

Testimony of

MICHAEL J. MAXWELL

on

Checking Terrorism at the Border

before

**The Subcommittee on International Terrorism
and Nonproliferation**

Committee on International Relations

U.S. HOUSE OF REPRESENTATIVES

Thursday, April 6, 2006

Good morning Chairman Royce, Ranking Member Sherman, and distinguished Members of the Subcommittee. Thank you for the opportunity to appear before you today to discuss immigration-related national security vulnerabilities facing the United States.

My name is Michael Maxwell and, until February 17 of this year, I was Director of the Office of Security and Investigations (OSI) at US Citizenship and Immigration Services (USCIS). I would like to begin by expressing my thanks to the men and women of OSI who stayed the course from day one, despite extraordinary pressure to take the easier path, and who remained loyal to the ideals of national security, integrity, and sacrifice. You would be hard-pressed to find a more dedicated group of professionals in either the public or the private sector, and I am proud to have served with them.

The USCIS Office of Security and Investigations

U.S. Citizenship and Immigration Services (USCIS) is the component of the Department of Homeland Security (DHS) that processes all applications for immigration status and documents—known as “immigration benefits”—including lawful permanent residence (the beneficiaries of which are issued “green cards”), U.S. citizenship, employment authorization, extensions of temporary permission to be in the United States, and asylum, that are filed by aliens who are already present in the United States. USCIS also processes the petitions filed by U.S. citizens, lawful permanent residents, and employers who seek to bring an alien to the United States, either permanently or on a temporary basis.

The Office of Security and Investigations was created by former USCIS Director Eduardo Aguirre to handle all the security needs of the agency, including:

- The physical security of the more than 200 USCIS facilities worldwide;
- Information security and the handling and designation of sensitive and classified documents;
- Operations security, for both domestic and international operations;
- Resolution of all USCIS employee background investigations;
- Protective services for the Director of USCIS and visiting dignitaries; and
- Internal affairs, among other duties.¹

OSI’s mandate from Director Aguirre was to “regain the public trust in the immigration service” by identifying, reporting, and resolving any security vulnerabilities that would permit the successful manipulation of the immigration system by either external or internal agents.

¹ See Attachment 1: Statement of Mission and Jurisdiction of OSI.

Checking Terrorism at the Border

Between May and December of 2004, with the support of Director Aguirre, I began to recruit top-notch security experts, mostly from other Federal agencies. By September of 2004, OSI had in place a small team of professionals who would plan and successfully execute the first ever naturalization ceremonies to be conducted in a war zone overseas for members of the United States Armed Forces.² Following an agency-wide initiative I led in early 2005 to evaluate the few existing USCIS security systems and resources, Director Aguirre authorized, in writing, the immediate hiring of 45 new personnel for OSI, including 23 criminal investigators to investigate allegations of employee corruption and wrongdoing.³ By May of 2005, I had been authorized a staffing level of 130 full-time employees and contract workers.⁴ My only option for bringing staff on board, however, was to transfer them laterally from other DHS components, because the Human Capital Office of Administration refused to post any new vacancy announcements, apparently because they did not approve of a law enforcement component within USCIS.

In August of 2005, not long after the departure of Director Aguirre, my staffing matrix was effectively cut from 130 to fewer than 50 personnel worldwide. USCIS Senior Leadership, as represented on the Senior Review Board (SRB),⁵ which must approve all significant expenditures, as well as the Human Capital Office of Administration, blatantly disregarded the written orders of former Director Aguirre and unilaterally decided that OSI should not be adequately staffed.⁶

In fact, with the approval of Acting Deputy Director Robert Divine, originally appointed by President Bush as Chief Counsel and the highest-ranking political appointee at USCIS following the departure of Aguirre's Deputy Director, Michael Petrucelli, OSI's authorized staffing level was set so low that, not only were we unable to open investigations into new allegations of employee corruption with clear national security implications, our ongoing national security investigations involving allegations of espionage and links to terrorism were jeopardized. OSI staff consisted primarily of:

- Six criminal investigators—one or two of whom were detailed to the DHS Office of Internal Security at any given time because of their expertise in national security investigations—to handle a backlog of 2,771 internal affairs complaints, including 528 that were criminal on their face and ranged from bribery and extortion to espionage and undue foreign influence;
- Six personnel security specialists to handle a backlog of 11,000 employee background investigations that had developed before OSI was created, plus the background

² See Attachment 2: Meritorious Civilian Service Award.

³ See Attachment 3: Memorandum from Maxwell to Aguirre, 03/09/05.

⁴ See Attachment 4: OSI Staffing Matrix as of 08/05.

⁵ See Attachment 5: Members of the SRB as of 01/19/06.

⁶ See Attachment 6: SRB overrules Director's orders.

Checking Terrorism at the Border

investigations of all the new employees being hired to help eliminate the application backlog;

- Nine physical security specialists to secure over 200 USCIS facilities worldwide; and
- One supervisory security specialist to ensure the continuity of operations (COOP) in the event of an attack or other crisis that impacts USCIS personnel or processes.

