been implemented. This has resulted in increased coordination between law enforcement, intelligence, and other government agencies—Department of State (DOS), Department of Homeland Security (DHS), Federal Bureau of Investigations (FBI), Central Intelligence Agency (CIA), National Security Agency (NSA) to name a few—with a particular focus on interagency data sharing, implementation of an integrated entry-exit system, and biometric collection. The steady stream of changes include the introduction of additional security clearance procedures for "List of 26" nationals from predominantly Muslim countries and "Terrible 6" countries; increasing applicability of security checks related to the Technology Alert List (TAL); and a marked increase in scrutiny of criminal histories and visa violations. Although many of these measures were expected after 9/11, visa applicants, faced with an entirely new consular framework, routinely encountered unpredictable surprises that caused unexpected and lengthy delays in visa issuance. Following a restrictive and frustrating period, we are only now starting to see a softening in policy and the application of a more rational and focused approach in consular processing.

As part of the coordinated efforts between government agencies, DOS has streamlined its visa application procedures and improved the security advisory opinion (SAO) process as well as processing times, thereby increasing efficiency and providing attorneys, visa applicants, and employers with a degree of predictability. Nevertheless, this different consular processing framework still provides numerous challenges to practitioners.

Have you ever wondered what a "hit" is? What are the different databases and to which law enforcement and intelligence agencies' are databases linked? Where does the information in a database come from? And what about these SAOs—Condors, Mantis, Donkeys, Eagles—why does DOS use these silly animal names? Have you ever wondered why your client has a "hit" when he or she has no criminal background or history of visa violations? Why can't these SAOs be processed ahead of time? What does it mean if an SAO is initiated?

This article hopes to demystify some of the processes by providing a general background to the different databases, the variety of SAOs, and the processes involved when a security check is initiated. Following are just some of the most commonly used terms that are associated with database sharing and security checks initiated by law enforcement, intelligence, and other government agencies.

WHAT IS A "HIT?"

A "hit" is when there is a match in one of the government databases for a foreign national. Hits can be based on name matches on terrorist lookout lists, potential security risks, prior visa problems such as overstays or denials, and criminal arrests or convictions. Even the result of a "close" name match with a suspected terrorist or criminal who has a similar name, date of birth, or place of birth could cause a hit.

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,

[*]

Tien-Li Loke Walsh is a senior attorney with Wolfsdorf Associates who practices exclusively in the area of immigration and nationality law. She is currently serving her second term on the AILA/DOS Liaison Committee and previously served two terms on the AILA/CSC Liaison Committee. She is listed in the *International Who's Who of Corporate Immigration Lawyers*. She completed her undergraduate studies at the University of Sydney, Australia, and received her J.D. from Boston University School of Law.

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).[1] 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.[2] CHIMERA ties together the 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.[3] 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.[4] 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.[5] Generally, visa refusals fall into two categories. A Category I refusal is one based on INA §§212(a)(1)(2)(3)(6) or (8), and a Category II refusal is one that can be overcome by additional evidence. A category I refusal must be entered in CLASS, as must any refusals under INA §214(b).[6]

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.[7] 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

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

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

[3] 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 Immigration Bulletin* 105 (Jan. 15, 2003) (hereinafter Sindelar).

[4] 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.

[5] *See* "Border Security: Visa Process Should Be Strengthened as an Antiterrorism Tool," Report to the Chairman, Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform, House of Representatives (Oct. 2002) by the United States Government Accountability Office, *posted on* AILA InfoNet at Doc. No. 02110545 (Nov. 5, 2002) (hereinafter Visa Process Should be Strengthened as an Antiterrorism Tool).

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

[7] *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*.

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.[8] 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.[9] 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 U.S. Citizenship and Immigration Services (USCIS) service centers and are valid for 90 calendar days.[10] This means that an IBIS check need not be repeated as long as adjudication of the application or petition occurs within 90 days of the prior IBIS check. However, if at the time of adjudication, the record does not contain evidence of an IBIS check conducted within the preceding 90 days, a check must be completed and incorporated in the record.

IDENT (Automated Biometric Fingerprint Identification System): This is DHS's automated fingerprint system, which begin operating in 1994 and is separate from the FBI's automated fingerprint identification system—IAFIS. 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 approximately six million illegal aliens who have been apprehended by DHS and enrolled in IDENT since it was deployed.[11]

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.

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

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

[9] *Id.*

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

[11] *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 United States Government Accountability Office, at 5 (hereinafter State Department Rollout of Biometric Visas); *see also* IDENT/IAFIS: The Batres Case and the Status of the Integration Project, Office of the Inspector General (Mar. 2004) at 2 (hereinafter, IDENT/IAFIS: The Batres Case).

applications that fall within these categories. The IPASS proposal is currently under review by DHS.

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

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

NCIC (National Crime Information Center): Created by the FBI in 1967, the NCIC was initially a national database of information on wanted individuals and stolen articles, vehicles, guns, and license plates. The NCIC and its sister system, the National Law Enforcement Telecommunications System (NLETS) contain a multitude of criminal history information and outstanding warrants submitted by participating federal, state, and local law enforcement agencies ranging from relatively minor shoplifting incidents to more serious offenses in the wants and warrants database. Criminal history is maintained in the Interstate Identification Index (III). Fingerprint information is maintained in IAFIS. Information in III can be accessed by name or FBI number through an NCIC terminal. The same information in III can also be accessed via fingerprint submission to IAFIS.[12] NCIC hits are discussed in detail later in this article.

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, 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.[13] The TAL was designed to assist in the

[12] IDENT/IAFIS: The Batres Case, *supra* note 11, at 8.

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

The critical fields list which constitutes the Technology Alert List (TAL) is as follows: (A) Conventional Munitions: technologies associated with warhead and large caliber projectiles, reactive armor and warhead defeat systems, fusing, and arming systems, electronic countermeasures and systems, new or novel explosives and formulations, automated

continued

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 pathogenecity, Freeze-drying (lyophilization), Fermentation technology, Cross-filtration equipment, High "DOP-rated filters" (*e.g.*, HEPA filters, ULPA filters), Microencapsulation, Aerosol sprayers and technology, aerosol and aerosolization technology, Spray or drum drying technology, Milling equipment or technology intended for the production of micron-sized particles, Technology for eliminating electrostatic charges of small particles, Flight training, Crop-dusting, aerosol dissemination, Unmanned aerial vehicle (UAV) technology, Fuses, detonators, and other munitions technology, Submunitions technology, Computer modeling of dissemination or contagion, Chemical absorption (nuclear-biological-chemical (NBC) protection). In the chemical area, includes Organophosphate 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.

continued

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

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

"Terrible 6" countries: The "Terrible 6" refers to countries identified as state sponsors of terrorism—currently designated as Cuba, Iran, Libya, North Korea, Sudan, and Syria. Iraq was removed from the list in October 2004, since Iraq is under "U.S. control," but Iraqi nationals still undergo extensive security checks.

