Testimony of

MICHAEL J. MAXWELL

on

Whether Attempted Implementation of the Senate Immigration Bill Will Result in an Administrative and National Security Nightmare

before

The Subcommittee on Immigration, Border Security, and Claims

Committee on the Judiciary

U.S. HOUSE OF REPRESENTATIVES

Thursday, July 27, 2006

Mr. Chairman and Members of the Subcommittee,

I am pleased to be here today to discuss the impact that implementation of S. 2611 by US Citizenship and Immigration Services (USCIS) would have on national security. As the former Director of the Office of Security and Investigations (OSI), the only law enforcement component within USCIS, I must point out that the basic premise of this hearing—that implementation of S. 2611 could *create* an administrative and national security nightmare—is faulty. The fact is that an administrative and national security nightmare *already exists* at USCIS under our current immigration policy. Implementation of the Senate bill would codify the nightmare and ensure that the criminals, terrorists, and foreign intelligence operatives who have already gamed our immigration system are issued legal immigration documents and allowed to stay permanently.

Asking USCIS to implement a proposal as sweeping as S. 2611 without first addressing the existing national security vulnerabilities in our immigration system would be irresponsible, at best, and could actually facilitate ongoing criminal enterprises. I also agree with Director Gonzalez who, on at least three occasions, has stated that it would be impossible for USCIS to implement the Senate bill within the prescribed time frame. The agency has neither the personnel nor the infrastructure to process an additional 10 to 20 million applications. I would go one step further and suggest that USCIS could never implement S. 2611 without fully compromising national security. The entire underlying immigration system is simply too flawed.

Doctor Gonzalez was warned by me, and by others, both prior to his confirmation as Director and immediately following, that USCIS is a vipers nest of career federal employees willing to cover up faults in the system to advance their careers, to obstruct ranking political appointees—including the previous Director—at the cost of national security, and to institute policies, programs, and systems independent of Headquarters and Administration direction for their own gain. Since I last briefed this subcommittee in September of 2005, nothing has changed. In fact, recent news from USCIS only verifies the fact that we are seeing the beginning of the convergence I predicted at that briefing: the perfect immigration storm.

Building on a Faulty Foundation

Our current immigration system is broken. On this statement there is virtually universal agreement, even among administration officials:

- During his October 18, 2005 testimony before the Senate Judiciary Committee, DHS Secretary Michael Chertoff stated, "we recognize that the current [immigration] situation is in desperate need of repair." He went on to acknowledge, "Parts of the system have nearly collapsed under the weight of numbers."

- At an April 5, 2006, press conference to announce the creation of task forces to combat immigration and document fraud, Assistant Secretary for Immigration and Customs Enforcement (ICE) Julie Myers pointed out that terrorists have used legal immigration channels like asylum to embed in American society. She noted that "each year tens of thousands of applications for immigration benefits are denied because of fraud, and those are just the ones we find.
- On April 13, 2006, Janice Sposato, head of the newly created National Security and Records Verification Directorate at USCIS, was quoted in a UPI article as saying that USCIS adjudicators sometimes find themselves in a "difficult and ambiguous legal situation" when trying to weed out those who might pose a terrorist threat. "I'm not going to tell you I have all the tools I need" to deny citizenship and other immigration benefits to potential terrorists, she acknowledged.
- On June 11, 2006, ICE posted the following on its website:

  "ICE also participates in the interagency **Identity & Benefits Fraud Task Force**, which seeks to restore integrity to the immigration process and prevent terrorists and criminals from entering the United States. . . . **Operation Integrity** is a new **Identity & Benefits Fraud** Unit initiative to restore integrity to the immigration system and to address vulnerabilities in the system that terrorist or criminal organizations could exploit to gain entry to the country. Operation Integrity will support a nationwide system of "IBF Task Forces" to detect, deter, and disrupt criminal and terrorist organizations that attempt to exploit the immigration system"
- On June 20, Karl Rove told the National Federation of Independent Business "immigration is turning into a big problem. The more you look at it, the more clear it is that every single part of the system is broken."

  Here are just a few examples to support Mr. Rove's critical assessment:
- The DHS Inspector General recently reported that, from 2001 through the first half of 2005, 45,000 high risk aliens from state sponsors of terrorism and special interest countries have been released into American communities because of the inability of DHS to conduct a thorough background check on aliens.[1]
- An internal USCIS document reveals a backlog, as of late September 2005, of more than 41,000 immigration applications with IBIS hits requiring further investigation.[2]
- Senior-level USCIS staff have information indicating that suspected terrorists have established bogus educational institutions in multiple U.S. communities and used the student visa program to move recruits into the United States.

---

[1] Attachment 1: *Detention and Removal of Illegal Aliens*, OIG-06-03, Office of the Inspector General, Department of Homeland Security, April 2006, p. 10.

[2] Attachment 2: "Draft—10/4/05 Initial Statement," p. 2.

- Recent USCIS immigration fraud assessments indicate that the incidence of fraud in some visa categories is as high as 33 percent.[3]
- Since 2004, at least 17 reports by the GAO and DHS OIG have revealed critical flaws in the way USCIS implements the immigration process. Annual reports by the Citizenship and Immigration Services Ombudsman identify additional problems.

Virtually every part of our immigration system is broken and needs to be reengineered. But there are three overarching issues that, in my professional view, must be addressed before any policy reforms can be effective. They are:

1. Rampant internal corruption;
2. A customer-service mentality that, despite vocal public denials by appointed official, invariably trumps national security concerns; and
3. A failure or refusal to share critical national security information even among the different component-agencies of the Department of Homeland Security (DHS), let alone with outside law enforcement or intelligence agencies.

Any one of these, individually, presents an opportunity for criminals, terrorists and foreign intelligence services to do this nation grave harm. Combined, these three issues present policy makers, law enforcement, the intelligence community and the American people, with the unenviable challenge we face today: managing the consequences of a failed immigration system. To continue forward, to build upon the existing foundation, is akin to building a house on a cracked foundation—it is only a matter of time before the foundation shifts and the house falls.

Rampant Internal Corruption

As the agency that hands out green cards, work permits, and citizenship, among other immigration benefits, the temptations for employees of USCIS to commit crime are constant. USCIS employees work in an atmosphere that permits—and often encourages—the waiving of rules. It is only a small step from granting a discretionary waiver of an eligibility rule to asking for a favor or a taking a bribe in exchange for granting that waiver. Once an employee learns he can get away with low-level corruption and still advance up the ranks, he or she becomes more brazen. The culture of corruption that permeated the old INS transferred intact to USCIS. This environment presents an easy target of opportunity for criminals, terrorists, and foreign intelligence operatives to ply their trade.

When I first briefed this Subcommittee on September 29, 2005, the Office of Security and Investigations had a backlog of 2,771 complaints against USCIS employees. The complaints alleged everything from overdue benefits and misuse of government property to bribery, undue influence of foreign governments, and espionage. Of the total backlog, 528 alleged

---

[3] *Immigration Benefits: Additional Controls and a Sanctions Strategy Could Enhance DHS's Ability to Control Benefits Fraud*, Government Accountability Office, March 2006, p. 16.

criminal violations. Included among these were national security cases, such as allegations that USCIS employees had provided material support to known terrorists or that they were being influenced by foreign intelligence services. Complaints with clear national security implications represented a small share of the total, but with these cases, even one is too many.

Allegedly corrupt employees ranged from mail clerks to top-level managers at headquarters and senior personnel in the field and overseas. Despite the fact that I had set aside money from OSI's budget to purchase a case management system to track these complaints, I was told that I could not purchase one, so we had no way to track our caseload or conduct link analyses. We had no way to investigate more than a small handful of criminal allegations since I was only permitted to hire six criminal investigators, despite the fact that I had been authorized in writing to hire 30. Since two of the six were assistant directors at OSI headquarters, I had a grand total of four investigators in the field.

Today, almost a year later, the backlog of misconduct complaints against USCIS employees is well over 3,000. This number does not include some 500 complaints that disappeared after Chief of Staff Paar and Deputy Director Divine took possession of all the complaints last winter and failed to return the same number they took.

Importantly this number also no longer includes service complaints (i.e., overdue immigration benefits), which are now separated and forwarded to the appropriate offices as they arrive. The total number of complaints, as well as the number that allege criminal violations, are unknown since OSI still has no case management system. New complaints are still coming in at a rate of around 50 per week, as was true when I was director. OSI still has a grand total of four criminal investigators in the field to handle all complaints. The two career special agents I had assigned to investigate espionage and terrorism-related allegations resigned in disgust, with one citing his desire to leave DHS to go "fight the war on terrorism."

While there are still multiple ongoing national security investigations and investigations against high-ranking USCIS personnel, there have been three high-profile arrests of USCIS employees in the past several months, along with one conviction.

- March 21, 2006— Eddie Romualdo Miranda, a USCIS adjudicator in Santa Ana, California, was arrested by local police on charges of attempted oral copulation and sexual battery under color of law for demanding sexual favors from a naturalization applicant in exchange for approving her application;
- March 22, 2006—Lisa Ann Gross, a contract employee of USCIS, was convicted of providing confidential law enforcement information to the target of a drug investigation after she gained unauthorized access to The Enforcement Communications System (TECS). This case represents the first criminal conviction in a case opened and investigated by OSI;
- June 7, 2006—Phillip A. Browne, a USCIS adjudicator in New York City, was arrested with his sister and 28 others and charged with arranging sham marriages, producing

fake documents, selling one million dollars worth of green cards, and laundering the proceeds over a period of more than four years. The FBI, ICE, and the DHS Office of the Inspector General (OIG) conducted the investigation and made the arrests.

- June 29, 2006—the FBI, arrested Robert T. Schofield, a former Deputy District Director in the Washington field office of USCIS, after a joint investigation with the OIG, for falsifying naturalization certificates for Asian immigrants. Allegations against Schofield for misconduct, including accepting bribes, unauthorized use of government credit cards, and falsifying immigration documents, date back at least 10 years. Arrested with Mr. Schofield was a Chinese national, Qiming Ye, referred to by authorities as an "immigration broker" for Chinese seeking immigration status in the United States.

I applaud the efforts of the local law enforcement officers and federal agents involved in the investigations listed above. Realistically, however, these cases represent the tip of the iceberg and numerous arrests should be forthcoming. At the time of my resignation as Director of OSI, the backlog of complaints included nearly 100 bribery allegations. Those allegations—which in March were intentionally under-reported by more than half to the DHS OIG by USCIS senior management—remain untouched, as do allegations of extortion, harboring illegal aliens, and structuring. Substantiated instances of foreign government influence and potential national security breeches by employees also have yet to be addressed, despite repeated warnings.

Yet USCIS still refuses to aggressively support the new Director of OSI and his staff with either a reasonable budget or a rational policy. As long as OSI remains woefully under funded, understaffed, and prohibited by management from carrying out its mission, rampant corruption will continue.

I warned both Chief of Staff Paar and then-Acting Deputy Director Divine on September 5, September 29, and 0ctober 5, 2005, that the lack of an Internal Audit Department at USCIS, capable of rooting out anomalies in the work product of supervisory immigration officers, presents a compelling national security threat. These warnings fell on deaf ears. In fact, I was ordered by both not to have direct contact or participate with the Joint Terrorism Task Force or the Intelligence Community.

USCIS staff at Headquarters continues to insist that sufficient safeguards are built into the system to prevent immigration officers from granting benefits to the wrong people for the wrong reasons. The recent arrests, along with the case of the Iraqi Asylum Officer that appeared in the Washington Times in April, belie their claims.[4] Consider the extent to which one immigration officer could compromise national security over the course of a thirty year career by granting immigration benefits at the behest of enemies of the state. When the nexus between foreign intelligence services and state sponsors of terrorism, such as Iran, is factored in with the lack of internal checks and balances at USCIS, and the temptations employees face,

[4] Attachment 3: Dinan, Stephen, "Iraq spy suspect oversaw U.S. asylum," Washington Times, April 6, 2007.

the result is a recipe for disaster—a disaster not in the making, but already upon us. At the time of my resignation, OSI had initiated more than ten national security preliminary inquires involving employees. Instead of monitoring the email of suspected corrupt employees, however, USCIS senior management is monitoring the email of potential whistleblowers and my own.

Only when employees face a serious risk of detection and prosecution will they begin to think twice about violating the law. In the meantime, the Senate bill represents new opportunities for corrupt employees and our adversaries. It would create a huge new pool of aliens willing to pay bribes or perform sexual favors in exchange for immigration benefits. Moreover, we know that both foreign intelligence service personnel and terrorists closely study our immigration system, the agencies that administer that system, and its personnel. Once the agency was thoroughly overwhelmed by its additional workload under S. 2611, the chance of detecting foreign intelligence service personnel or their proxies would be completely lost.

Overriding Customer-Service Mentality

USCIS is suffering from an identity crisis brought on by years of mismanagement and unwittingly encouraged by Congress. The central mission of USCIS is to execute the immigration laws enacted by Congress and to ensure that only those aliens who are eligible and who do not pose a risk to the United States or its residents are able to obtain permission to remain here. However, the agency sees itself as a "relocation facilitator" whose business is to serve aliens—the "customers"—wishing to reside here. The fact that the "customer" may be a violent criminal intending to victimize innocent Americans or a terrorist or spy intent on the destruction of the country is viewed as an acceptable risk. Historically, USCIS field offices have operated as fiefdoms and viewed headquarters as a necessary evil, worthy of lip service, but incapable of getting the job done. When policies were slow coming from inside the beltway, politically powerful Regional or District Directors would often implement their own policies and develop their own programs.

Despite vehement claims to the contrary by political appointees, USCIS is operating an immigration system designed not to aggressively deter or detect fraud, but first and foremost to approve applications. The desire to eliminate the backlog of benefit applications is so strong, for example, that USCIS management has redefined it at least three times in order to knock millions of pending applications off the list, including more than 235,000 that are awaiting an FBI name check.

USCIS senior leadership is much more concerned with reducing the backlog than with the integrity of the process. At one point, OSI opened a preliminary inquiry into allegations that over one million biometric files had disappeared from USCIS. Not long after we began investigating, we were assured that the biometrics had been found, though no one could quite explain what had happened. In another instance, allegations received by my office suggested that, since benefit applications are not counted toward the backlog until they are data entered,

boxes of A-files were being stacked and never entered into the computer systems so USCIS could report to Congress a reduction in the backlog.

The absolute lack of a national security perspective on the part of senior managers is clear in their responses to the following agency-wide issues that unmistakably jeopardize national security.

Auto-Adjudication System

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 an employment authorization document (EAD). As of May 2006, only five USCIS district offices were able to process all LPR applications within 90 days. Since none of the other district offices and none of the five service centers can meet this goal, 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.