The same senior leaders who absolutely refused to allow OSI to obtain the necessary resources to fulfill its mission also refused, time and time again, to act when confronted with major national security vulnerabilities my team and I identified in the immigration process. Each of the security breaches described below was brought immediately to the attention of top-level officials at USCIS. These breaches compromise virtually every part of the immigration system, leaving vulnerabilities that have been and likely *are being* exploited by enemies of the United States. Despite the fact that each identified threat has significant national security implications, USCIS leadership consistently failed—or refused—to correct them. Instead, top officials chose to cover them up, to dismiss them, and/or to target the employees who identified them, even when the solution was both obvious and feasible.

As a former police chief and national security specialist, I do not make these charges lightly. Over the past eight months, I have provided, through my attorney, thousands of pages of unclassified documents, including most of those attached to this statement, to Members of this Subcommittee and other Members of Congress. More recently, I have provided the same documents to the FBI, the GAO, and the DHS Office of Inspector General. On three separate occasions, I offered to provide Director Gonzalez a full set of these documents, but on each occasion, he declined my offer.

These documents, and others of which I have personal knowledge but am not at liberty to release or to discuss in an open forum, prove not only the existence of the national security vulnerabilities I will discuss today, but also the fact that senior government officials are aware of the vulnerabilities and have chosen to ignore them. More troubling is the fact that these same officials actually ordered me to ignore national security vulnerabilities I identified, even though my job was to address them. When I refused these orders, I was subjected to retaliation—some of which was as blatant as revoking my eligibility for Administratively Uncontrollable Overtime (AUO), which totaled 25 percent of my salary, on the very day that I was scheduled to brief the Immigration Reform Caucus;⁷ and some of which was more nefarious, like the challenge to my authority to authorize access to Sensitive Compartmented Information (SCI), in a move that I have no doubt would have led to the revocation of my own Top Secret/SCI clearance, had I not resigned when I did.

⁷ See Attachment 7: Eligibility for AUO revoked.

Internal Affairs

Mr. Chairman, written allegations set forth by USCIS employees, interviews conducted as recently as yesterday with USCIS line employees and high level managers, internal USCIS communications, and external investigative documents prepared by independent third agencies, compiled and delivered to this Congress over the last eight months, make clear that the integrity of the United States immigration system has been corrupted and the system is incapable of ensuring the security of our Homeland.

As the office responsible for internal affairs, OSI received 2,771 complaints about employees between August 2004 and October 2005. Over 1800 of these were originally declined for investigation by the DHS Office of the Inspector General and referred to OSI. Most of the remaining complaints were delivered to OSI by the ICE Office of Professional Responsibility once they gave up jurisdiction over USCIS complaints. The majority of all complaints received by OSI are service complaints (e.g., an alien complaining that he did not receive his immigration status in a timely way) or administrative issues (e.g., allegations of nepotism).

However, almost 20 percent of them—528 of the 2,771—allege criminal activities. Alleged crimes include bribery, harboring illegal aliens, money laundering, structuring, sale of documents, marriage fraud, extortion, undue foreign influence, and making false statements, among other things. Also included among these complaints are national security cases; for example, allegations of USCIS employees providing material support to known terrorists or being influenced by foreign intelligence services.⁸ Complaints with clear national security implications represent a small share of the total, but in cases such as these, even one is too many.

OSI is required to refer such cases to the FBI when they reach a certain threshold, since the Bureau has primary jurisdiction over all terrorism and counterintelligence investigations. In virtually all the cases we refer to the FBI, though, OSI is an active investigative partner. In fact, OSI agents have led or facilitated remote and sometimes classified national security operations; we have led national security interviews; we have participated in national security polygraph interviews; and we have developed behavioral analyses as investigative tools.

OSI also details its agents to the DHS-Headquarters Office of Security when the latter lacks sufficient resources to investigate these types of national security allegations, as we have criminal investigators with training and experience in both counterterrorism and counterintelligence operations. In fact, one of our investigators is currently detailed to the DHS Office of Security.⁹ For operational security reasons, these investigations had to be compartmentalized from all USCIS management except the Director, Deputy Director, or Chief

⁸ See Attachment 8: Weekly Internal Affairs Report, 02/17/06.

⁹ See Attachment 9: Email regarding detail to Office of Security.

Checking Terrorism at the Border

of Staff. At times, we reported directly to Admiral Loy, when he was Deputy Secretary, and later to Deputy Secretary Jackson.

As you would expect, we always prioritize complaints that appear to implicate national security. One of the most frustrating parts of my job, though, was the fact that we simply did not have the resources to open investigations into even the relatively small number of national security cases. While I cannot discuss on-going investigations in this open forum, I can tell you about some of the allegations OSI did not have the resources to investigate.

As you know, the USCIS employees who process applications for immigration status and documents are supposed to ensure that the applicant is not a terrorist or criminal. The database they use to do this is the The Enforcement Communications System, or TECS. TECS is essentially a gateway into the criminal and terrorist databases of some two dozen law enforcement and intelligence agencies, including the FBI, the Drug Enforcement Administration, Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP), which controls access to TECS, the intelligence community, and others. USCIS employees are granted different levels of access to TECS depending on how in-depth of a background investigation they have undergone. Those who have undergone a full background investigation are likely to be granted access to Level 3 TECS records, which include terrorist watch-lists, information about on-going national security and criminal investigations, and full criminal histories. Due to the sensitivity of the data, USCIS employees are required to log in and out of the system so their access can be tracked.