High density graphite is used in missile nosetips, jet vanes and nozzle throats. Selected specialty materials (*i.e.*, stealth and the performance of these materials) provide critical capabilities that exploit electromagnetic absorption, magnetic, or superconductivity characteristics. These technologies are associated with advanced metals and alloys, Non-composite ceramic materials, Ceramic, cermet, organic and carbon materials, Polymeric materials, Synthetics fluids, Hot isostatic, Densifications, Intermetallic, Organometals, Liquid and solid lubricant, Magnetic metals and superconductive conductors; (J) Information Security: Technologies associated with cryptography and cryptographic systems to ensure secrecy for communications, video, data and related software; (K) Laser and Directed Energy Systems Technology: Lasers have critical military applications, including incorporation in guided ordinance such as laser guided bombs and ranging devices. Directed energy technologies are used to generate electromagnetic radiation or particle beams and to project that energy on a specific target. Kinetic energy technologies are those used to impart a high velocity to a mass and direct it to a target. Directed energy and kinetic energy technologies have potential utility in countering missiles and other applications. Look for technologies associated with Atomic Vapor Laser Isotope Separation (AVLIS), Molecular Laser Isotope Separation (MLIS), High Energy Lasers (HEL) (*i.e.*, laser welders), Low Energy Lasers (LEL), Semiconductor lasers, Free electron lasers, Directed Energy (DE) systems, Kinetic Energy (KE) systems, Particle beam, beam 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 antisubmarine 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; (O) Urban Planning: Expertise in construction or design of systems or technologies necessary to sustain modern urban societies. (PLEASE NOTE: Urban Planning may not fall under the purview of INA §212 (a)(3)(a), U.S. technology transfer laws, or any other U.S. law or regulation. However, Urban Planning is a special interest item and posts are requested to refer such visa application requests to CA/VO/L/C for further review.) Technologies/skills include Architecture, Civil engineering, Community development, Environmental planning, Geography, Housing, Landscape architecture, Land use and comprehensive planning, and Urban design. *See* "State Dept. Updates Guidance on Technology Alert Checks," *posted on* AILA InfoNet at Doc. No. 03030449 (Mar. 4, 2003).

continued

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.

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

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

US-VISIT (United States Visitor and Immigrant Status Indicator Technology): This program is designed to collect and share information on foreign nationals traveling to the United States, providing the government with capability to record the entry and exit of non–U.S. citizens into and out of the United States.

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

Visas Mantis: Is an SAO triggered by the TAL designed to prevent the transfer of sensitive, dual-purpose technologies. The Visas Mantis is discussed in detail later in the article.

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

DATA SHARING BETWEEN GOVERNMENT AGENCIES

Since 9/11, DOS and other U.S. government agencies, including the CIA, FBI, and NSA have consulted in an extensive and ongoing review of visa issuing procedures. Over eight million records from the FBI's NCIC have been incorporated into CLASS, more than doubling the records on file to 18 million.[14] Additional name check records from the intelligence community through TIPOFF, along with data from the U.S. Marshals Service, were also incorporated into CLASS.[15] In addition, the CLASS and TIPOFF databases interface with IBIS, TECS II, NAILS, NIIS, the TSC, and the TTIC, which integrates and maintains the terrorist watchlists. All of this information, which is constantly updated, includes information on terrorists and foreign warrants, but also extensive information about any criminal convictions or arrests including relatively minor offenses for DUIs or shoplifting, and together with the CCD, provides

[14] *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.*

[15] *See* "Initiatives by the Bureau of Consular Affairs to Enhance National Security," Fact Sheet, Bureau of Consular Affairs, Washington, DC (Sept. 5, 2002), *available at www.state.gov/coalition/cr/fs/13316.htm*.

consular officers with access to critical information during the visa interview process.

WHAT ARE ALL THESE SECURITY CHECKS?

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, 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 distinction between 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) DOS to the various police and intelligence agencies—hence the avian code names. SAOs are differentiated by animals that "walk-in," and thus, require DOS action and response (*e.g.*, Visas Donkey or Visas Bear).[16]

Since 9/11, DOS has made significant changes and improvements to its system of SAOs. If an SAO is initiated, consular posts must now wait for an affirmative response from all appropriate government agencies prior to issuing a visa. In FY2003, DOS estimates that there were approximately 212,000 SAO cases processed, accounting for about 2.2 percent of all visa applications;[17] in FY2004, close to 200,000 SAOs were processed, including about 57,000 Condors and 18,000 Mantis cases.[18]

The following are some of the most common security checks that are initiated by consular posts.

"Visas Condor" Security Checks

Initiated on January 26, 2002, the Visas Condor SAO focuses on potential terrorism applicants, particularly males between the ages of 16 and 45 years of age. 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 extensive 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 such that additional security measures are initiated for applicants born in one of the "List of 26" or "Terrible 6" countries, and not just to citizens of those countries.[19]

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

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

[17] *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 Government Accountability Office, at 9, fn. 16 (hereinafter Improvements Needed To Reduce Time Taken to Adjudicate Visas for Science Students and Scholars). Between April and June 2003, the GAO reviewed approximately 5,000 SAOs; basing its sample on 71 of the 2,888 Visas Mantis SAOs. The GAO based its report in part, by observing visa operations and analyzing data obtained at seven consular posts in three countries—China, India, and Russia. These countries were chosen because they are a major source of science students (F-1) and scholars (J-1) visiting the United States. *Id.* at 2. Interestingly, the top four countries for foreign students and exchange visitors in FY2003 are South Korea (34,697 F-1s issued; 8,119 denied; 14,218 J-1s issued; 1,507 refused); China (mainland and Taiwan) (31,322 F-1s issued; 22,995 refused; 10,171 J-1s issued; 7,003 refused); Japan (25,962 F-1s issued; 1,387 refused; 11,377 J-1s issued; 305 refused); and India (20,320 F-1s issued; 17,973 refused; 5,311 J-1s visas issued; 1,718 refused). *Id.* at 9.

[18] *See* "DOS Answers to AILA's Questions," (Mar. 17, 2005), *to be posted on* AILA InfoNet.

[19] *See* "The Consul and the Visas Condor" (Dec. 4, 2002), *posted on* AILA InfoNet at Doc. No. 03012240 (Jan. 22, 2003), where AILA's Department of State Liaison Committee held an informal, off-the-record conversation with a senior visa officer at a U.S. consular post abroad on December 4, 2002. Interestingly, even if an applicant who is a citizen or national of a "List of 26" or "Terrible 6" country is refused a visa, consular officers will "send a Visas Condor anyway, because Washington wants to know about any interest by anyone from the 7 countries visiting the U.S." *Id.*

Based on experience, it appears that citizens or nationals from the List of 26 countries where there are few surnames or name similarity is common (*e.g.*, Patel, Mohammad Ali, Mohammad Siddiqui, etc.) create the most problems for consular posts. If there is a "hit" in the system and if there is no clarifying information such as a date of birth, a consular officer has no choice but to initiate a Condor security check. Additionally, any individual who has spent time, whether for short visits or extended assignments or periods as a minor (a common scenario involves the children of European "colonials" who were born in or spent part of their childhood in former Commonwealth colonies such as Malaysia, or where parents worked in the oil business and a child grew up in Saudi Arabia despite having European citizenship) in a "country of concern," could be subject to a Condor SAO.

At the end of 2003, DOS provided consular posts with additional factors and guidelines to consider when faced with potential Condor situations, but the guidance remains classified. However, it appears that this guidance has proven useful to consular posts. Anecdotal reports indicate that by mid-2004, applicants from some of these countries have not been subjected to Condor SAOs and receive their visas within normal nonimmigrant visa processing times.[20]

If a Condor SAO is required, DOS requires posts to wait for an affirmative response from all participating agencies prior to issuing a visa.[21] DOS currently reports that the average processing times for Condor SAOs is approximately 30 days. To date, there is no system to expedite these security checks. However, if a security check has been pending for over 45 days, counsel may call the VO public inquiries number at (202) 663-1225. E-mail inquiries via *legalnet@state.gov* are no longer accepted.[22]

NCIC Checks

As a result of increased database sharing between government agencies, consular posts have been inundated with "hits" from the millions of names added to the NCIC database, revealing criminal convictions including minor offenses such as simple DUIs and shoplifting. The NCIC check is now integrated into the CLASS name check that is performed on every visa applicant. Since DOS is not a law enforcement agency, consular posts do not have access to detailed information explaining the reason underlying the "hit." If an applicant's name is identified as a "hit," posts will request an appearance by the applicant in order to obtain a full set of fingerprints, which are submitted for further analysis to the FBI. The FBI is currently taking approximately two to four weeks to complete these checks. Although attorneys have attempted to be proactive and expedite the process by submitting copies of arrest records, final court dispositions and attorney-initiated FBI results at the initial visa application, consular officers are required to obtain fingerprints in any case of a NCIC name check "hit."[23] Once a post has received a response from the FBI via the National Visa Center, it may, at the consular officer's discretion, accept documentation from the applicant that matches the extract provided by the FBI.[24] However, consular posts will not accept submission of all related documents in lieu of initiating required security checks and fingerprinting.

