

Slide 1

**Fundamentals of Consular Processing**  
(Presentation based on *THE CONSULAR POSTS BOOK*, ILW Publications (2009), Rami Fakhoury and Mark Levey, eds.)

**General Seminar Overview:**

1. Role of the State Dept in Visa Processing: Information Gathering – New Attorney Vulnerabilities in International Practice - April 29
2. Coordination between the State Dept., USCIS/ICE, and other Federal Agencies - May 27
3. Set Up of Consular Posts: Who's Who Behind the Glass Wall, and How to Get Them to Work With You - June 24

Slide 2

**Introduction:**

Practicing Immigration Law and representing clients before U.S. consulates today has changed greatly since 2000:

- It is no longer enough to simply know the law and accurately present the information a client has given to you.
- In an era of massive corporate and financial fraud, there are no "safe" clients. All applications now go through a partially-automated investigative process.
- There is no longer a 4<sup>th</sup> Amendment "wall" that separates the information gathered by domestic law enforcement and international intelligence investigations.
- Attorneys no longer have a reasonable expectation of confidentiality in international communications with their clients.
- In recent times, the Consul's mission has shifted from Business Service to Front-Line Investigator. DOS has an enhanced role in National Security, and now works in close cooperation and shared data with DHS. Fraud detection methods are now very sophisticated.
- Due diligence is essential to consular and immigration practice. Even small firms must put in place a systematic risk management program.

This is not entirely a bad thing. As you become familiar with the new rules, you can provide additional value-added compliance advice to clients.

Slide 3

**SESSION 1 - Information Gathering, Data Mining, and Distributed Data Sharing -**

Monitoring of Attorney-Client International Communications, Immigration and Visa Applications Now Treated As Routine Intelligence Gathering, Counter-intelligence and Counter-Terrorism Functions

**Background Checks of Non-Immigrants and Immigrant Visa Applicants -Who Gets Checked, How it Gets Checked, and What to Expect**

When an attorney or company compliance officer signs off on an immigration application filed at USCIS Service Center or US Consular post abroad, information about the signor becomes part of an interlinked network of databases that connect 16 domestic law enforcement agencies and, in some cases, foreign governments. The principal databases we will be concerned with here are:

- **CLAIMS 3** is the USCIS legacy case application tracking and processing system used for the adjudication of applications and petitions for immigration benefits and services except asylum and naturalization. **CLAIMS 3** is the primary source of applicant/petitioner information that is used by USCIS to perform background checks, conduct the examination (review of the information that is being provided by petitioners), and adjudication (decision process to grant or decline petitions and applications for benefits).

## Slide 4

### Primary State Department Information and Lookout System – CLASS (Consular Lookout Assistance and Support System)

- US State Dept. operates **CLASS** (Consular Lookout Assistance and Support System) contains the consular lookout book – information from past findings of visa ineligibility as well as information of individuals suspected of being connected to terrorism. It gives visa officers a detailed understanding of the results from the various lookout systems (including namechecks, biometrics, and facial recognition). Since 2002, it has been a two-way sharing of lookout names with the DHS Treasury Enforcement Communications System (TECS), as well as with foreign governments for the international sharing of terrorist lookout information. CLASS replicates in real time the DHS IBIS lookout system. The lookout is available to DHS inspectors at Ports of Entry.
- Information about that attorney or company compliance officer becomes part of a two-way flow of data. Information routinely collected by **USCIS CLAIMS** and the **State Department CLASS systems** is deposited in a central data base, the **Background Check Service (BCS)**, accessible by both agencies and more than two dozen other federal agencies and, in a more limited fashion, also by state and local law enforcement. In addition, foreign allies and intelligence and law enforcement are granted access to this data pursuant to cooperative agreements.
- 

## Slide 5

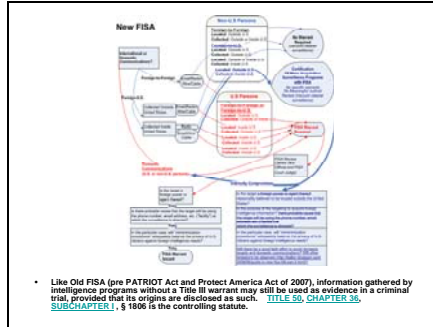
### New FISA

- **New FISA: Blanket Authorizations for Surveillance of International Communications** – “vacuum cleaner” collection means that your international communications are not secure or confidential.
- The next two panels illustrate how complex the FISA law is, but you should be aware of the basic fact that **information collected by intelligence agencies through warrantless electronic surveillance of international communications may be and is disclosed to law enforcement.**