OSI has seen far too many allegations recently where it appears that an employee or a contract worker may have entered TECS—or permitted someone else to enter TECS—in order to provide information to someone else. In fact, OSI recently got its first criminal conviction in a case involving a USCIS employee who accessed TECS in order to warn the target of a DEA investigation about the investigation.

More alarming, however, is an allegation that has not yet been investigated in which a Chinese-born U.S. citizen who works for USCIS permitted a family member to access TECS, print records from it, and then leave the building with those records. We do not know what records this person accessed or why, and yet this allegation is not being investigated because OSI's criminal investigators are already stretched to their limits.

Consider for a moment the potential repercussions of these types of investigations. One USCIS employee, co-opted by a foreign intelligence entity, with the ability to grant the immigration status of their choosing, to the person or persons of their choosing, at the time and location of their choosing. This threat represents a clear and ongoing danger to national security. The possibilities are even worse when you consider the nexus that this subcommittee knows to exist between countries with highly capable intelligence services and state sponsors of terrorism.

It may seem farfetched to think that a USCIS employee would be co-opted by a foreign intelligence agency. The fact is, however, that the new Director of USCIS, Dr. Emilio Gonzalez, in early 2006 at an open and unclassified session of a senior leadership meeting of almost two dozen senior managers mentioned two foreign intelligence operatives who work on behalf of USCIS at an interest section abroad and who are assisting aliens into the United States as we speak.

Restricted TECS Access

While there obviously is a problem at USCIS with unauthorized access to the TECS database, ironically, there also is a problem with insufficient access for USCIS employees who are deciding applications. The records accessible through TECS are grouped into four categories:

- Level 1 records are those from the user's own agency (i.e., Level 1 USCIS users would have access only to USCIS records);
- Level 2 records include all Level 1 records plus a sizeable share of the criminal records from the other law enforcement agencies (i.e., Level 2 USCIS users would have access to USCIS records, plus certain records from CBP, the FBI, the DEA, and so on);
- Level 3 records include Level 1 and 2 records, plus national security records, terrorist watch-lists, threats to public safety, and information about on-going investigations;
- Level 4 records include records from the three other levels, plus case notes, grand jury testimony, and other highly sensitive data that are provided only on a need-to-know basis.

Clearly, USCIS employees need access to the Level 3 records in order to properly vet applicants for immigration status and/or documents and ensure that known terrorists and others who present a threat to national security or public safety are not able to game the immigration system. On the other hand, because of the sensitive nature of some of these records, including on-going national security cases, it is important that access to Level 3 records be restricted to employees who themselves have been thoroughly vetted.

Thus, when DHS was created in January 2003, CBP, as the manager of TECS, entered into an agreement with USCIS that requires employees to undergo full background investigations before they may be granted Level 3 TECS access. The agreement included a two-year grandfather period during which legacy Immigration and Naturalization Service (INS) personnel who had had access to Level 3 TECS records at the INS would continue to have access so that USCIS would have time to complete background investigations on new employees and upgrade those on legacy employees when necessary.

Checking Terrorism at the Border

USCIS leadership, however, decided not to spend the money to require full background investigations on new personnel or to upgrade the background investigations on legacy personnel. Thus, when the grandfather period ended in January 2005, CBP began restricting access by USCIS employees with only limited background investigations, so that these employees can access only Level 1 (USCIS) records or, in some cases, Level 2 (USCIS plus limited criminal histories) records through TECS. They cannot access the national security, public safety, or terrorist records they need to process applications.

Other than a few sporadic meetings among USCIS senior staff and, once in a while, with some CBP officials, to talk about how many employees might have restricted access, USCIS leadership largely ignored the problem during the first nine months of 2005, despite complaints from the field and warnings from within Headquarters. Backlog elimination was the top priority of the agency, so employees were pressured to keep pumping out the applications, regardless of whether they had the ability to determine if an applicant was a known terrorist or presented some other threat to national security or public safety.

In early October 2005, the problem drew congressional and media attention. The Public Affairs office assured reporters that employees have access to all the records they need, while Acting Deputy Director (ADD) Robert Divine, Chief of Staff (CoS) Tom Paar, and Don Crocetti, the director of the Fraud Detection and National Security (FDNS) office, were frantically trying to figure out the difference between Level 2 and Level 3 TECS records in order to determine what critical information employees were missing.

During a late-night meeting in the second week of October, Crocetti acknowledged that Level 2 access leaves employees completely blind to sensitive national security, public safety, and terrorist records, along with information about on-going investigations. Deputy Director of Domestic Operations Janis Sposato told the group that 80 percent of all applications are processed through TECS at Level 3 as part of an automated background check system. She noted that some unknown portion of the remaining 20 percent are processed by the more than 1,700 employees with only Level 2 or below access, so critical national security indicators may have been missed. ADD Robert Divine's response to this information was, "I guess we've finally reached that point: Is immigration a right or a privilege?" In the ensuing debate, Divine and Acting General Counsel Dea Carpenter insisted that immigration to the United States is a right, not a privilege.