"False hits" are the biggest headaches for unsuspecting visa applicants. Unfortunately, anecdotal reports confirm that there have been an alarming number of false hits caused by similar or identical names, especially when the applicant is from a country where there are few surnames and name similar-

[20] 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), *to be posted on* AILA InfoNet.

[21] When first implemented, Visas Condor cables were sent to the FBI, CIA, the Department of Defense (DOD), and NSA. *See* Visa Process Should Be Strengthened as an Antiterrorism Tool, *supra* note 5, at 21–22. In September 2002, the FBI became the primary agency for conducting the name checks and clearing Condor cables, and the CIA started conducting name checks for selected Condor applications rather than all of them. According to CIA and DOJ officials, under the new procedures, the FBI's Name Check Unit conducts the initial Condor name checks, which involve running the applicant's information against their databases at headquarters, and in some cases, at the Foreign Terrorism Tracking Task Force (FTTTF). If these checks result in a possible match, then the FBI sends the information on the visa applicant to DOS, which then forwards it to the CIA. *Id.* at 24.

[22] *See* "DOS Answers to AILA's Questions," (Mar. 17, 2005), *to be posted on* AILA InfoNet. DOS is currently developing a system that would allow attorneys/applicants to follow up on an overdue SAO.

[23] 22 CFR §41.105 (b)(2); *see also* "DOS Answers to AILA Questions" (Oct. 2, 2002), *posted on* AILA InfoNet at Doc. No. 02100340 (Oct. 3, 2002).

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

ity is quite common. Sometimes a "hit" can be the result of name similarity, where the database is missing pertinent identifying information such as a date of birth or place of birth, but based on the name similarity, a security check must be completed. Approximately half of the names in the NCIC database are Latino and this has resulted in an alarming number of false hits for individuals with common Latino names. Applicants with such hits are not provided with an opportunity to show that they are not the same person as that on the database.[25] To date, there is no way to initiate the security check in advance of a visa application.[26]

DOS hopes that the worldwide deployment in summer 2005 of the software for electronic fingerprinting will improve processing times. This program will allow posts to capture digital fingerprints that are forwarded electronically to the FBI to compare with possible NCIC records.[27]

Other "Hits" in the System Resulting in a Visa Refusal[28]

If there is a "hit" in the system where an applicant is identified as the subject of a DHS-generated lookout entry indicating a definitive determination of inadmissibility, a consular officer may assume it is accurate and may proceed to refuse issuance of the visa, unless the eligibility is nonpermanent and can be overcome through changed circumstances (*e.g.*, medical or public charge ineligibilities), or the entry is based on an issue eligibility that is relevant only to ports of entry, and is not a basis for visa refusal (*e.g.*, under §212(a)(7)). Except in cases involving nonpermanent ineligibilities, the consular officer is not to look behind a definitive DHS finding or readjudicate the alien's eligibility with respect to the provision of inadmissibility described in the DHS lookout entry. If the entry is a "quasi-refusal" ("P" or provisional) lookout, the entry is not binding and an officer can evaluate the derogatory information and can adjudicate an alien's eligibility for the visa. If the consular officer issues the visa, it is supposed to be notated to alert a CBP officer that the consular officer was aware of the "hit" and otherwise concluded that the alien was eligible for the visa.[29]

The Technology Alert List (TAL) and Visas Mantis Security Checks

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

[25] 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 157, the provision of this information does not necessarily prevent a wary consular officer from initiating a security check on a discretionary basis.

[26] *See* "DOS Answers to AILA Questions" (Oct. 2, 2002), *supra* note 23.

[27] DOS launched the pilot program in Mexico City, then Ciudad Juarez, Monterrey, and Guadalajara. Initial reports confirm that these pilot program posts have been able to complete the check within the same day for false hits (usually within one to two hours), while clearances for positive hits are received within two days.

[28] While beyond the scope of the article, for two excellent articles that address the problem with lookout systems and provide critical guidance on how to challenge and remove a lookout entry, *see* T. Murphy & P. Larrabee, "Lookout! The Ever-Expanding Universe of Data: What To Do When Your Client is NAILed," 1 *Immigration & Nationality Law Handbook* 162–70 (2003–04 ed.) and R. Sindelar, *supra* note 3.

[29] *See id.* at 107. Furthermore, if an alien with a definitive DHS entry wishes to pursue his or her application, he or she will require a waiver of ineligibility from DHS (if available). *If* the alien maintains that the DHS finding was erroneous, the consular officer should generally advise the applicant to contact DHS directly to request reconsideration of the finding of ineligibility and deletion of any lookout. However, a consular officer may choose to contact DHS on behalf of the applicant in appropriate cases, such as where important U.S. interests are at stake or where the consular officer has information that could assist DHS in reconsideration of the case. Moreover, there is no purpose in issuing a visa without a waiver when there is a DHS ineligibility determination, since the applicant will become subject to removal at the port of entry. DHS has indicated that it may be possible to correct erroneous ineligibility determinations by filing for a correction of record pursuant to the provisions of 8 CFR §103.28. As provided in 9 FAM §40.6, Note 3.3, if, after the consular officer has refused an application based on a definitive DHS lookout entry, DHS determines that the finding was erroneous and deletes its entry, then the consular officer may process the case to conclusion.

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.[30] 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 or regimes. The increasing sophistication of off-the-shelf technology, dual-use technologies (technologies which have both civilian and military applications), allegations of lack of sufficient information about and controls on foreign students in the United States, recent tensions in the Middle East, and the 9/11 terrorist attacks have combined to renew concern among the law enforcement and intelligence communities that controlled U.S.-origin goods and information are vulnerable to theft.

The revised TAL consists of two parts: a "Critical Fields List" (CFL) of major fields of technology transfer concern, including those subject to export controls for nonproliferation reasons; and the DOS's list of designated state sponsors of terrorism, also known as the "Terrible 6" countries. While restrictions on the export of controlled goods and technologies applies to scientific and technical visitors from all countries, DOS instructs posts that applicants from the "Terrible 6" countries seeking to engage in one of the critical fields warrant special scrutiny and mandatory SAO checks.[31]

In comparison to the previous version, the updated TAL includes a vastly expanded list of associated technologies within each critical field, which details virtually every potential "dual use" application, where seemingly benign technologies have potential military applications. For example, the updated TAL includes a Chemical, Biotechnology, and Biomedical Engineering critical field—an all-encompassing list that includes almost every possible associated technology or skill involving chemistry, biochemistry, immunology, microbiology, pharmacology, genetic engineering, and chemical engineering to name a few. With such an all-inclusive list, nearly every research scientist, physician, academic, or engineer involved in any of these fields in commercial research laboratories, educational institutions and universities, or private industry may be subject to a TAL security check by a post erring on the side of caution.[32]

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

In all cases, consular officers must determine whether an applicant proposes to engage in advanced (doctoral, postdoctoral, or research scholar) research or studies, or business activity involving any of the scientific/technical fields listed in the Critical Fields List. The cable instructs posts that information in the public domain, *i.e*,. widely available to the public and information presented in an academic course generally is not relevant for U.S. technology transfer control purposes. Although the cable urges consular officials to use their judgment, it cautions officers to err on the side of caution if there are any doubts that any of the applicant's planned activities raise questions of possible ineligibility under INA §212 (a)(3)(A). If in doubt, consular officers must submit an SAO in the form of a Visas Mantis.[33] If a determination is made that the

[30] *See* "State Dept. Updates Guidance on Technology Alert Checks," *supra* note 13.