According to the GAO and the Citizenship and Immigration Services Ombudsman, this regulation has led to widespread fraud. Illegal aliens can simply file a fraudulent application for adjustment to LPR status, wait 90 days, and then receive 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 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 or a firearms license, board an aircraft, etc. The Citizenship and Immigration Services Ombudsman estimates that 325,569 EADs were issued to ineligible aliens between May 2004 and February 2006.[5]

Following my resignation, a tip I received from a USCIS/Fraud Detection and National Security (FDNS) Officer led to the discovery of an "auto-adjudication" system in use at the Texas Service Center. Additional whistleblowers stepped forward shortly thereafter and notified me that similar systems may be operating in other service centers. In order to address the demand for EADs as interim benefits, it appears that the Texas Service Center had developed a system that could process applications for EADs 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 examined the supporting documentation to look for signs of fraud. Instead, the EAD was approved automatically when the underlying application for LPR status had been pending for 90 days.

Further investigation led to additional whistleblower communications indicating that senior management had failed to inform the Chief Information Officer of the development of these systems and that they are not secure systems. In fact, they are completely unprotected against cyber intrusion, sabotage, and manipulation, like much of the IT system at USCIS.

---

[5] *Annual Report to Congress*, Citizenship and Immigration Services Ombudsman, Department of Homeland Security, June 2006, p. 20.

[Earlier this year, late on the day of a planned cyber-attack test of the USCIS IT system, the ICE Computer Security Incident Response Center, which was charged with detecting the intrusion, called USCIS IT Security personnel to ask if the test had been called off. Instead, they were informed that the attack had been launched as planned and the intrusion had been occurring undetected for the past eight hours.]

This auto-adjudication system only processes EADs that are linked to an application for adjustment to lawful permanent residence, which means that the initial, automated IBIS name check of the applicant is conducted when the underlying application is data entered. However, this initial IBIS name check searches only on the name of the applicant as clerical staff entered it into the computer system. It does not look for spelling variations or for aliases, and so is by no means a conclusive security check. By the time this system approves an EAD, it is likely that no one has actually looked at the application since the clerical staff received it from the applicant and verified only that it contained the proper fee and a signature. It seems apparent that the designers of this system gave no thought to fraud or national security, but instead were focused on convenience.

Remote Adjudication System

Another adjudication system identified during the same review that uncovered the auto-adjudication system is even more troubling. Staff at the National Benefits Center in Lee's Summit, Missouri, acknowledged that there is a program embedded in CLAIMS3, the backbone of the ICE/USCIS IT system, without the knowledge or approval of the USCIS or DHS Chief Information Officers. This rogue system, as it was referred to by IT Security personnel, allows a remote user to bypass the normal data-entry process and manually insert any number of immigration files (what appear to be fully adjudicated applications for EADs and replacement green cards) into the computer system so that all standard application screening processes, including the "Lock Box function," which accounts for the receipt of immigration processing fees, and ALL background checks, including the initial, automated IBIS check, are circumvented.

IT security staff intended to conduct a thorough investigation into this remote system, but after they submitted their initial report, they were prohibited from accessing CLAIMS3 to proceed with the investigation and were told to rewrite the report.[6] There are, apparently, two subsequent versions of this report, both of which have been sanitized to varying degrees. I have been told by a whistleblower that he was specifically told not to mention the existence of this remote adjudication system to OSI criminal investigators. Further, the Director of Adjudications at the National Benefits Center claimed to have no knowledge of any process allowing manual insertion of files into the system. Only the IT staff at the Center admitted knowledge of its existence.

---

[6] Attachment 4: *National Benefits Center Adjudication Process Review*, Office of the Chief Information Officer, March 23, 2006.

When I first mentioned the existence of this system during an April 2006 hearing before the Subcommittee on International Terrorism and Nonproliferation of the House International Relations Committee, USCIS claimed that only EAD applications from Mariel Cubans, documents submitted in response to Requests for Evidence, and applications that have been terminated by other Service Centers can be manually entered into CLAIMS3 at the National Benefits Center. However, this claim is not supported by the fact that the system is operated remotely from USCIS Headquarters in Washington, DC. Nor is it supported by the fact that the system is operated by a well-connected contract employee, or someone using his screen name, at Headquarters, and utilizes a post office box in Washington that comes back to the following address:

> Library of Congress, Cataloging Distribution Service, CDS/MU, PO Box 75840, Washington, DC 20013.

Finally, the attached screen scrape from the remote adjudication system shows that applications for both EADs (I-785s) and replacement green cards (I-90s) are being processed for aliens from a variety of countries other than Cuba, including China, Colombia, Germany, Mexico, Pakistan, Russia, and South Africa.[7] According to IT security experts, someone in Washington, DC, not in Lee's Summit, Missouri, is creating records indicating that benefits have been approved, even though no processing fee has been received by USCIS.

One would assume that if it were a legitimate system, the investigating IT staff would have been informed of its purpose and assured that it was being audited, rather than being forbidden from investigating further and forced to rewrite a report to remove potentially embarrassing information. Additionally, if it were a legitimate system, USCIS would be required to make it comply with the Federal Information Security and Management Act (FISMA), as is required for all DHS IT systems. Of course, certain agencies are allowed to manipulate immigration data in order to mount law enforcement sensitive operations. The large volume of records being created, among other things, argues against this explanation. If it is a law enforcement system, however, a poorly designed audit trail lifted the veil.

IBIS Checks on Aliens

The Enforcement Communications System (TECS), which is managed by Customs and Border Protection, is essentially a gateway to the Interagency Border Inspection System (IBIS), which consolidates the records of some two dozen Federal law enforcement and intelligence agencies—including the Federal Bureau of Investigation, the Drug Enforcement Agency, the Bureau of Alcohol, Tobacco and Firearms, and the intelligence community—and provides access to state criminal and motor vehicle records. Through TECS, authorized adjudicators can run a name through IBIS to find outstanding warrants, terrorist connections, immigration violations, and other information necessary for deciding whether an alien should be permitted to remain in the United States.

---

[7] Attachment 5: Screen scrape of applications processed remotely in one 30-day period, along with an edited version that shows more clearly the countries of origin of beneficiaries of the remote processing system.

On October 5, 2005, before the Acting Deputy Director and others, the USCIS Director of Fraud Detection and National Security, Louis "Don" Crocetti, explained the four categories of TECS records as follows:

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

When DHS was created in January 2003, CBP, as the manager of TECS, entered into an agreement with USCIS that required USCIS employees to undergo full background investigations (BIs) before they may be granted Level 3 TECS access. Because of the sensitive nature of some of these records, including on-going national security cases, it was and is important that access to Level 3 records be restricted to adjudicators who themselves have been thoroughly vetted.

The agreement included a two-year grandfather period during which legacy Immigration and Naturalization Service (INS) personnel that had had access to Level 3 TECS records at the INS would continue to have access so that USCIS would have time to complete BIs on new employees and upgrade those on legacy employees when necessary.

USCIS leadership, however, decided not to spend the money to require full BIs on new personnel or to upgrade the BIs on legacy personnel. Thus, when the grandfather period ended in January 2005, CBP began restricting access by USCIS adjudicators with only limited BIs, so that these adjudicators could access only Level 1 records or, in some cases, Level 2 records through TECS. They could not access the national security, public safety, or terrorist records they needed to adjudicate 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 adjudicators 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 OSI and certain FDNS personnel. Backlog elimination was the top priority of the agency, so adjudicators were pressured to keep pumping out the benefits 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.

Internal documents make the problem abundantly clear:

> " Without access to higher level extra-agency TECS records, USCIS employees with background check responsibilities may miss information that is critical to the adjudicative process. In the absence of this information, USCIS could grant an immigration benefit to someone who poses a threat to national security or public safety."[8]

When I first briefed this Subcommittee on September 29 of last year, I noted that roughly 1,700 USCIS adjudicators lacked sufficient access to TECS to determine whether an applicant has known terrorist connections or is a threat to public safety. About 80 percent of all applications filed with USCIS are processed through a batch system that automatically runs the proper level background check on each applicant. The other 20 percent, however, are handled individually and an adjudicator must conduct the background check in TECS. This tiered system was discussed in great detail at a meeting of senior leadership on October 5th 2005.

The purpose of the meeting was to prepare for a briefing that ADD Divine and CoS Paar would provide Secretary Chertoff on both internal corruption at USCIS and TECS access—or lack thereof—on October 7, 2005. Then-Acting Deputy Director Robert Divine, Chief of Staff Tom Paar, Chief Counsel Dea Carpenter, Director of FDNS Don Crocetti, then-Deputy Director of Domestic Operations Janice Sposato, and I were all present, as were a handful of other senior staff.

Director Crocetti and his staff presented the results of a test they had conducted on TECS. According to conclusive documentation from his National Security Chief of Staff, adjudicators with only TECS Level 1 or Level 2 access were totally missing national security and public safety information about applicants. In essence, they were operating blind.

We discussed the fact that, if background checks on 20 percent of the 7.3 million applications adjudicated by USCIS in FY 2005 were handled manually, that would mean that somewhere around 628,000 applications were likely processed by the 1,700 adjudicators who lacked Level 3 access to TECS. This figure did not take into account the fact that adjudicators without Level 3 access may be able to process cases faster because they get fewer background check "hits" to resolve.

The obvious conclusion was that all USCIS adjudicators needed access to Level 3 TECS records in order to properly vet applicants for immigration benefits and to ensure that known terrorists and others who present a threat to national security or public safety are not able to obtain immigration benefits. The only short-term solution would mean re-engineering the USCIS business process and slowing down adjudications by allowing only adjudicators with Level 3 access to conduct manual background checks. The long-term solution was to spend upwards of $10 million to upgrade security clearances for USCIS adjudicators. Of course, neither solution pleased top management.

---

[8] Attachment 6: *USCIS TECS Users Report*, Office of Fraud Detection and National Security, US Citizenship and Immigration Services, July 25, 2005, p. 6.

At that point, ADD Divine announced that we had reached a core question: Whether immigration to the United States is a right or a privilege. He then asserted that it has always been the position of INS and now USCIS that immigration is a right, rather than a privilege. Chief Counsel Carpenter concurred.

Thus, it is no surprise that, in the wake of this meeting, USCIS chose neither the short-term solution nor the long-term solution. Instead, since mid-October of 2005, senior USCIS managers have been meeting with CBP officials and trying to convince them to extend the grandfather period, to restore and/or upgrade TECS access to those adjudicators who have been cut off or restricted, and to waive in without the required background investigations contract workers hired to eliminate the 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.]

To date, not one adjudicator with a deficient background investigation has been scheduled for an upgrade and, while it does appear that CBP has extended the grandfather period, no memorandum of understanding between the two agencies has been signed. In fact, just four days ago (July 24), an adjudicator in the Midwest confirmed that he still has Level 2 TECS access, more than nine months after USCIS leadership was shown conclusively that adjudicators must have Level 3 access to ensure national security.

Background Investigations of Employees

My former office is tasked with adjudicating the background investigations of USCIS employees once the Office of Personnel Management gathers the information. Shortly after OSI was created, in the fall of 2004, we inherited a backlog of 11,000 pending BIs on USCIS employees. In light of the fact that I had a total of six personnel security specialists to adjudicate BIs, it is remarkable that we managed to reduce the backlog to about 7,000 by the time I resigned in February 2006. Because of the hiring frenzy driven by backlog elimination, however, OPM was sending new BIs at a rate of 3.5 for every one that OSI cleared.

I submitted at least eight proposals to increase the number of personnel security specialists to address this backlog, but they all were denied by senior management. Finally, in January 2006, CoS Paar approved 15 additional positions for OSI, but told me to prioritize internal affairs and indicated that five additional personnel security specialists to adjudicate background investigations should be sufficient. That is a total of 11 people to adjudicate the 7,000 backlogged BIs, plus the BIs for new adjudicators hired to eliminate the backlog, plus up to 4,000 upgraded BIs on current adjudicators whose access to TECS was or could be restricted.

Asylum Seekers with Terrorist Ties

As of March 10, 2006, the USCIS Headquarters Asylum Division had a segregated backlog of almost 900 asylum cases that it had not reported to Congress except as part of the overall backlog. This particular backlog includes two groups of asylum cases, both of which raise serious national security questions:

1. 369 cases in which the applicants claim that they have been falsely accused by their home government of engaging in terrorist activity; and
2. 515 cases in which the applicants have provided material support to a terrorist or a terrorist organization.

These asylum applicants are in the United States right now; some have been here since November 2004. Their cases are on hold because DHS and USCIS counsel, along with the Justice Department's Office of Immigration Litigation, asked the Asylum Division to refrain from denying asylum in cases like these—even though the applicants are inadmissible as terrorists or terrorist supporters—in order to give DHS time to develop procedures for considering whether the Secretary of Homeland Security should exercise his non-reviewable discretion to grant them a waiver of inadmissibility, so that they can stay permanently in the United States, despite their terrorist ties. DHS has established a working group to propose the procedures.

Failure to Share Information

National Security Hits on IBIS

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 adjudicators 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 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 will get no indication at all that national security information exists.) Adjudicators are not permitted to deny an application "just" because there is national security information or a record with another law enforcement agency. Instead, the adjudicator 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 adjudicator can acquire the national security information, in order to assess it, depends on at least two things:

1. The level of background investigation the adjudicator 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 a non-law enforcement employee will be able to get it. This is the genesis of the cases that are referred to what used to be called the "FOCUS group," but has been renamed the National Security and Records Verification Directorate (NSRV): adjudicators see that there is national security information on the alien, but they are unable to obtain the information to assess it.

The most troubling of these cases are applications for naturalization because 8 U.S.C. 1447(b) requires 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, and the court can either grant or approve the application, or it can order USCIS to issue a decision, regardless of whether a national security hit has been resolved. [The law also prohibits USCIS from scheduling the interview before the results of the background checks are returned, but, until recently, USCIS was ignoring this prohibition since it impeded backlog reduction.]

USCIS set up a group of adjudicators in Headquarters—formerly called FOCUS; currently, the NSRV—to review these applications and either advise field adjudicators or simply issue the final decisions. However, as non-law enforcement personnel, they may have no better access to the relevant law enforcement information than the original adjudicator who referred the application to Headquarters in the first place. OSI, whose law enforcement personnel have the security clearances and the contacts necessary to obtain the pertinent information, offered to assist adjudicators with these applications. Rather than utilizing OSI, however, USCIS leadership instructed adjudicators to contact only FDNS. 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 adjudicators to proceed with processing an application for U.S. citizenship, even though neither FDNS nor the adjudicator knew why the alien had generated a national security indicator.[9] 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 these 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 adjudicators 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 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 "FDNS has resolved <u>all national-security related IBIS hits since March 2005</u>.

---

[9] Attachments 7 and 8: FOCUS emails.