USCIS employees processed 7.5 million applications in FY 2005, so 1.5 million applications (20 percent) did not go through the automated background check system. If 1,700 out of 4,000 employees (43 percent) do not have Level 3 TECS access, then, not taking into account that those without Level 3 access may be able to process cases faster because they have to resolve fewer "hits" from TECS searches, those 1,700 employees processed some 645,000 applications. Furthermore, each application generally involves more than one individual and so requires more than one TECS search.

Checking Terrorism at the Border

At the conclusion of that late-night meeting, ADD Divine ordered Crocetti to lead the negotiations with CBP to resolve the TECS issue. Since then, Crocetti, sometimes accompanied by Divine and CoS Paar, has been meeting with CBP officials to convince them to extend the grandfather period and restore access to those employees who have been cut off and to waive in (without full background investigations) contract workers hired to eliminate the immigration application backlog. Granting contract workers who have not been vetted access to national security records would itself result in a significant security breach, since it could put sensitive national security information in the wrong hands and has already been shown to be a criminally negligent policy on the part of USCIS.

An increasing number of USCIS employees have had their access to TECS restricted since the grandfather period expired over one year ago, in January 2005. To date, not one employee with a deficient background investigation has been scheduled for an upgrade and no agreement to restore access has been reached with CBP.

To make matters worse, the ADD and the CoS have actively ensured that USCIS does not have the personnel it will need to upgrade employees' background investigations. OSI is responsible for processing background investigations on employees (the Office of Personnel Management (OPM) does the actual investigation and then sends it to OSI to resolve any inconsistencies and make a final determination on granting clearance).

Shortly after OSI was created, in the fall of 2004, we inherited a backlog of 11,000 pending background investigations on USCIS employees that INS and then ICE had failed to finalize. In light of the fact that we have had a total of six personnel security specialists to process background investigations over the past year, it is astonishing that we have managed to reduce the backlog to about 7,000. Because of the hiring frenzy driven by backlog elimination, however, OPM currently is sending OSI new background investigations at a rate of 3.5 for every one that OSI clears.

I presented at least eight proposals over the last year to increase the number of personnel security specialists to address this backlog, but all were denied by the Senior Review Board. CoS Paar approved 15 additional positions for OSI in mid-November 2005, but Human Capital refused to post the vacancies until after I resigned, and they have continued to delay the process so that none of the positions has yet been filled. Even if those five positions eventually are filled, that will be a total of 11 people to handle the 7,000 backlogged background investigations, plus the background investigations for new employees hired to eliminate the backlog, plus up to 5,000 upgraded background investigations on current employees whose access to TECS has been or could soon be restricted. The Chief of Staff and Deputy Director have been warned in writing on numerous occasions of this point of failure and both ignored the warnings. When the new Director of USCIS, Emilio Gonzalez, became aware of this situation, his immediate response was to order me to hire 17 personnel security specialists—above my authorized staff level—just to address the TECS access issue. *The very*

next day, however, CoS Paar overturned the Director's order and prohibited me from hiring any additional staff.

Irresponsible Policies

Information from various sources indicates that criminals and, potentially, terrorists are being granted immigration status and/or documents or being permitted to remain in the United States illegally through a variety of irresponsible policy decisions by USCIS leadership, the consequences of which they are well aware:

- 1) **Background Checks on Aliens**—USCIS Operation Instruction 105.10 instructs employees that “if no response is received to an FBI or CIA G-325 [name check] request within 40 days of the date of mailing [the request card] the application or petition shall be processed on the assumption that the results of the request are negative.”¹⁰ This policy flies in the face of the legal eligibility requirements for immigration status and of repeated public assurances by USCIS leadership that employees always wait for background check results before deciding any application for immigration status and/or documents. This Operation Instruction is listed on the USCIS website as current policy.

Since resigning from the agency, I have been told by USCIS employees, and had it confirmed by managers, that, not only are they instructed to move forward in processing applications before they receive background check results, but also that some have been instructed by supervisors, including legal counsel, to ignore “wants and warrants” on applicants because addressing them properly—i.e., looking into the reason for the arrest warrant to determine if a conviction may statutorily bar the applicant from the status or document for which he has applied—slows down processing times.

Moreover, I was told as recently as three weeks ago that USCIS District Offices and Service Centers are holding competitions and offering a variety of rewards, including cash bonuses, time off, movie tickets, and gift certificates, to employees and/or teams of employees with the fastest processing times. The quality of processing is not a factor; only the quantity of closed applications matters, and it is important to note that it takes a lot less time to approve an application than to deny one, since denials require written justifications and, often, appeals.