[31] *Id.*

[32] *Id.*

[33] 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, the

continued

technology involved presents a security risk, the applicant may be permanently barred under INA §212(a)(3)(A), which is nonwaiverable.

Despite this guidance, it appeared that the cable failed to provide consular posts and attorneys with clear direction[34] as to when an SAO is required and in fact, seemed to signal a bureaucratic shift towards initiating TAL SAO requests for all cases unless posts are absolutely sure the applicant will not be engaged in any of the technologies or skills listed on the TAL. In response to concern and criticism about the lack of clear guidance about the TAL, the DOS confirmed that the TAL guidance was significantly revised and shared with the field via cable on October 1, 2003, but it remains classified.[35] Interestingly, the TAL has recently been removed from the DOS website.[36]

The Visas Mantis Process

If a Mantis SAO is required, consular posts will transmit the request to the Visa Office (VO) at DOS and interested agencies.[37] In July 2004, the FBI, DOS, and DHS reached an agreement that fundamentally changed the FBI's role in the Visas Mantis process.[38] Officials from these agencies made a determination that the FBI could fulfill its law enforcement role in the Mantis process without routinely clearing Mantis cases. Under the new "no objections" policy, DOS does not have to wait for an FBI response before processing Mantis cases, but the FBI continues to receive information on visa applicants subject to Mantis checks.[39] Prior to this

spouse; project descriptions; annual reports; and letters of recommendation from a U.S. source or from abroad can be useful in helping to flesh out an applicant's real motives for travel. The cable instructs posts that such documents should be described in the SAO and held until the case has been closed. DOS encourages consular officers to provide as much information and details as possible in the SAO. *Id.*

[34] The GAO Report ("Improvements Needed To Reduce Time Taken to Adjudicate Visas for Science Students and Scholars") 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. *See* Improvements Needed To Reduce Time Taken to Adjudicate Visas for Science Students and Scholars, *supra* note 17, at 16.

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

[36] 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 (10/13/04)" *posted on* AILA InfoNet at Doc. No. 04120760 (Dec. 7, 2004).

[37] *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, *available at http://travel.state.gov/testimony10.html.*

[38] *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 United States Government Accountability Office, at 13, *posted on* AILA InfoNet at Doc. No. 05022266 (hereinafter Streamlined Visas Mantis Program).

[39] 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 Visa Office received twice a week. The CD is an 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 Visa Office'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 37. This policy resulted in a backlog of almost 1,000 cases and contributed to lengthy wait times for

continued

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

Under the current process, the other government clearing agencies are given 10 working days to respond to SAOs, but notify the Visa Office when they need additional time to clear a specific case.[40] 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.[41] According to DOS, waiting for highly classified reports through appropriate channels can be another reason for delay in responding to a consular post.[42] Once DOS receives all agency responses pertaining to the applicant, it summarizes them and prepares a response to the consular posts.[43] A cable is then transmitted to the post that indicates if DOS does or does not have an objection to issuing the visa, or that more information is needed.[44]

When initially introduced, there was extensive concern that delays in Mantis checks were impacting the business, academic, and scientific communities, and causing disruptions to ongoing research and commercial activities.[45] A February 2004, GAO Report ("Improvements Needed To Reduce Time Taken to Adjudicate Visas for Science Students and Scholars") found that interoperability problems among the systems that DOS and FBI use contributed to the delays in processing.[46] 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[47] at different points in the process.[48] In addition, feedback from officers at consular

applicants. In February 2004, it took the FBI an average of about 29 days to complete clearances on Mantis cases. In fact, FBI clearance often took longer than any other step in the Mantis process. The FBI's new role allows DOS to process Mantis cases more easily. It has also allowed DOS to clear about 1,000 Mantis cases on which FBI had maintained a "hold" for a lengthy period. *See* Streamlined Visas Mantis Program, *supra* note 38, at 14.

[40] Prior to this, the remaining agencies had 15 working days to respond to DOS. *See* Streamlined Visas Mantis Program, *supra* note 38, 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 to 17 days. *Id.*

[41] *See* Testimony of Janice L. Jacobs (Feb. 25, 2004), *supra* note 37.

[42] *Id.*

[43] *See* Improvements Needed To Reduce Time Taken to Adjudicate Visas for Science Students and Scholars, *supra* note 17, at 8.

[44] *Id.* at 8.

[45] The GAO found that visas for science students and scholars took, on average, 67 days from the date the SAO was submitted from post to the date DOS sent a response to the post. Furthermore, the GAO also found that as of October 1, 2003, 410 Visa Mantis cases submitted by seven posts in FY2003 were still pending after more than 60 days. In the sample, the GAO found that 67 of the visa applications completed processing and approval by December 23, 2002. In addition, three of the 67 applications had processing times in excess of 180 days. Four of the 71 sample cases remained pending as of December 3, 2003—of which three had been pending for more than 150 days and one for more than 240 days. *Id.* at 10–11. Based on the 5,000 SAOs received from consular posts between April and June 2003, 2,888 pertained to science students and scholars, of which approximately 58 percent were from China, 20 percent from Russia, and less than 2 percent from India. Of the 2,888 Visas Mantis cases identified during the sample time frame between April and June 2003, a total of 57 posts sent one or more Mantis SAOs to Washington. China accounted for 1762 SAOs (Shanghai sent 701; Beijing sent 600; Guangzhou sent 197; Chengdu sent 74; Shenyang sent 23; and Hong Kong sent 67 requests); Russia accounted for 567 SAOs (Moscow sent 505; St. Petersburg sent 37; Yekaterinburg sent 24; and Vladivostok sent one request). *See id.* at Appendix II at 31. The GAO based its report on a random sample of 71 cases from the 2,888 applications to measure the length of time taken at selected points in the visa process. *Id.*

Moreover, according to the FBI, Mantis SAOs are the most difficult to resolve because of the predominance of requests from China and commonality of Asian names. The majority of Chinese Mantis cases are, however, cleared within 120 days. Comments of Vincent Beirne, Deputy Chief, Advisory Opinion Division, Visa Office, Department of State at Technology Alert List & Export Control panel, 16th Annual AILA California Chapters Conference, San Diego (Nov. 2003).

[46] *See* Improvements Needed To Reduce Time Taken to Adjudicate Visas for Science Students and Scholars, *supra* note 17, at 10.