FDNS's Background Check Analysis Unit reviews, tracks, analyzes, and resolves all name-vetted hits related to national security" [emphasis added].[10] 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 writes 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].*[11]

In other words, USCIS immigration officers can "resolve" a national security hit and grant a benefit simply by asking the agency holding the information to turn it over, regardless of whether the adjudicator is actually able to obtain the data necessary to decide the application appropriately. One of the first lessons adjudicators 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 adjudicator 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.

Amazingly, other DHS component agencies have stated that they will not share threat information with USCIS regarding TECS-related inquiries:

> *"CBP has advised on many occasions that it considers USCIS to be a Third Party Agency and that it will not provide details surrounding records it has placed in TECS. . .This creates an impossible situation for USCIS employees conducting background check resolution activities, as ports-of-entry note they may not release information, and the National Targeting Center, CBP's operational center, states categorically that it will not provide any assistance to USCIS callers who have encountered a CBP hit. Unless there is JTTF involvement, USCIS will not receive derogatory input from CBP beyond a TECS record."*[12]

Likewise, according to a recent GAO report, ICE officials told GAO investigators that they "opposed allowing FDNS access to sensitive case management information. They said that there was a need to segregate sensitive law enforcement data about ongoing cases from non-law enforcement agencies like FDNS."[13]

---

[10] *A Review of US Citizenship and Immigration Services' Alien Security Checks*, OIG-06-06, Office of Inspector General, DHS, November 2005, p. 37.
[11] Attachment 9: Yates memo, March 29, 2005.
[12] See Attachment 6: *USCIS TECS Users Report*, Office of Fraud Detection and National Security, US Citizenship and Immigration Services, July 25, 2005, p. 7.
[13] *Immigration Benefits: Additional Controls and a Sanctions Strategy Could Enhance DHS's Ability to Control Benefits Fraud*, Government Accountability Office, March 2006, p. 33.

Other Alien Background Checks

Because USCIS is not a law enforcement agency, unlike its predecessor, the Immigration and Naturalization Service, it faces unnecessary obstacles when it comes to conducting certain kinds of background checks:

- The FBI does not permit non-law enforcement personnel to conduct name checks, so USCIS must submit to the FBI the name of every alien for whom a name check is required (applicants for lawful permanent residence, naturalization, asylum, and cancellation of removal make up the bulk of these) and then wait for the FBI to return the results of the check. USCIS also has to pay the FBI for each name check that is conducted. Because the FBI devotes insufficient manpower to the task of running these name checks, it has a growing backlog of checks that have been requested but not run.

  When I briefed the Subcommittee last September, the FBI's name check backlog stood at about 170,000. As of May 2006, the backlog had grown to almost 236,000. USCIS reported that about 65 percent of these had been pending for more than 90 days, while the other 35 percent had been pending for more than one year.

  Since adjudicators are not supposed to grant an immigration benefit until all required background checks are completed, this backlog can cause major delays in processing times. It also presents a major national security risk for two reasons: (1) the alien is already in the United States waiting for the benefit application to be adjudicated, so this delay could provide a terrorist all the time he needs to plan and carry out his attack; and (2) as long as all required background checks have been initiated, an immigration court can order USCIS to grant an immigration benefit, even though the FBI name check is still pending. This latter situation could easily result in the granting of U.S. citizenship or permanent residence to a known terrorist.

- USCIS adjudicators cannot routinely run criminal history checks on alien applicants. Because they are not law enforcement personnel, adjudicators are only allowed to routinely search for active arrest warrants for applicants. Only if an adjudicator has reason to believe that an alien has a criminal history may he request a criminal history check.[14] Adjudicators learn about convictions that occurred prior to the filing of an application for lawful permanent residence, naturalization, asylum, cancellation of removal, and certain categories of nonimmigrant status through the FBI fingerprint check, assuming that the convicting authority has reported the conviction to the FBI.

  However, if an alien is applying for a benefit that does not require an FBI fingerprint check or if the alien is convicted of a crime after he files an application and the FBI fingerprint check is done but before the application is adjudicated, the adjudicator may approve the application without ever knowing about the conviction.

---

[14] See Attachment 2: "Draft—10/4/05 Initial Statement," p. 4.

Outdated IT Systems

The IT systems at USCIS are antiquated, making it difficult or impossible even to share information from one district office to another. One IT professional at the agency told me recently that USCIS IT systems "could have been designed by a high school kid."

Director Gonzalez was asked during his October 18, 2005, confirmation hearing about USCIS' ability to implement a new guest worker program. His reply was, "I know the systems that exist right now wouldn't be able to handle it." He was right. At least three reports from the DHS IG and one from the GAO in the past year alone point to the urgent need for USCIS to modernize and secure its IT systems and to move away from the current paper-based system—though not to the auto-adjudication system the Texas Service Center has been testing. After spending millions of dollars of appropriated funds to modernize the IT system, in late 2005, USCIS scrapped two years of planning, program design and implementation, and started over. In the IT security realm, despite assuring the DHS IG that IT security would be a priority and despite specific IT threat data available to senior management, the IT security budget for USCIS in FY 06 stands at only $70,000.

When I attempted to spend 1.1 million dollars of my pre-approved budget on IT security related services, software, hardware and personnel, my request was denied. Michael Aytes, head of Domestic Operations, stated "if you test our IT systems, you will find something wrong and we will have to pay to fix it." My response was "better that my office find the problem than our adversaries, don't you think?"

Susceptibility to external manipulation of biographic immigration data, destruction of biometric data, and corruption of large data files is simply a reality at USCIS. Since February 2006 multiple personnel have spoken with me on the condition of anonymity regarding the potential security threats the IT systems at USCIS present. Due to the lack of a national security perspective, USCIS has an on-going problem with the mishandling of sensitive IT systems and information. Just last week, the personnel files of every full-time employee at USCIS (some 8,500 in all) were uplinked to the DHS intranet and emailed to some 135 individual email accounts via an unsecured route because management in the USCIS Budget Office failed to train a new employee in how to handle sensitive personnel files before ordering her to work with them. The files include employee names, social security numbers, dates of birth, home addresses, salaries, grades, and positions, among other things.

In a typical reaction to such an incident being exposed, management sought to scapegoat the new hire, rather than taking responsibility for their actions. Investigators were able to determine that at least 16 individuals accessed the files on the intranet, but because of the outdated system, they cannot determine who these individuals are. This breech of privacy is not only a security policy violation it may present personal security ramifications for certain federal employees working at USCIS.

Additional systems vulnerabilities are commonplace, including the downloading and placement of TECS terrorism-related files on desktop computers accessible both via the network and the internet.

Conclusion

The Senate bill acknowledges, at least implicitly, that we do not have control of our borders, that we have no interior enforcement to speak of, that background checks on legal applicants cannot determine who is or is not a terrorist, and that fraud has reached epidemic proportions. Then it proposes that we as much as triple legal immigration levels, institute a brand new temporary worker program that is not actually temporary, and give legal status to 10 to 20 million individuals who have broken our laws.

Secretary Chertoff recognized in his testimony before the Senate last fall that "parts of the system have nearly collapsed under the weight of numbers." I would argue that our whole immigration system has already collapsed under the weight of the current numbers. As we have seen over the past five months of debate, there is consensus that the entire immigration system needs to be redesigned. It defies logic, then, to build upon a foundation that has failed us, as the Senate bill would do.

Current immigration policy is an abject failure. As a leader in the global war on terrorism, we cannot afford to continue to ignore this fact. H.R. 4437 is a good first step toward the goal of addressing national security through both border security and interior enforcement. Additionally, it aggressively targets internal corruption and fraud at USCIS. S. 2611, on the other hand, ignores national security and proposes building a whole new immigration structure on top of a collapsed foundation.

Attachment 1

Table 6
OTMs Apprehended and Released by DRO From SIC and SST
(FY 2001 thru March 31, 2005)

Fiscal Year	SIC[10] Apprehensions	SST Apprehensions	Total SIC and SST Apprehension	Total Released From SIC and SST	Percent SIC and SST Aliens Apprehended and Released
2001	9,419	6,233	15,652	7,499	48%
2002	11,962	6,574	18,536	8,807	48%
2003	24,102	8,718	32,820	19,319	59%
2004	8,078	7,717	15,795	6,099	39%
2005[11]	3,824	4,889	8,713	3,284	38%
Total	**57,385**	**34,131**	**91,516**	**45,008**	**49%**

Source: DRO

[10] Excludes OTM aliens apprehended from SIC countries that are also classified as state sponsors of terrorism (Iran, Libya, Sudan, Syria)
[11] First six months of FY 2005

From: Detention and Removal of Illegal Aliens, OIG-06-33, Office of the Inspector General, DHS, April 2006.

Attachment 2

[Note: This document was compiled through a team effort that included staff from the Chief Counsel's office, Public Affairs, Congressional Relations, and others.]

Draft – 10/4/05

Initial Statement

Recent press articles, particularly those appearing this week in the Washington Times, suggest that some U.S. Citizenship and Immigration Services (CIS) adjudicators lack access to certain law enforcement data bases when adjudicating benefit applications, and that CIS has a backlog of approximately 2500 cases involving allegations of employee misconduct.

Before providing more detailed information regarding these concerns, it is important to emphasize that CIS' highest priority is preserving and protecting the integrity of the legal immigration system. While delivering timely, accurate and effective services is critical, CIS maintains an unwavering commitment to promoting national security and public safety. Toward that end, CIS conducts law enforcement checks on all applications and petitions before adjudicating them, and completes approximately 35 million background checks each year. CIS has in effect a strict policy requiring the resolution of all law enforcement checks prior to the approval of any related immigration application. Obtaining necessary information from a range of law enforcement and intelligence agencies is vital to this effort.

CIS is also places paramount importance on employee integrity. Allegations of misconduct are investigated thoroughly and, if substantiated, addressed with appropriate disciplinary action. With regard to the number of alleged misconduct cases mentioned in recent press reports (an estimated 2600) historical experience indicates that approximately 90% are likely to be either unsubstantiated or administrative in nature. CIS has worked hard to devote additional resources to our Office of Security and Investigations (OSI) to review and resolve outstanding cases, but it will take some time to mobilize these resources and eliminate backlogged allegations. CIS is committed to completing the backlog of internal investigations fully, fairly and expeditiously.

Does CIS Have Full Access to All Necessary Law Enforcement Data Bases?

[Here we need to fashion 2-3 sentences basically saying No, we do not have FULL access and state the reasons why. We then need to emphasize how even without full access, we ensure that no application is approved without resolution of all national security and other safety concerns. IF we had more complete access – here is what it would look like (the fix) and here is how it would render far more efficient and productive our day-to-day operations…]

CIS conducts computerized law enforcement background checks related to all applications and petitions. For some application types, the agency conducts several different kinds of law enforcement checks. If the results of any given check reveal the existence of derogatory information, CIS removes the case from normal processing, and seeks clarification and/or additional guidance from whichever law enforcement agency posted the background check information. Most often, that posting agency is Immigration and Customs Enforcement (ICE), or the Federal Bureau of Investigation (FBI), though other federal, state or local agencies may also be involved. **When CIS obtains sufficient information to adjudicate a case, it does so. No case is adjudicated without sufficient information either to deny the application, or to resolve any identified security or safety concern.**

CIS at times utilizes background check processes to alert ICE about pending applications filed by, or on behalf of, aliens deemed to be national security risk. We have in place protections to ensure that adjudications do not proceed in the face of unresolved law enforcement information.

We recognize that law enforcement information can and should be obtained at various stages in the adjudications process, not just immediately after filing but also at later stages of adjudication. **To ensure that security checks are completed and resolved prior to any final adjudication, CIS conducts regular quality assurance reviews. Recently the DHS Office of the Inspector General completed an evaluation of CIS security processes that resulted in the identification of no significant lapses.**

The standard law enforcement check performed by CIS on all applications is called an Inter Agency Border Inspection System (IBIS) check. The database at the heart of IBIS is the Treasury Enforcement Communication System (TECS). Since the formation of the DHS, some transition issues have arisen involving access by CIS adjudicators to TECS. These issues are predicated upon a very legitimate debate about the level of employee background checks that should be conducted prior to qualifying for TECS access. Negotiations about this issue are ongoing, with the Fraud Detection and National Security (FDNS) Unit representing CIS.

Related questions exist concerning the specific level of access to TECS information CIS adjudicators and FDNS staff should be given. *[Here we should describe each level and what it implies – Alice and/or Nick can you help?]* These implicate the law enforcement "need to know" requirement, and the level of personnel security clearances of employees seeking access. FDNS is likewise responsible for representing CIS in these negotiations.

With respect to the FBI's NCICIII database, CIS is encountering direct access difficulties, though not with regard to fingerprint checks *[add a sentence explaining why]*. Access issues do arise when we want to submit a name rather than fingerprint check. The CIS Office of the Chief Counsel has made numerous attempts to obtain fuller access to NCICIII for agency personnel.

[Here we need to explain in clear terms how Section 403 of the Patriot Act did not clearly provide for the use of FBI criminal history information in adjudications involving aliens already in and admitted to the U.S. We should further emphasize our support of an amendment to Section 104 of the Immigration and Nationality Act that would ensure that those charged with determining whether aliens will have temporary or permanent access to the U.S. through a grant of a visa, immigration benefit, or citizenship, are equipped with the same informational tools as law enforcement agencies, as their function is no less important in the war on terrorism. The FBI has provided direct access to NCICIII (via IBIS) to immigration inspectors at ports of entry for purposes of ensuring that aliens who seek to enter the U.S. are admissible (i.e. an immigration purpose or benefit), yet is has resisted providing that same access to CIS personnel adjudicating immigration benefit applications in the U.S. Attached is a comprehensive summary of both the access to criminal history information problem CIS confronts and the proposed remedial amendment.]

How Does CIS Identify Fraud and Potential Threats to National Security?

To strengthen national security and ensure the integrity of the legal immigration system while simultaneously administering immigration benefits in a timely and effective manner, CIS established a Fraud Detection and National Security (FDNS) Unit whose primary responsibilities are to:

- Detect, pursue, and deter immigration benefit fraud,
- Ensure background checks are conducted on all persons seeking benefits before benefits are granted,
- Identify systemic vulnerabilities and other weaknesses that compromise the integrity of the legal immigration system, and
- Perform as USCIS' primary conduit to/from law enforcement and intelligence agencies.

The headquarters (HQ)-based FDNS consists of four branches: 1) Fraud Detection, 2) Operations, 3) National Security, and 4) Administration/Support Services. A Background Check Analysis Unit (HQ-BCAU) within the National Security Branch receives and reviews all National Security Notifications (NSNs) resulting from IBIS hits. These NSNs, and the subsequent case resolution information in the form of a Case Resolution Record (CRR) are reviewed by the HQ-BCAU. All CRRs must be approved by the HQ-BCAU before a case may be released for adjudication. Sensitive national security-related cases are forward to the CIS Office of Field Operations' FOCUS [spell out] Unit, which provides adjudications-related advice and guidance. HQ BCAU's primary responsibilities include performing system checks and gathering information.