- 2) **Fingerprint Checks on Applicants for U.S. Citizenship**—OSI was notified that employees were not following DHS regulations that prohibit a naturalization exam from being scheduled before the fingerprint check results are returned by the FBI. This

¹⁰ See Attachment 10: Operation Instruction 105.10.

is a critical problem because there is a statutory 120-day window after the naturalization exam during which a final decision on the application for citizenship must be made. If a decision is not made during that window, for whatever reason, the alien may petition a court for a Writ of Mandamus, which orders USCIS to decide the application immediately. When I approached ADD Divine about this issue, he indicated that he was aware of the problem. He said that, as Chief Counsel, he had discussed this issue numerous times with USCIS senior staff, including then-Director of Domestic Operations Bill Yates. *Divine said he had concluded that since the fingerprint results come back before the 120-day window closes in 80 percent of cases, the other 20 percent represent an “acceptable risk.”*

Senior USCIS leadership at Headquarters meets every week for what are called “WIC” meetings. A detailed memo prepared for each of these meetings and distributed widely throughout the Federal government lists the activities that each unit within USCIS is involved in for the coming weeks and summarizes past activities. The WIC memo for the week of March 13, 2006 includes an item regarding “American-Arab Anti-Discrimination Committee (ACD) ‘120 Day Cases’ in District Court,” which says that the Department of Justice (DOJ) sees the current USCIS practice of scheduling the naturalization interview before receiving fingerprint results as a violation of regulations. It concludes that, while DOJ “understands the Congressional and Presidential mandates on processing times and backlog reduction that [US]CIS labors with,” DOJ fervently wishes that USCIS would stop violating its own rules, since the practice is tough to defend in court.¹¹

- 3) **Employment Authorization Documents**—A USCIS regulation (8 C.F.R. 274a.13) states that, if an application for adjustment to lawful permanent resident (LPR) status is not decided within 90 days, the applicant is entitled to file an I-765 application for an employment authorization document (EAD). This policy has led to large-scale fraud. The current processing times for an application for LPR status range from just under 6 months (the Nebraska and the Texas Service Centers each have one form of application for LPR status that is currently being processed within 6 months) to 60 months at the four service centers and from six months to 33 months at the larger district offices, so virtually all applicants—whether they are eligible or not and whether they are lawfully present in the United States or not—are able to obtain a legitimate EAD (applications for which both the service centers and district offices have only short processing times).

Under this policy, illegal aliens can simply file a fraudulent application, wait 90 days, and then ask for an EAD. Once they have the EAD, they can apply for a legitimate social security number and, even under the REAL ID Act, they can legally

¹¹ See Attachment 11: Memorandum for WIC Members, March 13, 2006, p. 4.

obtain a driver's license because they have an application for LPR status pending. With a social security number and a driver's license, they can get a job. According to the Government Accountability Office (GAO), an estimated 23,000 aliens were granted EADs on the basis of fraudulent applications for LPR status between 2000 and 2004. *When asked by the GAO to comment on the fraud resulting from this policy, USCIS leadership indicated that fairness to legitimate applicants outweighs the need to close security loopholes.*¹²

To make this situation worse, information I have just received in the past few days suggests two additional problems with the processing of I-765s, the application form for an EAD. First, it appears that the Texas Service Center has developed an "auto-adjudication" system that can process I-765s from start to finish without any human involvement at all. In other words, there is no point in the process when a USCIS employee actually examines the supporting documentation to look for signs of fraud. Instead, the I-765 application is processed automatically when the underlying application for LPR status has been sitting on the shelf for 90 days.¹³

The second issue, identified during the same review that uncovered the "auto-adjudication" system, is just as troubling. Staff at the National Benefits Center in Lee's Summit, Missouri, acknowledged that there is a way to bypass the normal application process and manually insert any number of applications into the computer system (CLAIMS3) so that the standard application screening process is circumvented. Independent investigators are currently attempting to determine how many applications have been improperly processed in this way and by whom.¹⁴

- 4) **Fingerprint Check Waivers**—A memo to Regional Directors from Michael Pearson, then head of Field Operations, sets out USCIS policy on the granting of waivers of the FBI fingerprint check requirement for aliens who "are unable to provide fingerprints," because of, among other things, "psychiatric conditions." The policy states:

The determination regarding the fingerprinting of applicants or petitioners who have accessible fingers but on whose behalf a claim is made that they cannot be fingerprinted for physiological reasons can be far less certain. Unless the ASC manager is certain of the bona fides of the inability of the person to be fingerprinted, the ASC manager should

¹² "Additional Controls and a Sanctions Strategy Could Enhance DHS's Ability to Control Benefit Fraud," Government Accountability Office, GAO-06-259, March 2006, pp. 22, 27.

¹³ Attachment 12: National Benefits Center documents (sensitive; for Members only).

¹⁴ Ibid.

Checking Terrorism at the Border

request that reasonable documentation be submitted by a Psychiatrist, a licensed Clinical Psychologist or a medical practitioner who has had long-term responsibility for the care of the applicant/petitioner [emphasis added].

In my 16 years in law enforcement, I have never heard of someone being exempt from fingerprinting due to a psychiatric condition. Moreover, I cannot fathom circumstances under which an ASC manager would be sufficiently qualified to determine the bona fides of the request for a waiver. At the very least, this policy should affirmatively require proof from a licensed professional, rather than just suggesting it if the manager cannot decide for himself.