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

[48] According to Improvements Needed To Reduce Time Taken to Adjudicate Visas for Science Students and Scholars, a Consular Affairs official stated that in fall 2003, there were about 700 Visas Mantis cases sent from Beijing that did not reach the FBI for the security check. The official did not know how the cases got lost but told the GAO that it took Consular Affairs about a month to identify that there was a problem and

continued

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. In addition to processing delays, it appears that many applicants also experienced significant delays in scheduling appointments for interviews, which added to the delays in visa issuance.[49]

DOS acknowledges that backlogs occurred based on the overburdened system, which required extensive cooperation between multiple government agencies not yet equipped to cope with the Mantis procedures. As part of the efforts to streamline Mantis procedures, the DOS created a special Mantis team of five full-time employees in the Visa Office, exclusively dedicated to technology transfer cases.[50] In addition to creating a special Mantis team and developing an electronic system, DOS, DHS, and the FBI also took other action to improve the Mantis program, in response to the GAO's suggestions in February 2004. These steps include providing additional guidance and feedback to consular posts; clarifying the roles and responsibilities of agencies involved in the Mantis process, reiterating DOS's policy of giving students and scholars priority in scheduling of interview appointments and extensions in the validity of Mantis clearances.[51] All of these initiatives resulted in a decline in Mantis processing times.

However, according to the most recent GAO Report released in February 2005, some issues still remain.[52] Consular officers at key posts continue to have questions about how to identify applicants and apply Mantis SAOs.[53] The GAO also found that

provide the FBI with the cases. As a result, several hundred visa applications were delayed for another month. *Id.*

[49] According to Improvements Needed To Reduce Time Taken to Adjudicate Visas for Science Students and Scholars, the posts visited had an average waiting time of two to three weeks to receive an interview appointment. Interviews at one point in summer of 2003 took as long as 12 weeks in Chennai, India; New Delhi had a wait of two to three weeks; two of the three Chinese posts had a two-week wait for an interview, although one had a wait of about five to six weeks. *Id.* at 19. However, many of the posts facing delays undertook certain initiatives such as opening on weekends or reserving appointments for students and scholars, etc. to accommodate applications. *Id.* at 19. DOS also maintains that every spring as students begin applying for visas, DOS instructs all posts to make special arrangements to facilitate visa interviews for students and researchers. Some posts do not require appointments, some reserve appointment slots for students, and some assign specific days to student processing. *See* Testimony of Janice L. Jacobs (Feb. 25, 2004) *supra* note 37.

[50] *See* Streamlined Visas Mantis Program, *supra* note 38, at 11.

[51] More specifically, in 2004 alone, DOS added a special presentation on Visas Mantis to the nonimmigrant visa portion of the Basic Consular Training course; funded a trip by Nonproliferation and Consular Affairs officials to a regional conference in China to make presentations and hold discussions with consular officers on specific Mantis issues; organized a series of video-teleconferences with posts that submit large numbers Mantis SAOs to provide direct feedback to embassy and consular officers on the quality of their Mantis requests; began issuing reports to the field about Mantis policy and procedural issues to "help consular officers understand the Mantis program better, provide guidance on what cases should be submitted as Visas Mantis SAO requests and what information should be included in those requests, and to give feedback on the quality of those requests." The first quarterly report was issued in March 2004, followed by two or more in July and October. DOS also arranged one-on-one meetings with the CA and NP officers for new junior officers assigned to posts with high Mantis volumes; provided feedback to individual consular officers on the Mantis SAOs submitted; and established a classified webpage through the DOS's intranet for consular officers to gain access to country-specific and other useful information related to the Mantis program. *See* Streamlined Visas Mantis Program, *supra* note 38, at 11–12.

[52] *Id.*

[53] Despite DOS's efforts, the GAO found that consular officers at key posts still need additional guidance. Some consular officers are still confused about how to apply the Mantis program. Officers in Beijing consistently told the GAO that they needed more clarity and guidance regarding how to use TAL. According to a key official in Beijing, because these officers do not have a scientific or technical backgrounds, they often do no understand what entries on the TAL mean or whether the visa applicant has advanced knowledge about the subject he or she plans to study in the United States. They are also confused about how to apply vague, seemingly benign categories. For example, consular officers in Beijing did not know whether to continue submitting Mantis requests for all individuals that fall under the category of "communications–wireless systems, advanced," even if the visa applicant works for a foreign multinational corporation that is not a Chinese government-owned telecom enterprise. Few of the consular officers that the GAO spoke to in China, Russia, and the Ukraine were familiar with the quarterly reports issued by Consular Affairs on Mantis issues. The only officer aware of the classified webpage maintained by the Consular Affairs Bureau told the GAO that he did not find it useful because it had very little information on it and because it was hard to access the classified computer, which was housed in a separate building from the consular section. The GAO also found that consular officers at the three posts did not have regular opportunities to interact with officials from the NP Bureau or the CA Bureau knowledgeable about the Mantis program. Although China accounts for more than half of the Mantis requests, only one of the six posts has held a video-teleconference. Kiev requested a video-teleconference in early

continued

continued

many posts are still not fully connected to DOS's electronic tracking system. As a result, consular officers still send Mantis cases both electronically and via cable, and some agencies still provide their responses via courier, leading to unnecessary delays.[54]

Based on its findings, the GAO recommended that DOS in coordination with DHS, develop a formal timeframe to complete full connectivity between all necessary U.S. agencies and bureaus; and provide additional opportunities for consular officials at key posts to interact directly with DOS officials responsible for the Visas Mantis program (including more frequent video-teleconferences, mandatory one-on-one meetings with officials knowledgeable about the program, and more visits by DOS officials to consular conferences).[55] According to DOS, they now have procedures for expediting individual cases when appropriate.[56]

DOS reports that the average processing time for Mantis checks as of March 2005, is approximately 14 days, which is significantly faster than the four- to six-month backlogs experienced by many in the past.[57] At any given moment, DOS has approximately 1,500 to 2,000 Mantis checks pending from the interagency review process.[58] Consular posts may not issue the visa until they receive an affirmative response from all participating agencies. If a Mantis clearance has been pending for over 45 days, one can call the Public Information office at (202) 663-1225.[59]

Validity of Visas Mantis Clearances Extended

On February 11, 2005, after interagency consultation with DHS, DOS extended the maximum validity of the Visas Mantis clearances for F-1, J-1,

2004, but had been unable to schedule one, as of December 2004. Finally, in Beijing, only one of the officers who had attended the consular conference was still at the post. *See* Streamlined Visas Mantis Program, *supra* note 38, at 16–18.

[54] Several law enforcement, intelligence, and nonintelligence agencies that receive Mantis cases, including the Departments of Commerce and Treasury, are not fully connected to the DOS's electronic tracking system. These agencies thus continue to receive Mantis cases through State's traditional cabling system. For the time being, officers send Mantis cases both electronically and via cable. The agencies that are responsible for routinely clearing Mantis checks provide their responses to DOS on CDs that must be hand-carried between the agencies, leading to further delays. DOS is working to establish full connectivity with other agencies; however, it has thus far failed to set a deadline for connectivity. In July 2004, DOS stated that it expected the FBI to begin relying on the network on a regular basis by the end of July 2004. DOS and the FBI also signed a Memorandum of Understanding (MOU) in July, outlining the terms of the FBI's electronic connectivity to the system. However, it was not until December 2004, that the FBI developed the ability to gain access to DOS's electronic tracking system to test the connection and discontinue use of the cabling system. Although the FBI no longer routinely clears Mantis cases, all agencies and bureaus that receive Mantis cases, regardless of whether they routinely clear cases, must be connected electronically to the system before use of the cabling system can be eliminated. DOS's goal was to establish connectivity to another intelligence agency responsible for clearing Mantis cases by the end of 2004, but an agency official told the GAO that a deadline of February 2005 was more realistic. However, DOS has not set milestones for connecting the remaining agencies that receive Mantis cases to the tracking system. *See id.*, at 17–18.

[55] *Id.* at 20.

[56] *See* Testimony of Janice L. Jacobs (Feb. 25, 2004), *supra* note 37. Prior to this testimony, DOS has always maintained that there are no procedures in place to expedite a Mantis SAO. The author is not yet aware of the specific procedures available to request an expedite.