FDNS staff is also assigned to each of the five CIS Production or Service Centers and operate in the form of Fraud Detection Units (FDUs). Each FDU is engaged in anti-fraud activities and "Top 5" IBIS background check operations: all IBIS hits that involve 1) National Security, 2) Public Safety, 3) Wants/Warrants, 4) Interpol, or 5) Absconders are forwarded to FDUs from Production Center IBIS Triage Units. The FDUs performs referral and/or resolution activities, and return information to adjudicators. Production Center IBIS Triage Units resolve non-"Top 5" IBIS hits.

Many CIS District Offices have an on-site local FDNS Immigration Officer (IO) to assist in anti-fraud efforts and IBIS National Security-related hit resolutions. These IOs are organized across the three CIS Regions, and guided by Regional FDNS Supervisors. Local IBIS units under CIS Field Service Operations are responsible for resolving non-National Security-related IBIS hits.

CIS conducts approximately 35 million IBIS checks each year. FDNS is responsible for processing all "TOP 5" IBIS hits through Production Center staff and National Security IBIS hits through District IOs.

As of September 24, 2005, the pending IBIS FDU workload consisted of 13,815 cases, including all National Security cases. Roughly 90% of the National Security IBIS workload is carried by the FDUs. The number of public safety cases referred from all Regions, including the Asylum Division and Production Centers totaled 11,997 for the ten-month period from September 2004 through June 2005.

[NOTE: The current IBIS backlog for the Center Triage units, which resolves other than "Top 5" hits, is approximately 26,000 cases]

In March 2005, CIS began requiring all of its offices to report National Security-related hits to the HQ-BCAU before commencing resolution activity. Since April 2005, an estimated 2000 NSNs have been submitted to the HQ-BCAU. Over this same six-month period, approximately 650 final resolutions were completed by FDNS staff and approved by the HQ-BCAU for release to adjudications or referral to FOCUS. Presently roughly 1350 resolutions are pending completion.

[Here we need to add a paragraph explaining how FDNS interfaces with OSI to identify fraud and potential threats to national security. Ideally this would include numbers of cases sent from OSI to FDNS and the course of such referrals. Point is that we are trying in a variety of ways to identify, isolate and resolve instances of fraud and national security risks.]

How Effectively Do CIS and ICE Share Law Enforcement and intelligence Information?

Presently CIS is seeking access to ICE's TECS Case Management System that includes information on past and present investigations and targets to compliment and reinforce our anti-fraud program. [Tom P. prefers that we try to present as united a front as possible vis a vis other DHS components as opposed to appearing in conflict with them] Obtaining details regarding watch-listed persons is part of a larger information sharing issue confronting various DHS components, the FBI, and other agencies upon whom CIS relies for background check protocol information. However, CIS typically encounters little difficulty isolating through watch lists and FBI name checks individual national security concerns *[why?]*. CIS also routinely shares information with other intelligence and investigative agencies, including ICE.

Is it True that up to 1300 CIS Adjudicators Have Been Shut out of TECS?

In January 2005, Customs and Border Protection (CBP) placed approximately 1300 of CIS' 8,642 employees into a "restricted profile." In general, these individuals either never had access to TECS, or had let such access lapse. Since then, CBP has moved virtually all of these individuals out of a restricted profile and designated them with Level 2 or 3 access depending on their background investigation level. Level 2 access pertains to all CIS-posted information as well as information any other posting agencies have relegated to Level 2. Level 3 access pertains to all CIS look outs as well as look outs established by other agencies. Other individuals who have since January 2005 lapsed into archive status may currently be in the restricted profile category. Administrative control over CIS users remains an open issue with CBP for all persons placed in the restricted profile. FDNS is currently negotiating with ICE and CBP regarding CIS access levels and associated background investigations, which is the greater agency issue as regards TECS.

What Is CIS FOCUS and What Does it Aim to Achieve?

FOCUS *[not an acronym so no longer translation]* is a group of seasoned adjudicators in the Office of Field Service Operations that was established to provide special attention and technical expertise in cases involving national security or public safety concerns. Until now the group has consisted largely of field adjudicators detailed from positions in the field, although permanent positions for FOCUS have been advertised and are in the process of being filled. While FOCUS adjudicators have the authority to decide cases directly, their strong preference is to provide field adjudicators with resources, information and advice to perform their duties in the best possible way.

Because FOCUS cases derive from the field, there is no set number or limit of FOCUS cases. This year FOCUS began its work by assisting the CIS Office of Chief Counsel with regard to the over 100 pending mandamus cases filed in federal court that implicate national security or significant public safety issues. FOCUS does not intend to limit its work, however, to helping resolve mandamus cases.

What Is the CIS Office of Special Investigations and How Many Potential Misconduct Cases Does it Have?

The CIS Office of Security & Investigations (OSI) was established in May 2004 to protect and promote agency-wide physical security standards and to prevent, detect and investigate allegations of CIS employee misconduct. Presently OSI employs six investigators, four of whom are assigned criminal cases, the remaining two investigators are in the process of developing OSI's infrastructure, policies and procedures. The four agents are actively investigating 8 cases, deemed priority cases, and have closed two cases administratively. OSI has received funding for, and will hire, six additional staff to serve as 1811 Criminal Investigators within 30 days.

Between October 2004 and September 2005, OSI received and reviewed approximately 1500 complaints that had been pending with the former Immigration and Naturalization Service (INS) and Immigrations and Customs Enforcement. Over that same period OSI has received an additional 1100 cases from a variety of sources including the DHS Office of Inspector General, the US State Department, the Drug Enforcement Administration. Although the OSI presently lacks a database to track and/or inventory all allegations, its Director estimates that about 500 of the total 2700 in-house complaints involve alleged criminal conduct.

Historically, What Was the Role of the INS Office of Internal Audit and Does It Differ from CIS OSI?

The Internal Investigations Branch, within Legacy INS Office of Internal Audit, managed the processes by which allegations of Service employee misconduct were reported, resolved and acted upon. It also conducted and oversaw the conduct of investigations and inquiries. The workload received within the Investigations Branch is attached, with a breakdown of how each allegation was handled.

An explanation of the categories to include an **8-year average (1995 – 2002)**[1] is as follows:

- ✓ Investigated by the DOJ OIG – Generally criminal in nature or the allegation was against a GS-15 or above. Note that OIA did not have the authority to conduct criminal investigations. **8.9%**
- ✓ Investigated by other, which was usually the DOJ Civil Rights Division. Such investigations involved abuse. **.5%**
- ✓ Investigated by the OIA – Administrative investigation involving a serious allegation of misconduct. Many times the OIG would try to get a US Attorney to take the case, but when this would not happen, the matter was referred to the OIA for investigation. **11.1%**
- ✓ Management Inquiry by field – These involved less serious matters that could be reviewed by the field management. **39.8%**
- ✓ Referral to management as information – Something management should be aware of but not enough information within the allegation on which to investigate or look into. **29.5%**
- ✓ File no/action. **4.7%**
- ✓ Other. **5.4%**

Although information was available in the OIA case management system as to what occupation codes were subjects of misconduct allegations, that information is currently not available. However, during the months after the creation of DHS, analysis had been done as to the percentage of allegations that related to adjudication and asylum officers, and the results showed between 10-15%.

The type of allegations reported in the OIA annual reports is attached.

Without a database to inventory the allegations received by CIS OSI, it is difficult to compare the work of this new internal investigations division with that performed by legacy INS OIA. Clearly, however, with regard to OSI allegations related to administrative or criminal misconduct, most appear related to what the legacy INS OIA would have also categorized as misconduct with the exception of an unknown number of customer service complaints received by the OSI concerning the time it takes to adjudicate immigration benefit applications. OSI does not yet track the latter type of correspondence.

Although approximately 50 CIS employees have been trained to investigate management inquiries, almost 40% of the legacy INS OIA caseload, this process has not been implemented by OSI because it lacks a database to track the allegations through resolution, a major point of concern for USCIS field leadership who stated the legacy process was "lacking and inefficient".

Of the Reported 50 Allegations Received Each Week by the OSI, Are These New Cases or Cases Filed in the Past That Are Only Now Being Forwarded to OSI from Other DHS Components? Has the DHS IG Reviewed and Referred Each of the 50 Cases to the OSI?

- Allegations referred to OSI by the DHS OIG are primarily new although a small number represent repeat allegations against one or more persons. As mentioned previously, OSI does receive allegations directly from ICE, CBP, US State Department and others. These allegations received directly by OSI must be sent to the DHS OIG for review. The OIG may accept the case, choose to investigate the case jointly with OSI, or refer the case back to OSI who will investigate the case unilaterally. Per an MOU with OIG, the OIG shall determine within one business day of the OSI referral whether to investigate the allegation or refer it back to CIS.

Attachments:

Overview of history of agency's request to receive legislative authority to access NCIC III.

Categories of Allegations within Legacy INS OIA

Attachment 1

Access to Criminal History Information. Section 403 of the USA PATRIOT Act amended section 105 of the Immigration and Nationality Act to provide for the use of FBI criminal history information for the purpose of determining admissibility to the United States in the visa or inspections context. However, after two years of work implementing section 403, DHS and DOS have found that this section needs several improvements. These amendments have been coordinated between DHS and DOS to meet the goals of both Departments.

[1] The total number of allegations for this 8 year period was 28,722.

In the case of DHS, section 403 did not clearly provide for the use of this important information in adjudications involving aliens already admitted to the United States. These benefit adjudications within the United States may be equally important to protecting the country from terrorism. For example, several of the September 11 hijackers applied to change their nonimmigrant status. This amendment clarifies that criminal history information shall be provided for use in immigration adjudication cases on the same terms as for visas and initial admission to the United States. Relatedly, it provides that immigration adjudications shall be considered a law enforcement purpose in order to ensure full access to FBI criminal history information.

In the case of DOS, the Department has received extracts from the FBI that contain only biographical information, but do not include information pertaining to the criminal offense or disposition. The information pertaining to the criminal offense or disposition is essential for the consular officer to access for determining the alien's eligibility for a visa and admissibility to the United States. The FBI contends that the National Crime Prevention and Privacy Compact, a statutory authority, prevents it from providing information on the extract pertaining to the crime or disposition without a fingerprint match (for positive identification). The FBI maintains that positive identification is required because consular officers are not law enforcement officials or serving a law enforcement purpose. The proposed amendments to the INA frame the consular visa adjudication function as serving a criminal justice purpose and grant consular officials direct access to NCIC records. Direct access would facilitate a more effective and efficient screening of legitimate travelers and travelers who are persons of interest.

Department of State personnel who adjudicate visas abroad act as the nation's first line of defense against terrorists and criminals who seek to enter the United States. Since the events of September 11, 2001, legislation has mandated interagency datashare. In light of the level of information shared and the coordination and cooperation with law enforcement and intelligence agencies in identifying persons of interest, the Department of State consular officer serves a criminal justice purpose and should be granted direct access to criminal history record information. This access would enhance the efficiency with which a consular officer is able to identify legitimate travelers from persons who may pose a threat if admitted to the U.S. Without direct access, consular officers must submit an applicant's fingerprints to the FBI causing significant delays and attendant adverse economic impact. The majority of submitted prints are returned as "no match" or the crime does not have impact on the individual's eligibility for a visa. The current procedures impose significant costs on the operational efficiency of consular sections. Direct consular access to the NCIC system is necessary for consular officers to meet the national security mandates imposed after 9/11. The statutory language suggested used the term Department of State personnel rather than consular officers as Visa or Passport personnel may be involved in rendering advisory opinions in visa cases or the decision to issue a passport.

Proposed Language:

(a) Section 104 of the Immigration and Nationality Act, 8 U.S.C. 1104, is amended by adding a new subsection (f) reading—

'(f) Notwithstanding any other provision of law, the powers, duties and functions conferred upon Department of State personnel relating to the granting or refusal of visas or passports may include activities that serve a criminal justice purpose.'

(b) Section 105 of the Immigration and Nationality Act, 8 U.S.C. 1105, is amended by-

(1) Amending paragraph (b)(1) to read—

'(b)(1) Notwithstanding any other provision of law, the Attorney General and the Director of the Federal Bureau of Investigation shall provide to the Department of Homeland Security and the Department of State access to the criminal history record information contained in the National Crime Information Center's Interstate Identification Index (NCIC-III), Wanted Persons File, and to any other files maintained by the National Crime Information Center, for the purpose of determining whether an applicant or petitioner for a visa, admission, or any benefit, relief or status under the immigration laws, or any beneficiary of an application or petition under the immigration laws, has a criminal history record indexed in any such file.';

(2) Amending paragraph (b)(2) to read—

'(b)(2) The Secretary of Homeland Security and Secretary of State shall have direct access, without any fee or charge, to the information described in paragraph (1) of this subsection to conduct name-based searches, file number searches and any other searches that any criminal justice or other law enforcement officials are entitled to conduct, and may contribute to the records maintained in the NCIC system. The Secretary of Homeland Security shall also receive, upon his request, access to such information by means of extracts of the records for placement in the appropriate database without any fee or charge.';

(c) Striking paragraphs (b)(3) and (b)(4); and

(d) Amending paragraph (c) to read –

‘(c) Notwithstanding any other law, adjudication of eligibility for benefits under the immigration laws, and other purposes relating to citizenship and immigration services, shall be considered to be criminal justice or law enforcement purposes with respect to access to or use of any information maintained by the National Crime Information Center or other criminal history information or records.’

FBI Objection:

The Department of Justice strongly opposes section 502 of the State Department s draft Authorization bill. That draft section seeks to eliminate certain provisions of Section 403 of the PATRIOT Act concerning the means of access by the Department of State and the INS (now DHS) to criminal history records maintained in the FBI s National Crime Information Center s Interstate Identification Index (NCIC-III) for purposes of determining whether a visa applicant or applicant for admission has a criminal history record in the III. Section 502 seeks to provide direct, unrestricted name-check access to the fingerprint-based criminal history records in the III to State and DHS *without* any requirement for fingerprints, and *without* a fee, for the purpose of granting a broad array of benefits to both aliens seeking entry in the United States and aliens already present in the United States. The proposal seeks to avoid the fingerprint requirement imposed by the National Crime Prevention and Privacy Compact for non-criminal justice criminal history background checks of the III by defining immigration and visa decisions as having a criminal justice purpose. By avoiding any fee for these checks, this proposal also places the cost of these incomplete name checks squarely on American taxpayers.

The Department of Justice opposes this proposal and believes that the issues it raises should be resolved through the interagency process because of all the Departmental equities involved. A legislative change of this nature should not go forward absent an interagency consensus.