- 5) **Refugee/Asylee Travel Documents**—As of late September 2005, USCIS employees handling applications for refugee/asylee travel documents were not comparing the photograph of the applicant for the travel documents with the original photograph submitted by the refugee or asylee and stored in the Image Storage and Retrieval System (ISRS). Thus, an illegal alien who can obtain biographical information about a legitimate refugee or asylee (from a corrupt immigration attorney, for example) can submit an application for travel documents using the real refugee/asylee's name and other biographical information, provide his own photograph, and be issued travel documents with his picture, but the name of an alien with legitimate USCIS records. The illegal alien can then obtain other documents based on the stolen identity established by the travel documents.

When USCIS leadership was made aware of this fraud scheme, a Domestic Operations representative responded by acknowledging that this "is a known vulnerability" they have been looking at "for the past year or so."¹⁵ This same individual clarified for ADD Divine that recent assurances Divine gave to Secretary Chertoff concerned verifying the identity of applicants related to I-90 adjudications, not refugee/asylee travel documents. Ironically in light of the issue in the paragraph below, ADD Divine noted that this issue "has particular poignancy as [USCIS] face[s] a flood of filings by Katrina victims seeking to replace documents." All parties acknowledged implicitly that requiring employees to compare the applicant's photo with the photo of the refugee/asylee that is stored in the Image Storage and Retrieval System (ISRS) would end fraud of this type.

USCIS Director Gonzalez contends that the *Standard Operating Procedures (SOP)* do, in fact, require such a comparison, so the problem is solved. Interestingly, the

¹⁵ See Attachment 13: Email exchange regarding Cameroon national.

Adjudicator's Handbook does not have such a requirement, but the bottom line is that the comparisons are not being done, regardless of what the *SOP* says. Employees have told me recently that, rather than actually changing the *SOP*, supervisors simply send out emails ordering employees to change the way they perform certain tasks, so as to speed up the work.

- 6) **Green Card Replacement**—In mid-December 2005, the ICE Office of Intelligence sent a memo to the USCIS Fraud Detection and National Security unit about a fraud scheme that ICE had uncovered that is similar to the one above.¹⁶ This scheme involved the I-90 application for a replacement/renewal green card (for lawful permanent residents)—the same application about which ADD Divine had reassured Sec. Chertoff. In this scheme, illegal aliens steal the identity of a lawful permanent resident. Each illegal alien then uses the LPR's name and Alien Registration Number to file an I-90 application for a replacement Permanent Resident Card ("green card") with the illegal alien's photo, fingerprints, and signature. Incredibly, USCIS actually captures the illegal aliens' photos, fingerprints, and signatures in the Image Storage and Retrieval System (ISRS), but employees fail to compare any of them with the photo, fingerprints or signature of the original applicant. ICE identified this as a vulnerability with "severe national security implications."
- 7) **Mandatory-Detention Aliens**—A policy memo sent to Regional and Service Center Directors by the now-retired head of Domestic Operations, *Bill Yates*, instructs *Service Centers NOT to serve a Notice to Appear (NTA), which initiates removal proceedings, on aliens who appear to be subject to mandatory detention under section 236(c) of the Immigration and Nationality Act (INA).*¹⁷ Instead, employees are instructed to decide the application, prepare and sign an NTA (unless they exercise prosecutorial discretion and decide to allow the convicted criminal to continue living in the United States illegally), and place a memorandum in the file explaining that they are handing the case over to ICE. Section 236(c) of the Immigration and Nationality Act requires that removable aliens who have been convicted of certain serious crimes be detained pending their removal (i.e., "mandatory-detention aliens"). Service Center employees and senior leadership at Headquarters confirm that this memo represents current USCIS policy.

The memo presents two separate issues: (a) whether this policy results in aliens who are subject to mandatory detention based on criminal convictions being allowed to remain free in American communities; and (b) the applicability and scope of prosecutorial discretion.

¹⁶ See Attachment 14: ICE memo and report (the latter is LES for Members only).

¹⁷ See Attachment 15: Yates memo on NTAs.

(a) *There is evidence that criminal aliens are being allowed to remain at large in U.S. communities as a result of this policy.* Part of the problem is that ICE officials (at least in some parts of the country) apparently have decided that ICE should be paid by USCIS each time it does its job and serves an NTA. A search for a missing alien file (A-file) that was being sought by an agent on the Joint Terrorism Task Force (JTTF) in the USCIS Philadelphia District Office recently resulted in the discovery of a stash of some 2,500 A-files of aliens whose applications for status and/or documents had been denied, but whose cases had not been turned over to ICE to issue NTAs because USCIS personnel at that office decided to hide the files rather than pay ICE to serve all those NTAs. According to the agent who found them, a majority of the files were for aliens from countries of interest.¹⁸ That means that aliens from special interest countries who do not qualify for legal status for whatever reason are still in the United States illegally, and there has been no effort to remove them from the country.

(b) The memo on prosecutorial discretion to which the Yates memo refers was issued by then-INS Commissioner Doris Meissner in response, according to the memo, to the Illegal Immigration Reform and Immigrant Responsibility Act of 1996. That law included several provisions aimed at getting criminal aliens off the streets and out of the country, including section 236(c) of the INA. Meissner asserts that immigration officers may appropriately exercise prosecutorial discretion “even when an alien is removable based on his or her criminal history and when the alien—if served with an NTA—would be subject to mandatory detention.” However, she reserves prosecutorial discretion to law enforcement entities, which USCIS absolutely refuses to be. As a self-avowed non-law enforcement agency, perhaps USCIS would be better off simply obeying the law.