[57] 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 in 51 *Chronicle of Higher Education*, Issue 7, at B10 (Oct. 8, 2004). By November 2004, the average processing time was only about 15 days. *See* Streamlined Visas Mantis Program, *supra* note 38, at 2. Data also shows a significant improvement in the number of Mantis cases pending for more than 60 days. In February 2004, the GAO found that 410 Mantis cases submitted by seven posts in China, India, and Russia had been pending for more than 60 days. Recent data provided by DOS indicates that as of October 2004, only 63 cases (or 9 percent of all pending Mantis cases) had been pending for more than 60 days. *Id.* at 7–8. In December 2004, only 81 cases out of more than 18,000 had been pending for more than 30 days. *See* "Student and Exchange visa Improvements," released by DOS as part of "DOS Answers to AILA's Questions," (Mar. 17, 2005), *to be posted on* AILA InfoNet.

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

[59] E-mail inquiries via *legalnet@state.gov* are no longer accepted. DOS is currently developing a system that would allow attorneys/applicants to follow up on an overdue SAO. *See* "DOS Answers to AILA's Questions," (Mar. 17, 2005), *to be posted on* AILA InfoNet.

H-1B, L-1, and B-1/B-2 visas.[60] This allows applicants to reapply for visas without undergoing frequent Mantis checks, if returning to the previous program of study or professional assignment. However, consular officers have discretion, if warranted, to initiate a Mantis SAO.

The validity period for F-1 applicants is up to the length of the academic program, to a maximum of four years. However, if the student changes programs, the clearance is no longer valid and an SAO will be initiated if the applicant applies for a new visa. H-1B, J-1, L-1, and O-1 applicants are eligible for clearances valid for the duration of their approved activity to a maximum of two years. If the nature of the foreign national's activities change, the clearance ceases to be valid and a new SAO is required. B-1/B-2 applicants can receive a Mantis clearance valid for one year, provided that that the original purpose for travel, as stated in the visa application has not changed on subsequent trips. The new clearance validity periods do not apply to applicants from state sponsors of terrorism.

These extended validities apply to any applicants who are reapplying for a visa within 12 months of the previously issued visa. DOS estimates that this change will allow the agency to cut in half the total number of Mantis clearances processed each year.[61] As before, consular officers may issue visas to applicants who have received Mantis clearance according to the applicant's reciprocity table, but in no case, for longer than 12 months.[62] Visas for Chinese and Russian Mantis applicants, which account for approximately 76 percent of all Mantis cases,[63] can only be issued single-entry visas valid for three months.[64]

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

DOS Improvements to the SAO Process

Based on the widespread problems encountered by participating government agencies in performing the various security checks, DOS made major changes in its use of electronic processing by developing a cable-less SAO process called the SAO Improvement Project (SAO IP).[65] DOS is in the midst

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

[61] *See* Streamlined Visas Mantis Program, *supra* note 38, at 16. The new validity periods are the result of negotiations between DOS, DHS, and the FBI. Although DOS and DHS proposed extending Mantis clearances in the summer of 2004, the FBI argued that an extension in Mantis clearances would significantly reduce its capability to track and investigate individuals subject to the Mantis program. The FBI maintained that without the same frequency of automatic Mantis notifications, it would have far less knowledge of when these individuals entered the country, where they go, and what they are supposed to do while in the United States. As a result, the FBI made its agreement conditional on receiving access to US-VISIT and SEVIS. In February 2005, the FBI and DHS reached agreement on the terms of FBI's access to these two systems, allowing the proposed extension of Mantis clearances to take effect. *Id.* at 16.

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

[63] China has one of the strictest visa reciprocity schedules for students and scholars. F-1 and J-1 applicants are limited to six-month, two-entry visas. However, DOS instructions to consular officers are to give single-entry, three-month visas to applicants who undergo Mantis checks. In 2004, DOS entered negotiations with Chinese government to revise the reciprocity schedule for business travelers, tourists, and students. However, in December, DOS informed the GAO that while the Chinese government agreed to extend visa validities for business travelers and tourists, it did not agree to do so for students and scholars. *See* Streamlined Visas Mantis Program, *supra* note 38, at 10.

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

[65] Testimony by Janice L. Jacobs (Feb. 25, 2004), *supra* note 37. In addition, DOS has also established a quality-control procedure with the Non-Proliferation Bureau (NP Bureau) to provide VO with feedback for posts regarding the information contained in Visas Mantis cables. The NP Bureau has started identifying cables that they have found well-prepared and contain all of the pertinent information NP analysts need to make an informed recommendation on visa eligibility. The NP Bureau also points out cables that do not contain sufficient information on which to reach a recommendation. It also calls to attention cables that have been submitted for applicants whose purpose of travel to the United States did not fall within the purview of the TAL. In all instances, NP's comments are passed on to the relevant post as a means of providing feedback and guidance to the post's officers. *See* Improvements Needed To Reduce Time Taken to Adjudicate Visas for Science Students and Scholars, *supra* note 17, at 44.

It is also providing expanded briefings on the Visas Mantis process to new consular officers at the National Foreign Affairs Training Center, including 12–15 hours of training devoted to the processing of SAOs, including Mantis. During this training, the NP Bureau, which reviews Mantis cases in

continued

of a $1 million project providing electronic interagency linkage aimed at improving efficiency between interagency processing. This includes the elimination of its traditional cabling system between consular posts and other federal government agencies in the SAO process.[66] The program uses real-time data-sharing, allowing for seamless electronic data transmission from posts, eliminating virtually all manual manipulation of data.[67] The other agencies will no longer receive a telegram (which is prone to cable formatting errors and misplacement of SAO requests), but a reliable data transmission through an interoperable network that begins with the CCD, which is expected to improve data integrity, accountability of responses in specific cases, and statistical reporting.[68] DOS hopes that posts will be able to forward cases to intelligence and law enforcement agencies as quickly as possible and eliminate any time period caused by processing by administrative staff. As of October 2004, DOS completed worldwide implementation of the SAO IP.[69] The SAO IP will operate through an interagency network known as the Open Source Information System (OSIS), which will provide interoperable data transmission.[70] Following initial interconnectivity problems between the FBI and DOS databases, the FBI is finally performing all name checks electronically through the CCD.[71] DOS is still at various stages with other SAO recipients in achieving connectivity to the CCD.[72]

BIOMETRIC TECHNOLOGIES

Section 303 of the Border Security Act mandates the use of biometric identifiers in all U.S. visas by October 26, 2004.[73] A biometric or biometric identifier is an objective measurement of a physical characteristic or personal behavior trait of an individual, which, when captured in a database, can be used to verify identity or check against other entries in a database. Some examples of features that can be measured for these purposes include the face, fingerprints, hand geometry, handwriting, iris, retina, and voice.

DOS, in conjunction with DHS, DOJ, and the National Institute of Standards and Technology (NIST) have studied the potential of biometric technologies in screening visa applicants and determined that the biometric identifier will consist of facial recognition (digital photographs) and fingerprint (two index fingerprints) technologies.[74] 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.[75] The inclusion of biometric data in travel records will also make it easier to replace lost or stolen travel documents.

DOS completed deployment of the Biometric Visa Program ahead of schedule and before the congressionally mandated deadline of October 26, 2004. As of October 7, 2004, all 207 NIV issuing posts

the Department, briefs on the proliferation threat and the importance of the Mantis screening process. *Id.* at 25; *see also* Testimony by Janice L. Jacobs (Feb. 25, 2004), *supra* note 37.