The Department of Justice does not concur in this proposal for the following reasons:

(1) Using Names Instead of Positive, Biometric Identification: This change is being proposed when there are still significant outstanding issues the Administration is trying to resolve about the implementation by the Department of Justice, the State Department, and DHS of the other, related provisions of section 403 of the PATRIOT Act regarding establishing and adopting a biometric technology standard and a fully integrated system that can be used to confirm the identity of persons applying for a United States visa or such persons seeking to enter the United States pursuant to a visa. There is general agreement by all Departments involved that a check of criminal history records is essential to processing applications for visa and immigration benefits. The Department of Justice, however, has, from the outset, argued that a fingerprint-based check for these purposes is both feasible and the most effective and reliable way to determine whether a relevant record exists on an applicant for a visa or a change in immigration status. While DHS and State have argued that full criminal history checks using fingerprints are too hard, take too long, and are too expensive, the security argument should trump these operational hardship arguments, especially since the operational hardship is a temporary condition under the control of DOS, DHS, and DOJ policymakers. Had a solution for the Congressional-tasking for biometric interoperability under section 403 been agreed upon by now, there would be no need to seek to broaden section 403's authority to do name-checks using extracts.

The FBI has pressed forward on this issue, but absent any DHS cooperation or requirements to drive funding for system modifications/ upgrades, the FBI can only make so much progress.

Currently, the FBI CJIS Division is running 5 ongoing pilots with Consular posts in Mexico and El Salvador and may be expanding to the UK shortly. The FBI's new flat transaction will make collection easier and less expensive and should be in place this Spring. In addition, the Homeland Security Counsel is currently working to produce the first cost estimates for 10-flat print checks at time of visa enrollment that are based on actual DHS-supplied transaction volume data. The statement in the sectional analysis of section 502 that the cost is not worth the benefit should not be accepted without considering this additional information now being developed. Given all of this, it is, at best, premature to consider negating the requirement for positive identification, particularly through a legislative mandate, by giving unrestricted, direct name-check access to III to State and DHS for these purposes.

(2) The inherent unreliability of name checks. The proposal ignores the steps that are needed to be taken in order to secure our borders. The focus should not be on expanding the name-based background check capabilities of State and DHS, but rather on moving those agencies, as quickly as possible, to a fingerprint-based background check system. Name checks are not reliable and present problems of both security gaps from false negatives and unfairness to applicants from false positives. A draft 15-month study by State and the FBI under Section 403(b) doesn't support decision-making without positive identification. In fact, the data shows that without positive identification:

- False Negative Problem - After a negative name check, the Consular Officer has no way of knowing whether the applicant who clears the name check is known in the criminal files under a different name. In these cases, an applicant might be issued a US Visa good for up to 10 years. This situation poses highest risk in countries that use different alphabets or highly variable spellings of the same name.

- False Positive Problem - After a positive name check, the consular officer will have no way of knowing that the returned criminal history information associates to the applicant. The draft PATRIOT Act 403(b) study showed that False Positives occurred 2 out of 3 times over a 15 month study period. In these cases, an applicant might be denied a US visa based on irrelevant information

In addition, the 1999 DOJ Name Check Efficacy Study showed that 11.7 percent of applicants with criminal history records in the study were not discovered by name checks. Moreover, the fact that the great majority of fingerprint-based background checks come back with a no record response is true of all applicant checks. That is not a reason to excuse the use of fingerprints for aliens seeking admission to or immigration benefits from the U.S., any more than it is to excuse fingerprints that are required of U.S. citizens in the many employment and licensing contexts involving background checks for criminal history using III information.

(3) Eliminating the Requirement for Follow-up Fingerprints. Under the interim extract approach, there is a requirement that fingerprints be submitted whenever there is a hit by a name check in order to get the full criminal history record. This requirement is totally missing in this proposal. Given the fact that applicants can wait for a decision on the visa or immigration benefits while fingerprints are run when there is a hit on a name, there is no reason to totally dispense with the followup fingerprint requirement during the interim name-check regiment under Section 403 of the PATRIOT Act, even if a way can be found of providing State and DHS with the ability to check names against the full III database, instead of the extract database (which is a subset of III). Moreover, as noted above, the proposal still ignores the fact that fingerprints are only submitted when the alien's name matches a name with a criminal history record. As a result, an alien with a hard to detect false ID would be able to receive a visa even though he or she may have criminal history record information under another name.

(4) Apparent Inconsistency with the National Crime Prevention and Privacy Compact. The proposal s attempt to redefine the processing of applications for visas or immigration benefits as including a criminal justice purpose creates an apparent contradiction or inconsistency with the terms of the National Crime Prevention and Privacy Compact which requires that checks of the III for non-criminal justice purposes be supported by fingerprints. The Compact was enacted by Congress and has been adopted by 22 states. It could undermine the integrity of the Compact to enact legislation declaring an activity to have a criminal justice purpose simply because Congress says it does, regardless of whether the declaration is consistent with how that language is used in the Compact and has been applied in practice. The Compact s fingerprint requirement was enacted for the same policy reasons discussed above regarding the unreliability of name-checks and the importance of using positive identification when a person is applying for benefits from the government where the security and protection of the public is at stake.

(5) No Consideration of the Budgetary Impact. This proposal fails to consider the budgetary impact of allowing DHS and State to have unrestricted administrative name-check use of and access to III criminal history records in processing alien applications for visas or for admission or adjustment of immigration status. U.S. civil applicants for employment or licensing or for positions of trust are required to submit fingerprints and pay a fee when a criminal history check of the III is required and authorized by law. Applicant fees typically include a surcharge that is used to support the operation the national fingerprint-based criminal history record system. If visa or immigration benefits can be processed without submitting fingerprints and a fee, not only will those benefits be granted without the greater security and accuracy of positive identification, the funds from the fingerprint fees will no longer be available to support the CJIS Division s record system. The lost funds will have to be made up through appropriations and perhaps otherwise subsidized through an increase in the surcharge in the applicant fees paid by U.S. citizens. There will also be a significant budgetary impact on the FBI CJIS Division that must be considered approximately 20 percent of the non-criminal justice fingerprint submissions are from DHS and State and their elimination definitely affect CJIS s West Virginia workforce.

(6) Access to Non-fingerprint Based NCIC Records Does Not Require this Change: The proposal s reference to access to name-based files in the NCIC, such as the wanted persons file, does not require this legislation. If desired, arrangements for access by State and DHS to such records can be made outside of the extract process under existing law.

Summary: In sum, whenever name-based searches are conducted utilizing the III for immigration and visa matters, such searches should be immediately followed up by the submission of fingerprints when a match occurs. More importantly, *all* aliens seeking a visa or an immigration benefit should have fingerprints taken of all ten fingers and have those fingerprints run against the III -- not just those aliens whose names happen to match. Aliens seeking these benefits should be required to bear the cost of processing the prints for the background check. These requirements are critical to ensure that immigration and visa decisions are based on accurate information. In addition, the collection of fingerprints would "freeze" an alien's identification -- preventing the alien from trying to use a different name at a later time. The collection of 10-fingerprints also would allow for the fingerprint's to be run against the FBI's latent fingerprint file. That file contains latent fingerprints taken from crime scenes and other locations of interest, such as scenes of terrorist activities.

USCIS Response to FBI Objection:

Since 9/11 (if not before) Congress has repeatedly emphasized and mandated the breaking down of artificial barriers to the sharing of relevant information between agencies. E.g, USA PATRIOT Act and Enhanced Border Security Act. At the highest levels, the Department of Justice (DOJ) has promoted this goal as well. See, e.g., Testimony of FBI Director Mueller before Senate Select Committee on Intelligence, Feb. 16, 2005 at 19 ("The FBI's Information Sharing Policy Group . . . brings together the FBI entities that generate and disseminate law enforcement information and intelligence to implement the FBI's goal of sharing as much as possible consistent with security and privacy protections."). DOJ's objections to this proposal are entirely inconsistent with this overarching Administration, DOJ and Congressional policy, and perpetuate the roadblocks to information sharing that prevent government agencies from communicating effectively with one another to prevent terrorism.

What this proposal seeks to do, in short, is no more than to ensure that those charged with the critical function of determining whether aliens will have temporary or permanent access to the United States through a grant of a visa, immigration benefit, or citizenship, are equipped with the same informational tools as law enforcement agencies, as their function is no less important in the war on terrorism. The FBI has provided direct access to NCIC III (via IBIS) to immigration inspectors at ports for purposes of ensuring that aliens who seek to enter the U.S. (i.e. an immigration purpose and benefit) are admissible, yet it has resisted providing that same access to USCIS personnel providing immigration benefits within the United States. This distinction is capricious, since the inspection and adjudication function are analogous to each other and of equal potential importance in fighting terrorism. DHS seeks to ensure the same type of direct access to determine whether aliens who file applications that can lead to their obtaining travel and entry documents (and work authorization) are also admissible, and if they are in the U.S., that they are not deportable due to disqualifying criminal records. DOS seeks the same direct NCIC III access in order to make determinations on aliens seeking visas to enter this country. The rationale for permitting direct access to immigration inspectors who have responsibility for approving an alien for the immigration benefit of admission to the U.S. applies equally to DHS adjudicators and DOS consular officers who have responsibility for approving aliens for the immigration benefits and documents that allow them to enter (and remain in) the U.S.

DHS does take and submit ten fingerprints to the FBI for criminal history checks on aliens seeking many forms of immigration benefits (e.g. naturalization, adjustment to permanent residency, asylum, temporary protected status, among others). DHS is also expanding the categories of applicants and petitioners for immigration benefits and documents who will be required to submit full sets of fingerprints as rapidly as resources and available technology permit. However, direct access to NCIC III would greatly facilitate DHS' ability to identify, via name checks, those individuals who have a disqualifying criminal history record, but who might otherwise be missed while routine ten printing is being expanded. Direct name access to NCIC III will also assist DHS in identifying those individuals who may have positive "hits" that require further verification of the alien's identity through fingerprint submission. At the moment, criminal history "hits" are often received on aliens in the NCIC "wants and warrants" files and other NCIC files to which the FBI currently does permit DHS direct access, but the information is not necessarily disqualifying for the particular immigration benefit (e.g. certain misdemeanors). With direct NCIC III access, DHS could "triage" its benefit cases and focus enforcement efforts on those cases where the "hit" was of a type likely to disqualify the person for the application or petition at issue. If it received such a "hit" via a name check of NCIC III, DHS or DOS could follow up by requesting fingerprints of the individual for further verification of identity so as not to deny a benefit to the wrong individual. Finally, direct access to NCIC III would assist DHS adjudicators in determining what may have happened in terms of conviction, acquittal or other follow-up activity in the case of an individual for whom DHS has received a "hit", or an FBI name check "hit" from the FBI's investigative records for which the FBI does not require DHS to submit fingerprints.

No one would dispute that fully fingerprint-based checks are more reliable to determine identity than name checks, but DOJ's position that name-check access should not be provided at all because print-based checks for all should be done is, essentially, rejecting a substantial improvement because it does not result in perfection. Indeed, the same argument suggests that law enforcement use of NCIC information without full prints is equally flawed, yet law enforcement agencies, in matters where liberty is at stake, are authorized to use the system. Furthermore DOJ's position that name checks are "not reliable" is contradicted by its own stated position to Congress; in a draft letter to Chairman Sensenbrenner circulated interagency in early March, DOJ took the position that a match between a visa applicant's identifying information (e.g., name, date of birth, place of birth, country of citizenship) and a record in the terrorist watchlist by itself provides reasonable ground to believe that the alien is inadmissible, and thus that the visa must be denied. How can DOJ take this position on the one hand, while on the other argue that the Department of State should not be permitted to do name-checks of criminal history information for the purpose of determining visa eligibility because of their "inherent unreliability"?

DOJ's opposition cites budget concerns. In essence the DOJ argument is this: DHS should be required to submit fingerprints rather than have name-check access, so that the FBI can continue to collect fees to pay the salaries of the people who look at the fingerprints. We do not believe that this argument is a credible reason not to share information, and it is thoroughly inconsistent with the repeated public statements of DOJ and the FBI that their goal is to remove barriers to interagency information-sharing.

Attachment 3

The Washington Times
www.washingtontimes.com

Iraq spy suspect oversaw U.S. asylum

By Stephen Dinan

THE WASHINGTON TIMES

Published April 6, 2006

An Iraqi-born U.S. citizen suspected of being a foreign intelligence agent was employed by U.S. Citizenship and Immigration Services to rule on asylum applications, including those from unfriendly Middle Eastern nations, according to documents obtained from Congress by The Washington Times.

Michael J. Maxwell, the former head of the Office of Security and Investigations at USCIS, is expected to testify about the Iraqi case and other breakdowns at the agency to a House subcommittee today.

Mr. Maxwell will tell legislators that the immigration system is being used by enemy governments to place agents in the United States.

The suspected agent, whose name has not been released, judged 180 asylum applications while at USCIS, the agency that also rules on green cards, citizenship and employment authorization.

A database check during Mr. Maxwell's investigation turned up national-security questions about nearly two dozen of those cases.

Mr. Maxwell will also tell the panel about criminal accusations pending against USCIS workers and that top USCIS officials have deceived Congress and obstructed the duties of his office, the agency's internal affairs division.

"The immigration system as a whole is so broken that our adversaries can game it," Mr. Maxwell told The Times when asked about the documents this week. "I can assure you they're using it against us; they can with impunity."

His testimony comes as the Senate debates whether to enact a guest-worker program that would allow current illegal aliens and future foreign workers a new path to citizenship.

An opponent of a guest-worker program, Rep. Ed Royce, chairman of the House International Relations subcommittee on terrorism and nonproliferation, which is holding the hearing, said USCIS is "deeply flawed" and focuses too much on processing applications and not enough on security, according to his prepared statement.

The House immigration-enforcement bill passed in December included an amendment by Mr. Royce, California Republican, that puts law enforcement at the top of USCIS' priorities.

Emilio Gonzalez, the agency's new director, told reporters last month that he has made national security the top priority.

"The minute I walked through these doors here, I let it be known -- under my watch, it's all about security," he said.

Mr. Gonzalez said the lack of access to databases for some adjudicators -- another subject Mr. Maxwell is expected to testify about -- hasn't hurt the agency because other agencies can do those checks and share information.

USCIS officials said they will wait to see Mr. Maxwell's testimony to respond specifically, but Angelica Alfonso-Royals, a USCIS spokeswoman, said, "We take any allegations of potential misconduct seriously and are investigating them fully."

Mr. Maxwell now works as an independent consultant on security matters, and a client is Numbers USA, which lobbies for stricter immigration controls and against a guest-worker program. He said this week that the Iraq case was not an isolated case.

"We know the asylum process is in shambles. We know fraud is rampant," he said, adding that documents show top officials know this and refuse to do anything about it.

In the case of the suspected agent, whose name was blacked out in the documents The Times obtained, Mr. Maxwell said there were many red flags.