National Security Indicators

As of August 2005, some 1,400 immigration applications, most for U.S. citizenship, that had generated national security hits on IBIS were sitting in limbo at USCIS headquarters because the employees trying to process them were unable to obtain the national security information that caused them to be flagged. If a government agency (e.g., FBI, CIA, DEA, ATF) has national security information about an alien, or when an agency has an ongoing investigation that involves an alien, the USCIS employee who runs a name check in TECS will

¹⁸ See Attachment 16: Update on Philadelphia A-files.

see only a statement indicating that the particular agency has national security information regarding the alien. (This is assuming that the employee has Level 3 TECS access; without such access, the employee may get no indication at all that national security information exists.) Employees are not permitted to deny an application “just” because there is national security information or a record with another law enforcement agency. Instead, the employee must request, acquire, and assess the information to see if it makes the alien statutorily ineligible for the immigration status or document being sought, or inadmissible or deportable. However, whether or not an employee can get the national security information, in order to assess it, depends on at least two things:

- 1) The level of background investigation the employee has undergone, which determines the types of information he or she is lawfully permitted to access; and
- 2) The nature of the national security information, which determines the willingness or ability of the agency with the information to share it with non-law enforcement personnel (all USCIS employees, including those in the Fraud Detection and National Security unit, are non-law enforcement except for the 1811 criminal investigators and some of the 0080 security specialists who work in OSI).

The more sensitive the national security information, the less likely that the non-law enforcement employee will be able to get it. This is the genesis of the so-called “FOCUS” cases—employees see that there is national security information on the alien, but they are unable to obtain the information to assess it. The bulk of FOCUS cases are applications for naturalization because naturalization regulations require USCIS to make a final decision within 120 days of interviewing the applicant. Once that 120-day window closes, the applicant can petition a court for a writ of mandamus, and the court will order USCIS to issue a decision. USCIS set up a group of employees, the FOCUS group, to review these applications and issue the final decisions. However, as non-law enforcement personnel, they may have no better access to the relevant information than the original employee who sent the application to Headquarters in the first place. (In fact, some FOCUS employees do not even have access to Level 3 TECS records.¹⁹) OSI, whose law enforcement personnel have the security clearances and the contacts necessary to obtain the pertinent information, offered to assist employees with these applications. Rather than utilizing OSI, however, USCIS leadership instructed the FOCUS group members to contact FDNS—the official USCIS liaison with outside law enforcement and intelligence agencies—when they need additional information about any of these cases. Since FDNS lacks law enforcement personnel, it, too, has been unable to obtain the necessary information from these outside agencies in some cases.

In documented instances, FDNS has instructed FOCUS employees to grant a benefit, even though neither FDNS nor the FOCUS employee knew why the alien generated a national

¹⁹ See Attachment 17: O’Reilly email.

Checking Terrorism at the Border

security indicator.²⁰ Despite the fact that my staff was willing and able to assist in obtaining the national security information that was otherwise unavailable to USCIS, I was ordered directly by Acting Deputy Director Divine to remove myself and my staff from any involvement with the FOCUS cases and to cease any communication with the FBI and the intelligence community. I was told repeatedly that FDNS was the official liaison and so I was to have no further contact with any law enforcement or intelligence agencies or participate in any information sharing, either within USCIS or outside USCIS. I have been told that my successor is working under the same constraints.

The result is that FOCUS employees are faced with a choice between approving an application for U.S. citizenship with limited information about what raised a national security flag versus denying the application, perhaps wrongly, or asking someone at OSI to violate the direct order of the Acting Deputy Director and the Chief of Staff in order to share critical information with them.

In a November 2005 report on Alien Security Checks by DHS-OIG, USCIS told the IG investigator that “FDNS has resolved all national-security related IBIS hits since March 2005. FDNS’s Background Check Analysis Unit reviews, tracks, analyzes, and resolves all name-vetted hits related to national security” [emphasis added]. Technically, this statement is true, but only because the former head of Domestic Operations redefined the word “resolution.” In a memo dated March 29, 2005, Bill Yates says in a footnote:

“Resolution is accomplished when all available information from the agency that posted the lookout(s) is obtained. A resolution is not always a finite product. Law enforcement agencies may refuse to give details surrounding an investigation; they may also request that an adjudication be placed in abeyance during an ongoing investigation, as there is often a concern that either an approval or a denial may jeopardize the investigation itself” [emphasis added].

In other words, USCIS employees can “resolve” a national security hit simply by asking why the alien is flagged, regardless of whether the employee is actually able to obtain the data necessary to decide the application appropriately. One of the first lessons employees are taught is that they must grant the benefit unless they can find a statutory reason to deny it. ***Without the national security information from the law enforcement agency, the employee must grant the benefit unless there is another ground on which to deny it, even where the applicant may present a serious threat to national security.***

Mr. Chairman and Members of the Subcommittee, as you can see, USCIS is operating an immigration system designed not to aggressively deter or detect fraud, but first and foremost to approve applications. Ours is a system that rewards criminals and facilitates the movement of terrorists.