Finally, DOS is also monitoring resource needs at posts. To alleviate staffing concerns, temporary adjudicating officers are sent to the posts as needed. DOS will also add an additional 80 officers in 2004. However, the decision to add these new officers was made before the August 2003 Personal Appearance Waiver (PAW) policy and thus it is unknown if there are enough resources for the task at hand. *See* Improvements Needed To Reduce Time Taken to Adjudicate Visas for Science Students and Scholars, *supra* note 17, at 24. Add to this the implementation of the biometric visa program by October 26, 2004, which will undoubtedly overwhelm existing consular resources.

[66] *See* Testimony by Janice L. Jacobs (Feb. 25, 2004), *supra* note 37.

[67] *Id.*

[68] *Id.* The SAO IP allows DOS to more easily produce and track certain statistics, including the average SAO processing times, the number of SAOs submitted by each post, and the amount of time each step in the process is taking. *See* Streamlined Visas Mantis Program, *supra* note 38, 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.*

[69] It was hoped that the cables would be phased out by December 31, 2004, but it appears that some posts still continue to use cables. *See* "DOS Answers AILA Questions," *posted on* AILA InfoNet at Doc. No. 04120760 (Dec. 7, 2004); *see also* "DOS Answers to AILA's Questions," (Mar. 17, 2005), *to be posted on* AILA InfoNet.

[70] *See* Janice L. Jacobs testimony (Feb. 25, 2004), *supra* note 37.

[71] *See* "DOS Answers to AILA's Questions," (Mar. 17, 2005), *to be posted on* AILA InfoNet.

[72] *Id.*

[73] *See* Border Security Act, *supra* note 1.

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

[75] *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* Improvements Needed To Reduce Time Taken to Adjudicate Visas for Science Students and Scholars, *supra* note 17, at 36.

were collecting biometrics for nonimmigrant visas and all 125 IV issuing posts for immigrant and diversity visas.[76] The inkless fingerprint scanning generally takes approximately 30 seconds.[77] As soon as the fingerprints are enrolled, they are sent electronically, along with the digital photograph and biographic data, to the CCD in Washington. The CCD relays the fingerprint files to IDENT over a reliable, direct transmission line, which sends the results back to the CCD for relay back to the post.[78] The current turnaround time is approximately 30 minutes.[79]

IDENT searches for matches, triggering a response back to the post indicating a "hit" or no existing record (N/R). A "hit" means a person is on a watchlist or that the person has been previously entered into the system, either at a port of entry or by applying for a visa at a consular post. If the fingerprints match fingerprints provided by the FBI in the IDENT lookout database, the IDENT system returns to the post an FBI file number.[80] At present, consular posts do not have access to the FBI record associated with that file number.[81] If there is no match in the IDENT system, then the visa applicant's fingerprints are stored in IDENT and a fingerprint identification number (FIN) is returned to the post.[82] If the system cannot determine whether the applicant's prints match a set previously entered, the system sends the data to biometric experts to determine if a subject's print has a match or that there is no record in the system.[83] Until the information from IDENT is received, the visa system is locked with regard to that visa application. Once the visa has been issued, the nonimmigrant visa system sends to IBIS the issued visa data, including the visa applicant's photo and fingerprint identification number.[84]

Although the technological installation progressed smoothly due to a well-planned rollout of equipment and software and fewer technical problems than anticipated, a recent GAO Report recommended that DHS and DOS develop and provide comprehensive guidance on how the Biometric Visa Program should be used to help adjudicate visas and that DOS direct each consular post to develop an implementation plan based on this guidance.[85]

Although there was significant concern about the impact of the biometric collection program, most consular posts have successfully completed the transition without any significant delays in interview scheduling or visa issuance times.

However, the fingerprint analysis is only the first step in the biometric program. DOS is about to launch the facial recognition phase of the program, beginning with high-fraud posts. Facial recognition will initially be used for applicants who are currently not subject to biometric collection (*i.e.*, those under 14 years and over 79 years of age and diplomats), and also to any applicants from "Terrible 6" coun-

[76] "Completion of Biometric Deployment" (Oct. 8, 2004), *posted* AILA InfoNet at Doc. No. 05011962 (Jan. 19, 2005). According to DOS, it had 3,567 hits in DHS's IDENT watchlist since it began biometric collection, almost all of which were for wanted persons for immigration violations, or for criminal history records submitted by the FBI. Of these 3,567 IDENT watchlist hits, 1,434 did not have a corresponding CLASS category 1 hit and 3,324 did not exactly match the applicant's name or date of birth in the NIV or IV system. *Id.*

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

[78] *Id.*

[79] *See* State Department Rollout of Biometric Visas, *supra* note 11, at 4. According to DOS data gathered from February to August 2004, the total biometric visa process averaged about 30 minutes for an applicant's prints to be sent from a consular post to the CCD, then on to IDENT analysis, and then for the response to be returned to the post. However if "human analysis" is required, DHS has up to 24 hours to provide a response back to the post. *Id.* at 7.

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

[81] *Id.*

[82] *Id.*

[83] *See* State Department Rollout of Biometric Visas, *supra* note 11, at 5–6.

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

[85] *See* State Department Rollout of Biometric Visas, *supra* note 11, at 2. The GAO found that consular officers are unclear on how to use the program and the information available from IDENT on visa applicants. For example, officers are unclear about who should scan the fingerprints and whether fingerprints should be collected before or during or after the visa interview; whether information on visa applications from the DHS database should be considered by the visa-adjudicating officer during or after the interview; and who should have responsibility for reviewing the IDENT information before visa issuance—raising some concern that key information about an applicant could be overlooked if the interviewing officer is not the same officer reviewing the IDENT information. According to the GAO, consular officers need to know how the program's information about visa applicants is intended to be used in order to maximize program effectiveness and determine optimal workflow management and resource issues. *Id.*

tries.[86] 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. This will mean the end of same-day processing for most posts, except in limited emergency situations.[87]

US-VISIT

The Biometric Visa Program—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's automated entry/exit system, US-VISIT, which was launched on January 5, 2004.[88] US-VISIT is designed to collect and share information on foreign nationals traveling to the United States, providing the government with capability to record the entry and exit of non–U.S. citizens into and out of the United States. Although the idea of the entry-exit program was introduced in 1996, the 9/11 terrorist acts accelerated its implementation and also introduced the concept of biometrics as the technology standard that would be used in the US-VISIT system. The overall implementation of US-VISIT calls for the collection of personal data, photos, and fingerprints at consular posts abroad and at ports of entry, as well as extensive database and information sharing. It also provides officials with information about persons who are in the United States in violation of the terms of their admission to the United States.

Upon arrival in the United States, a foreign national who is subject to US-VISIT is inspected by CBP inspectors at a port of entry. The individual's travel documents are scanned, and a digital photograph and inkless fingerprints of both index fingers are taken. If a foreign national has received a nonimmigrant visa 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.[89] If the system shows a mismatch of fingerprints or a watchlist hit, the foreign national is held for further screening or processing.

The US-VISIT enrollment process takes approximately 10–15 seconds.[90] 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.[91] If CBP ran the IDENT checks during the admissions process, it would add approximately five minutes to every US-VISIT enrollment, wreaking havoc at any port of entry.[92]

[86] *See* "DOS Answers to AILA's Questions," (Mar. 17, 2005), *to be posted on* AILA InfoNet.