"There are indicators throughout this entire case that I saw, professionals within the FBI and the intelligence community saw, that all pointed one way -- we were dealing with an individual who was a member of a foreign intelligence agency that had been working within CIS," Mr. Maxwell said.

"The danger was that he was granting asylum to anybody that he wanted to, with impunity, at a time of his choosing. Who was he letting into this country?"

The man was in demand at USCIS because of his language skills. He was able to do interviews without the need for a translator. At the time, that seemed to be a big benefit to the speed of the process, but in retrospect, Mr. Maxwell said, it posed a security risk.

Mr. Maxwell said they first became suspicious of the man when, while on a yearlong assignment to the Defense Department in Iraq, he walked outside the Green Zone in Baghdad and disappeared. According to documents, authorities first thought he had been taken hostage but concluded he had left of his own accord.

Mr. Maxwell began an investigation that found that the man had been hired by USCIS even though negative "national security information" in his background check caused other federal agencies to pass on him.

A national security polygraph showed repeated deception on his part, and in interviews with Mr. Maxwell, he denied having traveled to Iran, Syria and Jordan while he worked for USCIS, even though electronic databases showed he had made the trips.

The man also made "persistent requests" that Mr. Maxwell help him achieve secret or top-secret clearance so he could go back to work for the Defense Department. Mr. Maxwell said that request was weird because Defense would have had to do its own background check anyway.

The man has since left USCIS and the United States so Mr. Maxwell closed his investigation. But Mr. Maxwell said that despite his findings, USCIS doesn't even have the ability to go back and see whether any of the 180 cases the former employee approved should be revoked.

"With no internal audit function at CIS, we don't know who we let into this country," Mr. Maxwell said.

Attachment 4

National Benefits Center Adjudication Process Review

OFFICE OF THE CHIEF INFORMATION OFFICER
UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES

March 23, 2006

DEPARTMENT OF HOMELAND SECURITY

Summary

USCIS OCIO contract personnel (Total Systems Technologies Corporation, TSTC) were tasked with investigating allegations that an auto-adjudicate function was being used at the National Benefits Center which allowed processing of I-485 (Adjustment of Status) applications without appropriate adjudicator review.

Based upon the initial review, consisting of documentation reviews, interviews and an initial review of CLAIMS 3 soft data, it does not appear that there is any means for "auto adjudication" to take place with I-485 applications being processed at the National Benefits Center. These interviews included discussions with Information Technology staff, Director of Adjudication, Director of the Fraud Detection Unit, and the Director of Records. There does appear, however that there is a little – known manual data entry process that provides the ability to insert a benefits application into the CLAIMS3 database without using the established lockbox or e-File input methods.

Findings

According to IT Department personnel, an unknown number of benefits applications are processed manually at the National Benefits Center. After a full review of the C3 Database a final number of manually processed applications will be known. The National Benefits Center has only one person with access privileges to manually enter these benefits applications and OCIO Security could not assess the number of applications processed in the fashion. OCIO Security will ascertain the validity of this statement once the C3 Database has be fully reviewed. The IT staff could conceivably make direct changes to the Claims 3 database. The Director of Adjudication was not aware of any method of accepting application other than the Lock Box submissions from Los Angeles and Chicago.

Once the benefits application information is entered (either manually, by the aforementioned person with access privileges, or electronically via the Lock Box function) it is uploaded to C3 and this initiates the Interagency Border Inspection System (IBIS) screening of the applicant. IBIS is a Mainframe application owned by the Department of Treasury and it provides access to the FBI's National Crime Information Center (NCIC) and allows its users to interface with all fifty states via the National Law Enforcement Telecommunications Systems (NLETS) for the purpose of reviewing records of wanted persons and/or criminal histories.

All applications receive an IBIS check within the first ten/fifteen days of arrival at the National Benefits Center and if a benefits application is idle for more than 90 days an additional IBIS check is run. The current I-485 process requires a great deal of manual interaction using 2 computer applications (a GUI based application and a text based application) running on NBC workstations. The I-765 and I-90 are often filed at the same time as the I-485. In the event they are not filed at the same time, they must be linked to a current I-485 before they are processed. The adjudication of the I-485 includes IBIS checks, biometrics capture for FBI finger print check, FBI name checks, and a personal

interview. While using the 2 adjudication applications, all adjudicator's actions inputs or changes to records are logged in a database and can be audited.

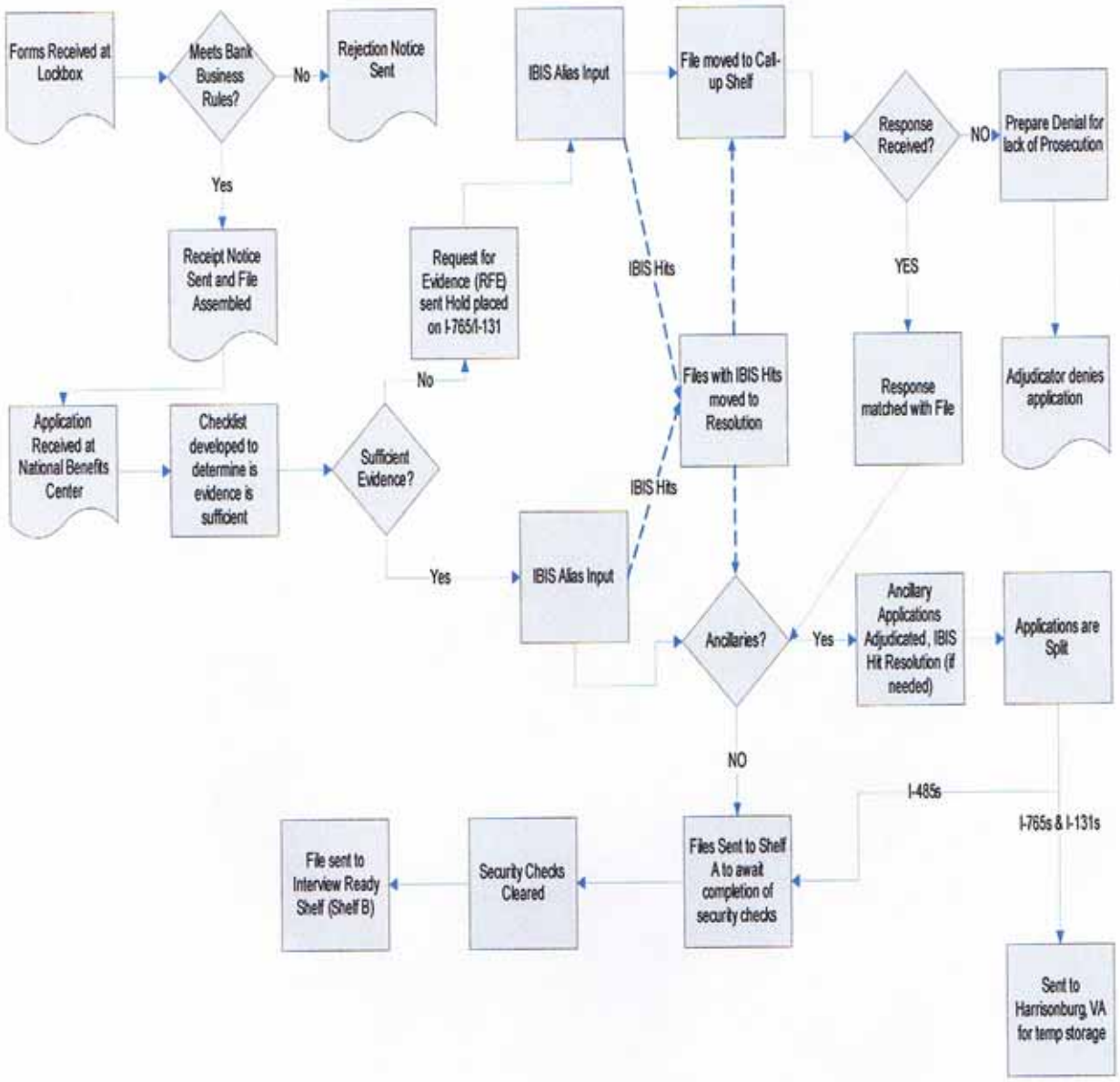
The one item that can be generated without the involvement of an adjudicator is the I-765. This is due to the fact that 8 CFR §274a.13 states the following:

> *The district director shall adjudicate the application within 90 days from the date of receipt of the application by the INS, except in the case of an initial application for employment authorization under § 274a.12(c)(8), which is governed by paragraph (a)(2) of this section, and § 274a.12(c)(9) in so far as it is governed by § § 245.13(j) and 245.15(n) of this chapter. Failure to complete the adjudication within 90 days will result in the grant of an employment authorization document for a period not to exceed 240 days. Such authorization shall be subject to any conditions noted on the employment authorization document. However, if the director adjudicates the application prior to the expiration date of the interim employment authorization and denies the individual's employment authorization application, the interim employment authorization granted under this section shall automatically terminate as of the date of the director's adjudication and denial. (Amended 7/1/94; 59 FR 33903) (Amended 1/4/95; 59 FR 62284) (Amended effective 6/22/98; 63 FR 27823) (Corrected 7/21/98; 63 FR 39121) (Amended effective 6/11/99; 64 FR 25756) (Amended 3/24/00; 65 FR 15835).*

IT staff identified an application I-765 SQA that was developed by the Texas Service Center (TSC), it is currently being tested and has not been incorporated at the National Benefits Center. This modification/application does have an auto-adjudication aspect to it but a detailed code review is required to fully understand the functionality. This will be completed by OCIO Security in the coming weeks. NBC IT staff stated that the auto-adjudication function of the I765 SQA application had failed tests at NBC and was not currently in use though it was being used at other service centers (Dallas).

On the last day of the NBC visit, the focus of the review became the benefits application process flow and the CLAIMS 3 uploads. The review staff focused on the input and output of the benefits processing by the National Benefits Center. It was determined that an unknown number of authenticated users were able to submit adjudicated applications that appear to have circumvented the established adjudication process as described in the following process flow diagram.

Process Flow



Conclusion

USCIS OCIO is in the process of conducting a thorough analysis of CLAIMS 3 data to determine the identity of the users that are able to process benefits applications without following the normal adjudication process and also to determine the number of applications that are currently processed in that fashion. This analysis will also provide the ability to determine the individual applications that were processed through the lock box/e-File processes, or by alternative methods. Based on these initial findings it appears that a full CLAIMS 3 process and code review are warranted. This process and code review will be conducted by OCIO Security once database access has been granted. The results of the review will be provided to the appropriate DHS personnel upon completion.

Attachment 5

MSC0427150001	I765	A074	951027	MIA	H4	593258511	UKRAI	RUSSI	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0427150002	I765	A074	951027	MIA	H4	591315990	RUSSI	RUSSI	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0427150003	I765	A095	A30129	NEW	H4	043067651	COLOM	COLOM	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0504150001	I765	A095	A30223	MIA	B2		COLOM	COLOM	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0504150002	I765	A095	A20418	MIA	B2		COLOM	COLOM	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0504150003	I765	A078	A30109	MIA	B2	771017985	COLOM	COLOM	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0504150004	I765	A095	A40203	ELP	B2	646789065	MEXIC	MEXIC	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0510950008	I765	A029	950926	WAS	B2	003881309	ITALY	ITALY	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0502550005	I90	A095					ARMEN			FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0502550006	I90	A095					SAFRI			FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0417850001	I765	A078	A20806	WAS	H4	626230176	GUATE	GUATE	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0503150002	I90	A037				503044945	HONDU			FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0504550008	I765	A095	A20812	NYC	B2	035703031	MOROC	MOROC	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0504550009	I765	A095	A20812	NYC	B2	222964299	MOROC	MOROC	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0504550010	I765	A095	A20812	NYC	B2	400610631	MOROC	MOROC	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0504550011	I765	A095	A20812	NYC	B2	685014778	MOROC	MOROC	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0504550007	I765	A095	A20812	NYC	B2	536519983	MOROC	MOROC	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0503850013	I765	A029	A10907	MIA	H4	485311438	COLOM	COLOM	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0503850014	I765	A029	A10907	MIA	H4	504332432	COLOM	COLOM	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0503850015	I765	A029	A10907	MIA	H4	493190068	COLOM	COLOM	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0504550006	I765	A029	A00921	NYC	B2	049026646	MOROC	MOROC	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0417950002	I765	A078	A20806	WAS	H4	626230175	GUATE	GUATE	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0417950003	I765	A078	A20805	WAS	H4	625234698	GUATE	GUATE	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0417950004	I765	A078	A20806	WAS	H4	625232925	GUATE	GUATE	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0417950005	I765	A077	A10910	WAS	H4	671078964	COLOM	COLOM	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0417950006	I765	A077	A10910	WAS	H4	671077740	COLOM	COLOM	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0417950007	I765	A077	A10910	WAS	H4		COLOM	COLOM	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0417950008	I765	A077	A10910	WAS	H4		COLOM	COLOM	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0417950009	I765	A073	A21015	WAS	H4	595386197	COLOM	COLOM	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0503850010	I765	A077	A31129	WAS	H4	538394674	PHILI	CANAD	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0503850011	I765	A095	A20812	NYC	H4	446173324	MOROC	MOROC	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0503850012	I765	A029	790101	LOS	H4	007021959	CHINA	CHINA	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0418150001	I90	A095					PAKIS			FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0502450007	I765	A029	840117	MIA	B2	602660846	COLOM	COLOM	C4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0502450008	I765	A029	890801	LOS	B2	257692109	COLOM	COLOM	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0502450009	I765	A029	A11201	MIA	B2	241998893	COLOM	COLOM	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0503850004	I765	A027	861215	LOS	H4	257559759	MEXIC	MEXIC	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0503850005	I765	A027	861215	LOS	H4	228393819	MEXIC	MEXIC	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0503850006	I765	A072	910828	NYC	H4	051865026	LITHU	LITHU	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0503850007	I765	A072	910828	NYC	H4	133782741	LITHU	LITHU	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0503850008	I765	A072	910928	NYC	H4	133783978	LITHU	LITHU	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013
MSC0503850009	I765	A072	A11020	BOS	H4	026866071	DOMIN	DOMIN	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC 20013