## Slide 6

- **The present FISA rules that are most relevant to U.S. persons, such as attorneys who communicate internationally are as follows:**
- Surveillance targeted at communications between two U.S. persons inside the U.S. require Title III or FISA warrants, as under old FISA (pre-USA Patriot Act, pre-Protect America Act of 2007). One change in the new law is that targeted surveillance against a U.S. person abroad now also requires a FISA or Title III warrant, regardless of the target's location.
- **Electronic communications coming from abroad, or going abroad, are subject to “vacuum cleaner” collection under blanket authorizations.** The standard for issuance of such a program authorization is that the “primary purpose” of data collection is the acquisition of “foreign intelligence.” **No judicial probable cause finding is necessary for blanket programs. Collection sources may now be inside or outside the U.S. – the new FISA law removed that distinction.**
- No specific FISA warrant is required for blanket collection. Minimization procedures for US person data remain classified, set by US AG and DNI with FISC sign off. There is an exception to minimization of US person data collected under blanket programs when analysis reveals evidence of serious criminal activity or terrorism. See, Sec. 1505. **Data indicating serious illicit activities may be retained and shared by intelligence and law enforcement agencies with Memos of Understanding (MOUs) in place.**
- Foreign-to-foreign e-mail exchanged between foreigners will no longer require a FISA warrant, even if acquired from a storage facility, router, or switching node located in the United States. Your firm's computer files or records system containing information of this type – e.g., copies of communications between non-US persons abroad to which you may be a third part -- may be subject to warrantless remote search.

## Slide 7



## Slide 8

- Expanded roster of selected countries are eligible for The Visa Waiver Program (VWP).
- The new ESTA background check system, what gets checked.
  - As of January, 2009, entrants under the Visa Waiver Program (VWP) will be required to hold passports with "biometric indicators", and will be processed through a new registration system, ESTA.
- VWP and B-1/B-2 applications are now both subjected to background checks and reviewed for 9 FAM grounds of inadmissibility. VWP denial may be based on mere arrest or derogatory information – grounds for VWP denial are broader than visa denial.
- VWP clearances are made on-line and first-time applicants should be made several weeks in advance, if possible. In most cases, approvals are nearly instantaneous. Approvals generally good for multiple entries of 90 days each over a two-year period. Denied VWP applicants must apply for visa at consulate with jurisdiction.
- The new VWP background check system, Electronic System for Travel Authorization (ESTA), is operated by DHS – ESTA contains information gained from foreign governments, perhaps of dubious quality. No appeal of ESTA decision. No means to check or challenge basis of denial or records. Visa application is only recourse.
- Basis for denial of ESTA application – mere arrest or other police or security record – may differ from those that would preclude visa issuance.
- Foreign Affairs Manual (9 FAM) defines criminal and other grounds of inadmissibility that may arise in a CLASS or ESTA check, reviewed in Chap. 2.

## Slide 9

- ### Grounds of Inadmissibility
- Foreign Affairs Manual (9 FAM) defines criminal and other grounds of inadmissibility that may arise in a CLASS or ESTA check, reviewed in Chap. 2.
  - The vast majority of visa denials arise from the applicants' inability to overcome the presumption that they intend to immigrate to the United States (INA Sec. 214(b)). Most denials are B-1/B-2 visitors visas. If an applicant wants to overcome the presumption of being an intending immigrant, s/he normally shows that s/he has strong ties and economic, social, or other reasons to return at the end of their lawful nonimmigrant stay in the U.S. Denial rates vary widely depending upon the country of application from more than 20 percent for poorer African and Eastern European to less than three percent for wealthier Middle East/Gulf countries.
  - Exceptions to this include the business immigration categories H, L, O, where "dual-intent" is permitted, as well as various diplomatic categories.
  - Another common basis for NVV refusal is found in INA Section 221(g) - This ground for denial can apply to any visa application, non-immigrant as well as to beneficiaries seeking issuance of an immigrant visa. Applicants will receive one of several versions of a 221(g) response letter depending upon their circumstances.
  - 221(g) Temporary Refusal – failure to demonstrate eligibility
    - Rather than resulting in outright denial of a visa, in many instances receipt of a notice of Section 221(g) visa refusal requesting additional information. This ground may apply to all IV and NVV visa categories. In many cases, this might more accurately be termed a provisional denial or, "well, and we'll get back to you when your visa is ready" letter. Applicants from countries such as Russia, China, India, and Pakistan who have backgrounds in aerospace or defense engineering should expect that during the interview the consular officer will hand over two sets of papers. The first is a 222(g) notice and the other will be a check list of additional documents that must be provided, such as resumes, project descriptions, etc.
  - Applicants from certain countries with technology training or experience may require an additional background check, a Security Advisory Opinion (SAO), such as a Visa Mania check. Ninety percent of visa applicants delayed owing to a requirement for a Visa Mania check are Chinese and Russian nationals. Only 2.5 percent of all applicants require an SAO.