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

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

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

[90] *Id.*

[91] *Id.*

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

The individual's name is also checked against the IBIS database and the wants and warrants section of the NCIC database.[93] IBIS contains certain terrorist watchlist information from the TIPOFF system maintained by DOS. Both the IBIS and NCIC checks are text-based checks and not biometric checks.[94]

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.[95] 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 legacy INS 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.[96]

There are additional concerns about the interoperability of the database systems. The notion of a comprehensive watchlist database system is thoroughly dependent on the accuracy of the information in the database. Currently, the separate databases from the three immigration bureaus have not been fully integrated into US-VISIT.[97] Moreover, the system used by IDENT is based on a flat two-print. However, the lack of integration between IDENT and IAFIS, which is based on a rolled 10-print fingerprint has resulted in significant problems. Unfortunately, the two- versus 10-print baseline creates problems with false matches on print checks and also does not interface well when the two-print IDENT print is run against the 10-print rolled IAFIS system.[98] The database integration program to make the IAFIS/IDENT systems interoperable by FY2006–07 is already two years behind schedule.[99]

Visa Waiver Country Applicants

§303(c) of the Border Security Act also contained a separate provision requiring the use of biometric identifiers for passports of applicants from Visa Waiver Program (VWP) countries. This biometric identifier requirement coincided with a second requirement that requires VWP travelers to present a

[93] *See* Statement of Kathleen Campbell Walker on behalf of AILA 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, Jan. 28, 2004, *posted on* AILA InfoNet at Doc. No. 04012940 (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 nonimmigrant visa 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.*

[94] *See* Statement by Kathleen Campbell Walker, *supra* note 93.

[95] 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 6 or more months later the alien would be at the same location. Particularly, if an alien were intending to overstay, it is likely that the alien would have provided only a temporary or false location as to where the alien was intending to go.

See Statement by Kathleen Campbell Walker, *supra* note 93.

[96] *Id.*

[97] *Id.*

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

[99] *Id. See also* IDENT/IAFIS: The Batres Case, *supra* note 11, at 15. The integration of IDENT and IAFIS is based on a single 10-fingerprint workstation capable of querying IDENT using index fingerprints and IAFIS using 10 fingerprints. The electronic IAFIS response would indicate a match or not match. When there was a match, IAFIS would electronically transmit the criminal history Record of Arrest and Prosecutions (RAP) sheet to the workstation from which the query was made. *Id.* at 14.

machine-readable passport (MRP) when applying for visa-free entry into the United States after October 26, 2004.[100] It is important to note that the machine-readable passport requirement is a separate obligation to the biometric requirement.[101] Under the MRP requirement, a passport issued on or before October 25, 2004, will be valid for VWP entry to the United States after October 26, 2004, as long as it is machine-readable. If it is not machine-readable, the VWP traveler must obtain a nonimmigrant visa.[102] On October 22, 2004, CBP announced that it would, at its discretion, parole on a one-time basis, those applicants for admission under the VWP who do not possess machine-readable passports and who are not associated with terrorism or criminality, or who will not add to the illegal population in the United States. However, on May 12, 2005, DHS announced that this limited period and discretionary authority to issue a one-time parole would end on June 26, 2005.[103]

With respect to the biometric identifier requirement, the International Civil Aviation Organization (ICAO)[104] determined that facial recognition, in the form of a facial image stored in a contactless chip embedded in passports, as the preferred biometric identifier. The original deadline of October 26, 2004, mandated that VWP countries establish a program to issue ICAO-compliant passports by that date, such that travelers from VWP countries, whose passports are issued on or after October 26, 2004, must present a machine-readable passport with the appropriate biometric identifier or must otherwise apply for a nonimmigrant visa at a consular post in order to enter the United States after October 26, 2004. Although all VWP countries made varying degrees of progress toward compliance with the requirement to have a program in place to issue biometric passports, only one or two countries would have had production capability in place by October 26, 2004.[105] None of the larger countries (Japan, the United Kingdom, France, Germany, Ireland, Italy, or Spain) would have been able to issue passports with the ICAO biometric by October 26, 2004.[106] Japan and the United Kingdom anticipated that they could not begin until late 2005; others not until 2006.[107] Most of these countries simply could not overcome the hard-technology hurdles of designing, testing, and rolling out biometric passports on a large scale. On August 9, 2004, VWP countries were granted a one-year extension to October 26, 2005, to comply with the biometric identifier mandate. However, based on the continuing technical difficulties, DOS and DHS will likely have to request another extension after October 26, 2005.

SECURITY CHECKS PERFORMED BY DHS

Although beyond the scope of this article, DHS also performs standard security checks on all nonimmigrant and immigrant visa applications filed with USCIS service centers. Similar to many of the

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

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

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

[103] "CBP Guidance on Paroling VWP Applicants Without Machine-Readable Passports," *posted on* AILA InfoNet at Doc. No. 05033174 (Mar. 31, 2005). After June 26, 2005, transportation carriers will be fined $3,000 per violation, for transporting any VWP traveler to the United States without a MRP. *See* "DHS and DOS Advise that All VWP Travelers to the U.S. Must Possess Machine Readable Passports as of 6/26/05," *posted on* AILA InfoNet at Doc. No. *Posted on* AILA InfoNet at Doc. No. 05051269 (May 12, 2005).

[104] 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.

[105] *See* Testimony of Maura Harty (Jan. 28, 2004), *supra* note 77. Australia and New Zealand may make the October 26, 2004 deadline. Some countries have indicated that implementing a biometric program may have been possible by the deadline, but they are putting on the brakes because of questions of interoperability (can a U.S. POE scanner read a Danish biometric chip?) that remain unresolved. *See* "DOS Instructs on Machine-Readable and Biometric Requirements," *supra* note 101.

[106] Even the United States will not be able to comply with this deadline and will likely only introduce the new biometric U.S. passport by then end of 2005.*Id.*

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

other security checks that are initiated during consular processing, foreign nationals applying for immigration benefits in the United States have encountered significant delays.

IBIS checks are conducted by USCIS on all nonimmigrant, immigrant, and citizenship applications. IBIS provides USCIS with any information on prior visa history, wants and warrants, as well as information on known terrorists. Checks are performed on both beneficiaries and petitioners and take approximately four to five minutes per case. Approximately 95 percent of cases do not show any derogatory information. If there is a "hit," USCIS checks with the agency that input the original information before adjudicating the petition.

For permanent residence applications, fingerprint checks (IAFIS 10-print) are completed prior to adjudicating any I-485 applications, asylum applications, or any other applications for permanent residence. Fingerprint checks provide USCIS with criminal histories but not wants and warrants.

The third security check performed by USCIS is the "FBI name check," which provides information about whether a person is currently or has ever been investigated by a relevant government agency. If there is a hit, USCIS does not have any specific information about the hit as it is not a law enforcement agency, and it must wait for the FBI to resolve the hit. If the name check is returned with a "no information" response, USCIS periodically reruns the check on a set schedule. If the record is listed as pending, a list of records must be forwarded to USCIS headquarters, which then follows up with the FBI. The FBI does not retain data on any security check that it performs, so every time a name check is needed, the foreign national has to go through the same process again. There is no method of noting that a problem has come up previously and been resolved.[108]

CONCLUSION

As the various law enforcement, intelligence, and government agencies coordinate their efforts at data sharing and jointly perform security checks at the consular level, it has become increasingly important to understand how the consular framework operates. The complications and the delays that can occur can frustrate even the most patient of visa applicants. Therefore, complete familiarity with nonimmigrant consular processing procedures and an in-depth understanding of the maze of security measures and related issues are vital to assisting foreign nationals and their employers in navigating the complex consular process.

[108] USCIS is about to test a background check system called "BCS" that will track the status of checks and keep data. *See* "Minutes of 10/28/04 Liaison Meeting," *posted on* AILA InfoNet at Doc. No. 05012163 (Jan. 21, 2005).