MSC0503850001	I765	A027	861215	LOS	H4	428559535	MEXIC	MEXIC	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC	20013
MSC0503850002	I765	A027	861215	LOS	H4	528617092	MEXIC	MEXIC	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC	20013
MSC0503850003	I765	A027	861215	LOS	H4	504085237		MEXIC	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC	20013
MSC0419250001	I765	A076	A40604	WAS	H4	001948292	COLOM	COLOM	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC	20013
MSC0419250002	I765	A079	A40604	WAS	H4	620274156	MEXIC	MEXIC	H4	FDN/BOB MCGRAW PO BOX 75840	WASHINGTON	DC	20013
MSC0419250003	I765	A078	A40604	WAS	H4	620272783	MEXIC	MEXIC	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC	20013
MSC0419250004	I765	A029	A30228	WAS	H4	523710846	MEXIC	MEXIC	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC	20013
MSC0419250005	I765	A029	A30228	WAS	H4	013720465	MEXIC	MEXIC	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC	20013
MSC0419250006	I765	A029	A30228	WAS	H4	519311862	MEXIC	MEXIC	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC	20013
MSC0419250007	I765	A029	A30228	WAS	H4	528914406	MEXIC	MEXIC	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC	20013
MSC0419250008	I765	A029	A30228	WAS	H4	537150030	MEXIC	MEXIC	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC	20013
MSC0419250009	I765	A029	A30228	WAS	H4	241639693	MEXIC	MEXIC	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC	20013
MSC0419250010	I765	A029	A30228	WAS	H4	433757047	MEXIC	MEXIC	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC	20013
MSC0419250011	I765	A029	A30228	WAS	H4	505255812	MEXIC	MEXIC	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC	20013
MSC0504550004	I765	A029	A00804	NYC	B2	649227424	RUSSI	RUSSI	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC	20013
MSC0504550005	I765	A077	A10101	SYS	EWI		MEXIC	MEXIC	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC	20013
MSC0420050001	I765	A097	A20720	NEW	E2	519658276	GERMA	GERMA	E2	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC	20013
MSC0420050002	I90	A017				485948634	CUBA			FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC	20013
MSC0420050004	I765	A095	910427	MIA	H4	221904511	COLOM	COLOM	H4	FDNS/BOB MCGRAW PO BOX 75840	WASHINGTON	DC	20013

Attachment 6

U.S. Citizenship and Immigration Services
Office of Fraud Detection and National Security
USCIS TECS Users Report

July 25, 2005

U.S. Citizenship and Immigration Services
Office of Fraud Detection and National Security
USCIS TECS USERS Report
July 25, 2005

PURPOSE: TECS access and information availability is of critical importance to USCIS' background check protocols. Four topics of concern are listed in brief below and analyzed within this document:

1) **TECS Access Levels for USCIS Users:** Examines the access level required for USCIS to carry out its background check protocols; the connection between background investigation levels and authorized TECS access; and the 1993 agreement between legacy INS and the legacy US Customs Service, which stipulates that a Full Background Investigation (Full BI) is necessary to access extra-agency lookout records above "Level 1."
2) **USCIS Loss of Administrative Control Over a USCIS TECS User Group:** Examines circumstances surrounding the removal by Customs and Border Protection (CBP) of a group of USCIS TECS users from USCIS administrative control, and implications to the USCIS background check mission.
3) **Creation of a USCIS agency profile/code by CBP:** Examines the history and creation of a distinct, restrictive agency code by CBP for USCIS, and its current status.
4) **Designation of USCIS as a "Third Party Agency" by CBP for Purposes of Sharing Information in the TECS system.** Examines the impact of this incongruent policy on the USCIS background check mission.

BACKGROUND: USICS access to lookout information from other agencies through TECS is dictated by a 1993[1] agreement between legacy INS and US Customs. The 1993 agreement lays out three background investigation types, which generally determine a user's access to TECS functions and data. With a *National Crime Information Center* (NCIC, AKA Type 1) background investigation, a user will have access only to their own agency's records. In the TECS user profile, the "BI Level" code is represented as "1." Employees with a *National Agency Check with Inquiries* background investigation (NACI, AKA Type 2) are authorized access to data from other agencies, but only records coded as Level 1 records in TECS; the TECS user profile displays this as "BI Level" "2." A *Full Background Investigation* (AKA Type 3) is required for access to records from other agencies coded higher than Level 1; the TECS user profile shows this as "BI Level" "3."

Issues with USCIS TECS access derive from modifications to the system and agency profiles by Customs and Border Protection (CBP), its current owner. On December 31, 2004, CBP migrated into the Treasury Enforcement Communication System (TECS) data from two Department of Justice databases upon which USCIS has relied heavily for information. As part of the migration process, both the Nonimmigrant Information System (NIIS) and the National Automated Immigration Lookout System (NAILS) were eliminated, requiring USCIS personnel who had not previously had access to TECS to obtain such access. At the same time, CBP removed USCIS from the TECS administrative framework that had been established for the Immigration and Naturalization Service (INS) in 1993, and created a separate National System Control Officer and hierarchy for USCIS.

Concomitant with this effort, CBP undertook to create a distinct USCIS agency user profile that would severely limit the access USCIS employees would have to records in TECS, *regardless of each user's*

---

[1] *Memorandum of Understanding Between the U.S. Custom's Service and the Immigration and Naturalization Service for the use of the Treasury Enforcement Communications System (TECS);* April 12, 1993; Michael H. Lane (Deputy Commissioner, USCS) and Michael T. Lempres (Executive Commissioner, US INS), signatories.

background investigation level. This USCIS user profile—coded B16—would not provide access to level 2,3, or 4 records from any agency outside USCIS, and would severely limit the number of agencies whose Level 1 records could be viewed. For example, USCIS would have no access to records from ICE, the Secret Service, DEA, and Interpol. Indeed, the only extra-agency records to which USCIS would have access under the B-16 profile were to be those from TIPOFF and the Department of State, with a limited number available from CBP, but even these would be at no higher than Level 1.[2] As established, the B-16 profile would have afforded USCIS users access even less than that established for a NACI, or Type 2 background investigation (BI), under the 1993 agreement. Recall that a NACI, or Type 2 BI, authorizes access to Level 1 records for all agencies, and that a Full BI authorizes access to extra-agency records above that level.

It was the intention of CBP to assign all USCIS users to the new "B16" profile. The plan was brought to the attention of USCIS leadership, which advised officials at CBP responsible for the proposal that the 1993 Memorandum of Understanding (MOU) authorized access to records owned by other agencies as long as employees met the Background Investigation (BI) levels stipulated in the agreement. CBP was persuaded to abort the restrictive aspects of the profile; but to date no retraction of the proposed profile description has been provided to USCIS. This is unsettling because CBP has begun coding USCIS users as B16.[3]

Aside from the general agency B16 coding issue, CBP did in fact manage to restrict TECS access for those USCIS employees in PICS who did not have access to TECS (including those who had allowed their access to lapse) at the time of the data migration in December 2004. Moreover, unlike all other employees within the USCIS TECS structure, USCIS is unable to make changes to access profiles within this group (coded as "XNNI"[4]), regardless of the background investigation level of an employee. It is suspected that a number of people in this group probably already had a full background investigation on record, but because they did not have access to TECS at the time of the data migration, they were, regardless, relegated by CBP to the XNNI profile once access was requested and granted by the system. Since January 2005, USCIS has been unable to reclaim administrative control over the TECS users in this group. At issue has been the demand by CBP to forward background check level information for USCIS employees. While USCIS has been willing to convey this information, there has been to date no agreement on the mechanism for delivering the information.

CBP placed no restriction on future employees, however. After establishing PICS identification for any new employee, USCIS can establish appropriate TECS access.

In fact, as part of the 1993 agreement, legacy INS had administrative control over its users, and was responsible for assigning access in TECS to each user commensurate with their background investigation type. There was, apparently, no mechanism for an automatic conveyance of background investigation level into TECS for assignment of access. Each System Control Officer filled the "BI Level" field themselves, based upon their knowledge of the process, the user's background investigation type, and any standing managerial limitations on use. While there are some USCIS employees outside of the administrative control of USCIS at the present time, USCIS does assign TECS access by associated BI Level to most of its employees. Twelve years have passed since the agreement was signed; in the interim. INS was dissolved and the U.S. Customs Service reorganized. In accordance with the 1993 MOU, and because of recent concern by USCIS over agency access, the accuracy of the "BI Level" entries into each user's profile by their respective System Control Officer raises three critical questions: 1) Are there USCIS employees that have greater TECS access than their background check level seemingly authorizes? 2) Are there USCIS employees that do not have the access to which they are entitled by

---

[2] "USCIS TECS Subject Access," December 17, 2004; conveyed to USCIS by Beverley Davidson, OIT Enforcement Systems Branch, CBP.

[3] TECS user profile records show some USCIS employees with B16 agency codes, some with B01 (described as "INS On-line").

[4] The XNNI profile allows access only to data in TECS identified as having derived from NIIS or NAILS, and is therefore not sufficient to complete background check protocols.

virtue of their background investigation level? 3) Is it reasonable, at this point in time, and considering the extraordinary information needs and budget constraints faced by the entire Department of Homeland Security, for CBP to impose a requirement for a "Full BI" on DHS employees with a "need to know"?

OBJECTIVE: With CBP's removal of USCIS from the legacy INS TECS administrative structure, its establishment of a distinct TECS hierarchy for USCIS, its attempt to restrict USCIS access to TECS, and its subsequent creation of a user group with limited TECS access that is also outside of our agency's administrative control, FDNS recognized two urgent needs: the first to determine current TECS access levels for all USCIS employees; and the second, to analyze the relationship between each employee's TECS access level and their background investigation category of record.

Ultimately, USCIS staff must possess a TECS access level necessary to ensure the retrieval of mission-critical national security and public safety information. Collective INS needs were addressed and met in 1993 with the access authorized by a Full Background Investigation (Full BI) and an agency profile not otherwise restricted. Certainly the events of 9/11 and the evolution of USCIS' background check protocols dictate that this agency must maintain access commensurate with what was afforded under INS. Information related to national security and public safety addresses our agency's greatest vulnerability. USCIS must prevent the extension of benefits to individuals not so entitled, and identify all risks to national security and public safety to do so.

This report presents the following data: a summary of TECS Access Levels for all USCIS users; a summary of actual USCIS Background Investigation levels for those USCIS users whose TECS profiles show they have had a full background investigation (BI Level 3), whether or not they have had the required Full BI; and a summary of the Background Investigation Levels for USCIS users assigned by CBP to the XNNI restricted profile (which is outside of USCIS TECS administrative control).

FINDINGS: Chart A, directly below, shows the USCIS TECS user community at 6,572 persons. Of this total, 4,950, or 75% have access at the level authorized only by a full background investigation. This is represented in TECS as "BI LVL 3." Around 16%, or 1,073 people, are noted with "BI LVL2" access. Some 515 people have been assigned by CBP with the very restricted XNNI profile—essentially receiving only information migrated into TECS from NAILS and NIIS and USCIS data. The XNNI profile cannot be changed by USCIS, and is without regard to the BI level the employee may have.

Chart A

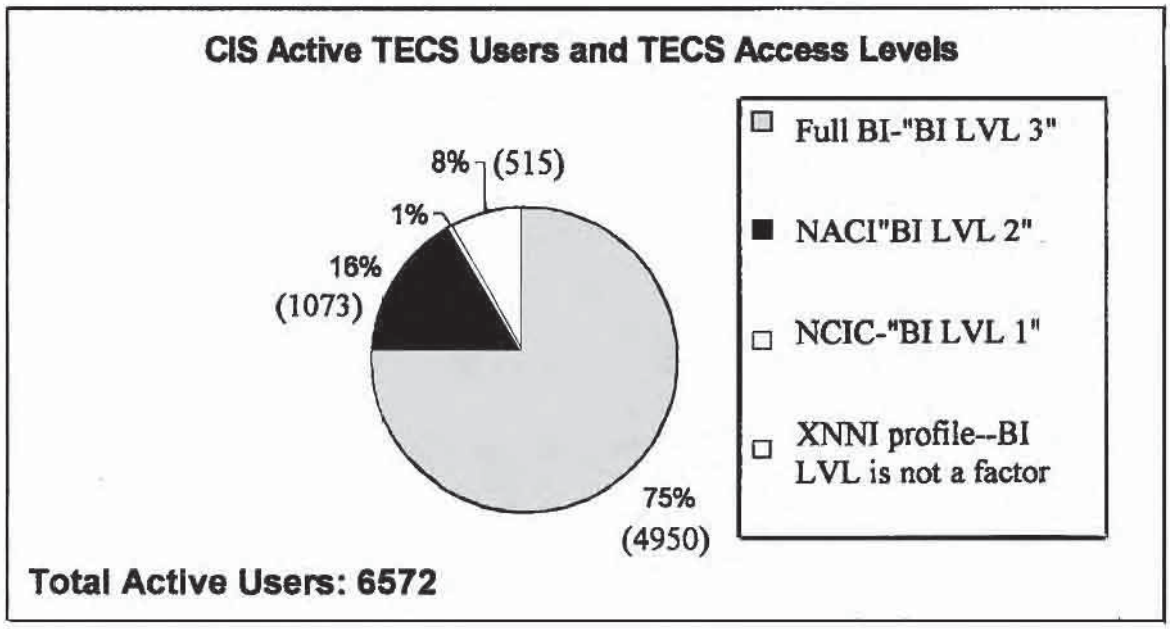


Chart B, below, examines the 75% of USCIS users (4,950 people) with "BI Level 3" access. Of this total, 49% are registered in PICS as having had the required Full Background Investigation. Another 51% are registered as having had only a Limited Background Investigation. This may be due to an SCO granting an incorrect access level or failing to down-grade an employee whose subsequent background investigations were limited in scope.