²⁰ See Attachments 18 and 19: FOCUS emails.

Checking Terrorism at the Border

On no less than 8 occasions in the past year, the DHS Inspector General and the GAO have reported critical, systemic failures in the immigration system. They have raised the national security red flag with regard to cyber attack, terrorist attack, criminal fraud, and penetration by foreign intelligence agents posing as temporary workers. All while the bad guys are patiently working within the framework of our legal immigration system, often with the explicit help of USCIS.

Currently, the USCIS Headquarters Asylum Division has backlog of almost 1000 asylum cases that it has not reported to you as Members of Congress, to the Inspector General, or to the American people. This backlog includes two kinds of asylum claimants:

- a. Individuals who claim that they have been falsely accused by their home government of terrorist activity; and
- b. Individuals who have provided material support to a terrorist or a terrorist organization.

These asylum claimants, most of whom fall into the second category, are in the United States right now. Some have been awaiting a decision since late 2004 on whether the Secretary of Homeland Security, after consulting with the Secretary of State and the Attorney General, will grant them a waiver of inadmissibility, so that they can stay permanently in the United States, despite having provided material support to terrorists. It is no wonder DHS does not want to report this backlog.

But there is more. The USCIS Headquarters Fraud Detection National Security unit also has an unreported backlog.²¹ As of September 24, 2005, this backlog included 13,815 immigration applications that had resulted in an IBIS "hit" involving national security, public safety, wants/warrants, Interpol, or absconders. FDNS had a separate backlog of 26,000 immigration applications that resulted in some other kind of IBIS "hit."

In late March 2005, FDNS began requiring that all national security-related IBIS hits be sent to Headquarters for resolution. During the 6 months between April 2005 and the end of September, FDNS HQ received 2,000 national security hits and reached "final resolution" on 650, leaving 1,350 pending by the beginning of October.

This backlog of national security cases is particularly disturbing when put in the context of USCIS's definition of how to "resolve" a national security case. One has to wonder how many of them were "resolved" simply by asking for the national security information and then granting the application when the agency with the information refused to share it. We have proof of at least one case where that would have happened, had OSI not stepped in and provided the national security information.²² The USCIS General Counsel's office points out

²¹ See Attachment 20: USCIS response to press.

²² See Attachment 18: FOCUS email

another such case, except that they expect to grant the application for citizenship despite the national security hit because the national security information “is unavailable to USCIS at this time.”²³

Perhaps the following finding from the GAO sheds light on the truth:

Verifying any applicant-submitted evidence in pursuit of its fraud-prevention objectives represents a resource commitment for USCIS and a potential trade-off with its production and customer service-related objectives. In fiscal year 2004, USCIS had a backlog of several million applications and has developed a plan to eliminate it by the end of fiscal year 2006. In June 2004, USCIS reported that it would have to increase monthly production by about 20 percent to achieve its legislatively mandated goal of adjudicating all applications within 6 months or less by the end of fiscal year 2006. It would be impossible for USCIS to verify all of the key information or interview all individuals related to the millions of applications it adjudicates each year approximately 7.5 million applications in fiscal year 2005 without seriously compromising its service-related objectives.”²⁴

USCIS leadership has been warned repeatedly of national security vulnerabilities in the asylum, refugee, citizenship, information technology, and green card renewal systems by me personally, by the GAO, by the Inspector General, and no doubt, by others. Time and again, they have ignored warnings of systemic weaknesses wide open to exploitation by criminals, terrorists, and foreign agents. When faced with irrefutable proof of vulnerabilities, they attempted to balance national security and customer service and explained to me that immigration was a right not a privilege. They have knowingly misled Congress, the Inspector General’s Office, the GAO, and perhaps most disheartening, the American people. They are attempting to simply reboot the immigration system, in the hope that whatever system conflict there is will just resolve itself. In this case, however, if you just reinstall the same software, with the same software engineers, and without the necessary safeguards in place to catch viruses or deter hackers, the system simply replicates itself and bogs down all over again, until one day there is a catastrophic failure. This root conflict is not going to go away without immediate and enormous change. The immigration process itself is flawed and is being exploited internally and externally by criminals, terrorists, and foreign intelligence agencies.

In closing Mr. Chairman, I sit before this committee, having lost my career, my passion for service to the government, my faith that someone somewhere would do the right thing within DHS. I know there are more good men and women in the agency who would like nothing more than to do their part in fixing this broken system. I have now been able to present some of the information I have gathered to the FBI, the GAO, the Inspector General,

²³ See Attachment 11: Memorandum for WIC Members, March 13, 2006, p. 4, 3rd item.

²⁴ “Additional Controls and a Sanctions Strategy Could Enhance DHS’s Ability to Control Benefit Fraud,” Government Accountability Office, GAO-06-259, March 2006, p. 26..

Checking Terrorism at the Border

and to you. Thankfully, senior leadership can no longer retaliate against me, for I am no longer employed by DHS. Based on the response I have seen thus far, I am hopeful that enough people will come forward that, with your help, we will finally be able to force serious change on an agency that has needed it desperately for decades.

Chairman Royce, Ranking Member Sherman, and Members of the Committee, thank you all for your support. I would be happy to answer any questions you may have at this time.