## Slide 10

### Security Advisory Opinions (SAO)

- If a legal opinion or security background check is required, a **Security Advisory Opinion (SAO)**, a "visa cable," is sought from State Department Visa Office at Foggy Bottom. **Chapter 3** describes the **factors that may trigger an SAO** – normally, potential national security threats, but may also be criminal grounds or even questions about technical eligibility for the immigration benefits sought.
- A domestic unit within the Visa Security Program issues Security Advisory Opinions (SAOs) for such visa applicants, who undergo an FBI name check and potential investigation through other law enforcement and national security agencies. SAOs would apply to any applicant deemed to pose some sort of threat, such as industrial espionage, illegal technology transfer or terrorism.
- **Chapter 7** provides the **inquiry procedures** lawyers can access if the SAO process is delayed or the attorney needs to communicate with the State Department about a case.

## Slide 11

### Two Categories of Visa Denials

- **221(g) Denial and Return of Petition for Revocation**
- A more worrisome situation for applicants is receipt of an unexpected Sec. 221(g) denial, particularly one in which the factual grounds are vaguely alluded to or not stated on the Form OF-160. That may occur in cases where USCIS has previously approved a petition, such as in H-1L, as well as in IV processing cases. Most denials in this situation happen after new, derogatory information is revealed during the interview. A consular officer may conclude that there was fraud involved, or a potential temporary worker doesn't qualify for the position described in the petition, or that a bona-fide fiancée or other family relationship does not exist.
- **May be difficult to correct** – Consuls will state that it no longer has jurisdiction after a petition is returned, and the USCIS is generally not receptive to inquiries about such cases. However, attorney intervention is essential to successfully resolve or mitigate issues. IVs should be made priority for the Consul, and if disavowed then addressed to the Service Center Director. In many cases, filing a new petition with filing fees may be required. Subsequent petition likely to be filed.
- Other complications, such as fraud investigation and unlawful presence may also be triggered.
- **Two categories of Visa Denials: Category 1 – permanently inadmissible** (e.g., fraud, aggravated felon, terrorist, engaged in genocide, totalitarian Party member, serious adverse foreign policy consequences); and **Category 2 – Temporarily inadmissible** (e.g., some criminal grounds, aliens previously removed/unlawful presence, communicable disease grounds, foreign medical graduate, public charge, intending immigrant, failure to demonstrate eligibility for visa, etc.). If visa is denied, consular is supposed to explain grounds and any available remedies or waiver, unless the grounds are related to national security.
- **Waivers of inadmissibility** are available for virtually all grounds of inadmissibility, and are frequently granted when vigorously pursued. Basis for waivers are humanitarian, family unity or national interest reasons. While some waivers are routinely granted, such as health, others involve showings of extraordinary equities or compelling national interest. Like relief in removal proceedings, waivers of criminal or national security grounds is an area of specialized practice that often requires extensive knowledge and experience.

## Slide 12

### 9 FAM – Guide to Criminal Grounds of Inadmissibility

- 9 FAM is considered a definitive authority for visa eligibility purposes. That volume reviews and interprets many specific issues related to criminal grounds of inadmissibility, including definitions and illustrations of:
  - Aggravated Felonies;
  - Crimes of Moral Turpitude (CMT);
  - Two or more non-CMT convictions;
  - Petty offense exception;
  - What constitutes a conviction for immigration purpose;
  - Legal issues and distinctions can be arcane and dependent upon foreign law and state law interpretations;
  - Definitions of crime change over time – laws applicable at time of conviction are usually controlling;
  - Thorough legal research, including close reading of 9 FAM, and briefing essential to overcoming a consular determination of inadmissibility based on alleged criminal history.

## Slide 13

### Session One Discussion

- Discussion of select consular posts
- Hot topics update

## Slide 14

### SESSION 2. Coordination between USCIS/ICE, CIA, FBI, the State Dept and other Federal Agencies.

- USCIS examiners and State Department employees now have easy access to a vast number of federal records, such as tax returns for previous years. They have automated systems to spot fraud.
- Investigations for the State Dept. are carried out by the **Bureau of Diplomatic Security Service (DS)**, along with FBI and CIA.
- **Chapter 4 - multiple-agency task forces** investigate **USCIS benefits and document frauds**. DSS is the agency charged with the enforcement of **passport fraud and visa fraud**, which includes **material misrepresentations** in the making of false applications, as well as the use of false documents in applications to the State Department. **DHS/ICE** has primary jurisdiction over similar crimes performed within the U.S. to facilitate **immigration fraud** against USCIS.

## Slide 15

### Targeted Surveillance, Federal Task Forces, Agency Audits, and Automated Fraud Detection of Visa and Immigration Applications.

- Court found in *Al-Haramain* case that US Gov't had illegally spied on int'l communications of U.S. attorneys representing clients in terrorism-related proceedings. (2008)
- *Kuene* money-laundering case points out problems of representing criminal clients and tainted fees. (2008)
- Immigration Attorneys targeted as accomplices by federal **Benefits and Documents Fraud Task Forces**, including DOS. (since 2006)
- **Agency Audits** - DOL Audited All Labor Certifications Submitted by major Immigration Law Firm under fraud-detection rubric. Major financial and reputational loss to law firm. (2008)
- DHS Federal Register announcement of **random H-1B and L-1 fraud audits**. (September 2008)
- USCIS report found what it determined to be a fraud rate of more than 20 percent among H-1B renewals selected for study. (September 2008)

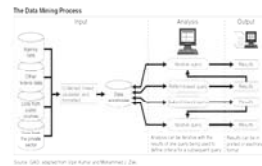
## Slide 16

### Automated Fraud Detection and Random Benefit Fraud Assessments

- **Fraud Detection and National Security Data System (FDNS-DS)**
  - On August 18, 2008, DHS published regs – announced new data-mining system designed to be “a central repository . . . to record, track, and manage the background check and adjudicative processes related to immigration applications and petitions with suspected or confirmed fraud, criminal activity, egregious public safety, and/or national security concerns, and cases randomly selected for benefit fraud assessments (BFAs)”
- **USCIS/DOS Data Collection, Analysis and Dissemination Systems perform random Benefits Frauds Audits** - USCIS has entered into a Memorandum of Understanding with the Department of State providing them with access to the FDNS-DS. That system “will store information concerning cases randomly selected for BFAs and will track interactions with Immigration and Citizenship Enforcement (ICE) and other LEAs (e.g., the Federal Bureau of Investigation [FBI], the Drug Enforcement Administration [DEA], and U.S. Customs and Border Protection [CBP]) in cases involving fraud or other criminal activity, and the Department of State in cases involving fraud related to selected types of visas for entry into the United States.”

## Slide 17

- **DS also investigates terrorism, espionage and illegal technology transfer, narcotics, and large-scale trafficking.** DS has for more than a decade worked in joint task forces with multiple intelligence and law enforcement agencies.
- **Chapter 7** describes the panoply of **data-mining and profiling programs** that are now applied to millions of visa and immigration applications received each year.



## Slide 18

- **DS** has contracted to build an integrated database as part of an expanding effort to **target non-immigrant visa fraud, particularly H and L cases**, at US Consular posts abroad.
- The Visa Security Program issues Security Advisory Opinions (SAOs) for visa applicants who are red-flagged. These subjects undergo an **FBI name check** – an intensive background check – and potential further investigation through other national security agencies, including analysis of communications intercepts. SAOs would apply to any applicant deemed to pose some sort of threat, such as industrial espionage, illegal technology transfer or terrorism.
- The threats of terrorism, nuclear proliferation and serious transnational crime have driven massive investments in the data processing and analysis capabilities.

## Slide 19

### Session 2 Discussion

- Discussion of select consular posts
- Hot topics update

## Slide 20

### Session 3. Set Up of Consular Posts: Who's Who Behind the Glass Wall, and How to Get Them to Work With You

- **Chapter 8** provides a practical guide to risk factors and self-audits. This section will help you approach cases like a consular examiner or USCIS examiner. This will make it easy for them to approve your client's application.
- Consular officers are looking for red-flags that identify risky applicants. You should be aware of what these are, minimize, and address them pro-actively.
- Even beginning attorneys, solo practitioners and small companies can use these guidelines to develop in-house systems to manage risks.
- **Develop a Risk Management Profile to identify risks.** Identify high-risks: (1) risk profile each new client; (2) do a risk profile for your own firm (or company); and (3) identify additional risks for client counter-parties (the client's banks and other law firms).

## Slide 21

- **Chapter 8** provides a pro-active guide to identifying and addressing the concerns of consular officials and adjudicators.
- Perform due diligence by carrying out an appropriate level of background checking and document authentication.
- **To fail to carry out due diligence is negligent, but to act with knowledge of fraud or misrepresentation is criminal.**
- Finally, **Chapter 9** provides a report on the issues that attorneys can expect to encounter at two dozen foreign consulates, and details the local problems that can lead to consular delays, refusals, or more serious enforcement actions.

Slide 22

Session 3 Discussion

- Discussion of select consular posts
- Hot topics update