Chart B

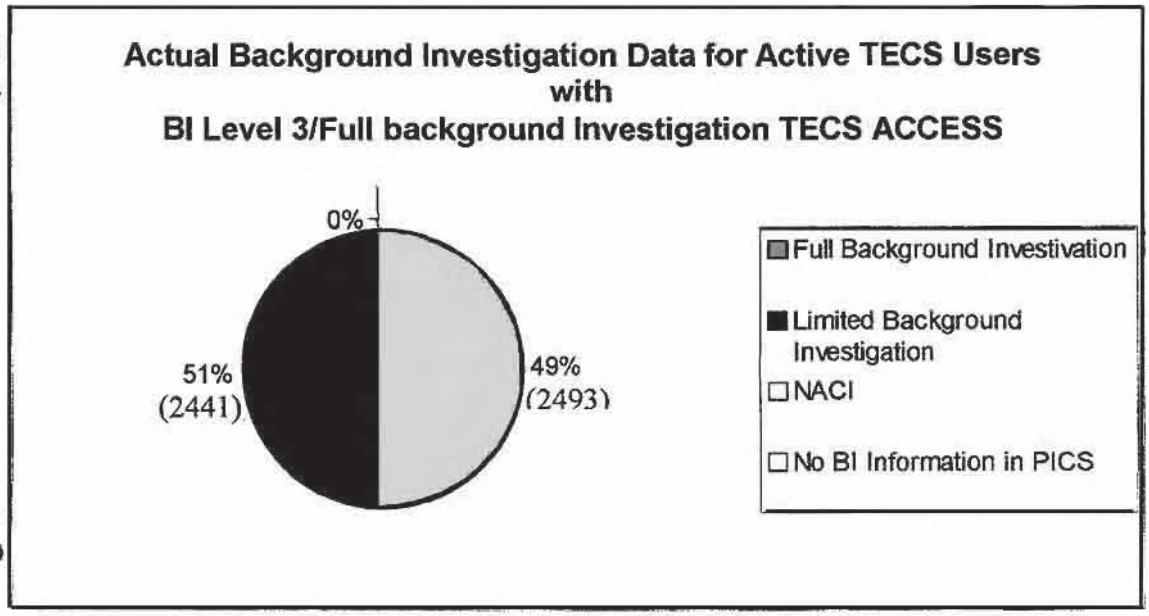
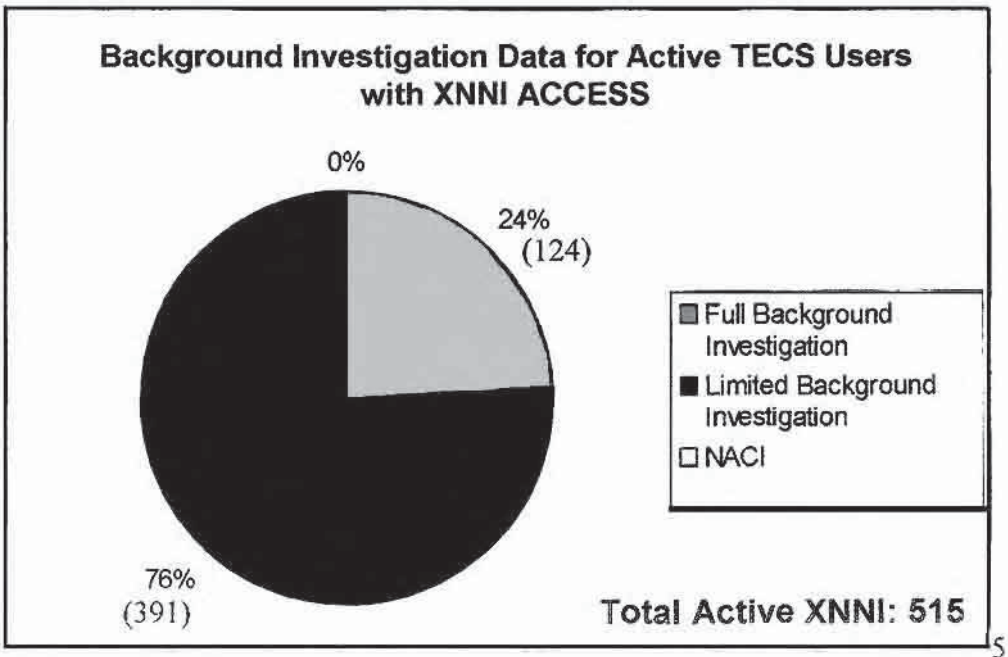


Chart C, below, examines the 8% of USCIS users (515 people) with the severely restricted XNNI profile. Of this total, 24% are registered in PICS as having had a Full Background Investigation. They are entitled, therefore, to access afforded by a Full BI—BI Level 3. Another 76% are registered as having had only a Limited Background Investigation, which, according to the 1993 MOU certainly does authorize at least Level 1 access to other agency records, which far exceeds the information returned with an XNNI Access.

Chart C



SUMMARY AND RECOMMENDATIONS: Without access to higher level extra-agency TECS records, USCIS employees with background check responsibilities may miss information that is critical to the adjudicative process. In the absence of this information, USCIS could grant an immigration benefit to someone who poses a threat to national security or public safety. Notwithstanding the partial unilateral abrogation of the 1993 MOU by CBP at the end of 2004, USCIS employees are entitled to full TECS access with a *completed* full background investigation.

Recommendation #1. *USCIS should examine means to conduct, complete, and maintain full field investigations for all employees with background check responsibilities.* This summary does not identify individuals in USCIS with background check responsibilities; for purposes of this analysis, all persons with access to TECS were presumed to be engaged in background check activity. The following summary and analysis approximates the maximum number of persons for whom a full background investigation may need to be conducted by USCIS, as of June, 2005:

1) 75% of all USCIS users (4,950 of 6,572) have BI Level 3 access:

- BUT, 51% of these users DO NOT have the required full background investigation for this access. It is possible that these persons had an initial full BI, but subsequent investigations were not conducted at the same level. Their access in TECS, however, was never downgraded. This equates to **2,441** additional full background investigations.

2) 25% of all USCIS users (1,643 of 6,572) have less than BI Level 3 access.

- 68% of these users are under the administrative control of USCIS; once a full BI is completed for them, USCIS can upgrade their TECS access level.
- 32% of these 1,643 employees were removed from USCIS administrative control by CBP. Despite the fact that 124 of these users have the required Full BI, USCIS cannot upgrade their TECS access. These 124 should not require a new full BI.[5]
- In this subgroup, then, **1,478** additional full background investigations may be required

The total number of persons identified in 1) and 2) above for whom a full field investigation may need to be conducted in order for those employees to gain full access to TECS is *3,919*. Because some employees with current access to TECS functions may not be engaged in background check activity, the total number of required investigations will likely be smaller.

Recommendation #2. *USCIS must regain administrative control over the user group coded "XNNI"—without the requirement of transmitting background investigation information to CBP.* CBP's compartmentalization and removal from USCIS administrative control of those employees who did not have TECS access at the time of the data migration is contrary to the 1993 MOU and the 2004 establishment by CBP of a USCIS TECS hierarchy. The 1993 MOU requires the user agency to coordinate and designate TECS access for its employees.

Recommendation #3. *USCIS must be guaranteed that there are no restrictive aspects to the B16 agency code. We also need to know why some of our employees are coded as B16, and others are still B01.* CBP must advise USCIS of the meaning of the agency code set for USCIS—B16—as this code originally implied not only an agency identifier but a restricted profile for all USCIS users, regardless of background investigation level. As noted earlier, CBP has not conveyed the information, though the agency has indeed moved personnel in USCIS from the B01 agency code to the B16.

---

[5] The total number of persons outside of USCIS' administrative control may be slightly larger than 515, because only Active TECS users were counted. Some USCIS employees who were assigned to the XNNI group stopped using TECS, because their access was insufficient. Their accounts became inactive.

Recommendation #4. *USCIS must work to eliminate the information bias demonstrated by CBP against this agency.* CBP has advised on many occasions that it considers USCIS to be a "Third Party Agency," and that it will not provide details surrounding records it has placed in TECS. This assertion has been made by upper management, despite the fact that CBP's own TECS training module states that all organizational elements under DHS are considered part of a single agency, and that information can be shared simply by establishing that a DHS employee has a "need to know." This creates an impossible situation for USCIS employees conducting background check resolution activities, as ports-of-entry note they may not release information, and the National Targeting Center, CBP's operational center, states categorically that it will not provide any assistance to USCIS callers who have encountered a CBP hit. While some of the hits involve the JTTF and can be accessed by employing the assistance of the TSC, unless there is a JTTF involvement, USCIS will not receive derogatory input from CBP beyond a TECS record.

Attachment 7

From: Nolin, Patricia
Sent: Friday, September 09, 2005 8:45 AM
To: Mullin, Geoffrey M
Subject: [redacted] (PDOB: Somalia; 02/10/1968) [redacted]

Importance: High
Sensitivity: Confidential

Geoff, Not sure if I should be making this request, but I'll take a chance. The above-referenced individual has filed a Mandamus against the Service relating to his unadjudicated N400 application. The Name Check Process returned a POSITIVE RESULT and the FBI LHM and FDNS follow-up provides FOCUS with no details, other than the individual is the subject of an ongoing investigation with national security implications. According to FDNS, in order to maintain 'case integrity' the FBI did not provide specifics of the case, but the case should be placed in Abeyance. I was wondering if you would be able to obtain more detailed information regarding the investigation along to assist FOCUS with this case and information that could be used in open court before the judge to explain the need for placing the case in Abeyance. Thanks for your help, Pat

Attachment 8

From: Haas, Dennis
Sent: Thursday, September 15, 2005 1:40 PM
To: Miner, Lloyd W; Berglund, John M; Mullin, Geoffrey M
Subject: FW: Interview Notes

Sensitivity: Confidential

Geoff:

See below traffic.

-----Original Message-----
From: Sposato, Janis A
Sent: Thursday, September 15, 2005 1:28 PM
To: Maxwell, Michael J
Cc: Aytes, Michael; Yates, William R; Paar, Tom; Haas, Dennis
Subject: RE: Interview Notes
Sensitivity: Confidential

Thank you Michael. You and your staff have been very responsive to me and to Focus, and I appreciate that.
Janis

----Original Message-----
om: Maxwell, Michael J
Sent: Thursday, September 15, 2005 1:26 PM
To: Sposato, Janis A
Cc: Aytes, Michael; Yates, William R; Paar, Tom; Haas, Dennis
Subject: RE: Interview Notes
Importance: High
Sensitivity: Confidential

Janis,

I have spoken with Tom Paar on this particular case. I need to make my position clear to all parties. With the approval of the Chief of Staff, in this case only, we can finish the job and share the information. However, in the future, I have been directed to cease OSI participation in the FOCUS initiative and, as seen in the email below, had already directed my staff that OSI shall not be involved in future FOCUS initiatives unless approved by Bill, the COS, and ADD.

I will have Geoff Mullin contact Pat to close the loop and then must withdraw from the process.

Vr,

Michael

-----Original Message-----
From: Sposato, Janis A
Sent: Thursday, September 15, 2005 1:03 PM
Maxwell, Michael J
Cc: Aytes, Michael; Yates, William R
Subject: FW: Interview Notes
Importance: High

Maxwell, Michael J

From: Sposato, Janis A
Sent: Thursday, September 15, 2005 1:03 PM
o: Maxwell, Michael J
Cc: Aytes, Michael; Yates, William R
Subject: FW: Interview Notes

Importance: High
Sensitivity: Confidential

Michael
I don't want to interfere with whatever instructions you got from Robert, but one of our FOCUS mandamus cases seems to have gotten caught in the middle. I understand that your staff had contacted Secret Service and obtained adverse information for us about the applicant, but that they now feel constrained to share it. Can you see your way clear to allow your staff to share what they have? Or would you rather I ask Robert for permission? I apologize for putting you on the spot.
Janis

-----Original Message-----
From: Nolin, Patricia
Sent: Thursday, September 15, 2005 9:20 AM
To: Sposato, Janis A
Cc: Mulrean, Mary C; Leclair, Kellie
Subject: FW: Interview Notes
Importance: High
Sensitivity: Confidential

Janis, FOCUS was hoping to use information that OSI (Office of Security and investigation) was going to provide in support of this N400 case. According to information previously provided by OSI, this individual is involved in moving large sums of money, and under current investigation by the Secret Service. According to the information FDNS provided FOCUS, there was no derogatory information and we should proceed with adjudication. FOCUS needs the information available to OSI in order to render an appropriate decision in this case. Thanks, Pat

-----Original Message-----
From: Leclair, Kellie
Sent: Thursday, September 15, 2005 9:08 AM
To: Nolin, Patricia
Subject: FW: Interview Notes
Importance: High
Sensitivity: Confidential

Pat,
This is regarding the [redacted] mandamus case.
Thanks,
Kellie

-----Original Message-----
From: Mullin, Geoffrey M
Sent: Wednesday, September 14, 2005 6:48 PM
To: Leclair, Kellie
Cc: 'john.berglund@dhs.gov'
Subject: Interview Notes

Kellie,
Recvd your message ref reviewing the interview notes you have just been forwarded. I would like to assist but I have been instructed that I will be directly defying the Acting

Deputy Directors order if I do. You may ask Pat to ask her boss to talk with Director Maxwell as I know he is receptive to our doing whatever we can to help you guys. Hoipe this can be resolved in time!
Geoff

Sent from my BlackBerry Wireless Handheld

Attachment 9

U.S. Department of Homeland Security
Washington, DC 20258

U.S. Citizenship and Immigration Services

HQ 70/2.1

Interoffice Memorandum

To: Asylum Directors
Regional Directors
District Directors
Service Center Directors
National Benefits Center Director

From: William R. Yates
Associate Director of Operations

for Joseph Cuddihy
Associate Director, Office of Refugee, Asylum, and International Relations

Date: March 29, 2005

Subject: CLARIFICATION and MODIFICATION of New Resolution Process for IBIS National Security/Terrorism-Related Positive Results

This memorandum provides clarification and modification to some of the procedures described in the November 29, 2004 memorandum entitled *"New Resolution Process for IBIS National Security/Terrorism-Related Positive Results."*

Background

USCIS, as an integral part of the Department of Homeland Security, conducts many millions of background checks on persons seeking to obtain or receive benefits under the INA each year. Our ongoing effort to maintain and enhance National Security and Public Safety demands constant resolve and cooperation. In order to achieve the highest level of success, the office of Fraud Detection and National Security (FDNS) was created; its first priority is to identify persons who pose a threat to national security or public safety. To accomplish this mission, the FDNS develops and oversees background check policy and procedures.

I. Modifications to the November 29, 2004 IBIS National Security Resolution Process

A. Procedural Change for all National Security Notifications (NSN)

In order for the FDNS to appropriately oversee the IBIS National Security/Terrorism-related hit resolution process, and also acquire significant data relevant to the background check process, it has been determined that HQ FDNS should receive notification on all National Security/Terrorism- related IBIS hits, and review all notifications before USCIS offices proceed with resolution.

Effective immediately, all offices, through the FDU or FDNS Immigration Officer, will complete and e-mail the form *IBIS-National Security Notification (NSN)* to HQ FDNS at **FDNS-IBIS@dhs.gov** whenever an IBIS National Security/Terrorism-related hit is encountered.[1] Use the revised NSN form posted on the FDNS website. After the encountering office forwards an NSN to HQ FDNS, it must wait for confirmation from HQ FDNS before proceeding with resolution—HQ FDNS will review every NSN for completeness, and inform the submitting office if the NSN must be revised and resubmitted. Once the form is deemed complete by HQ FDNS, the submitting office will be notified either to proceed with the resolution locally or to await a resolution by HQ FDNS.[2] (While most resolutions will still be performed by submitting offices, some cases will be selected for resolution at HQ FDNS.)

B. **Procedural Change for all National Security Case Resolution Records**

HQ FDNS will also review and analyze all USCIS national security resolutions, requiring the following modification to the November 29, 2004 memorandum: Effective immediately, all national security case resolutions must be emailed to HQ FDNS at **FDNS-IBIS@dhs.gov** (use the form *IBIS-National Security Case Resolution Record*, released with the November 29, 2004 memorandum).[3] ALL further action on these cases must be suspended until they are cleared for adjudication by either the HQ FDNS Background Check Analysis Unit (BCAU)[4] or FOCUS[5], as described in the process that follows.

---

[1] A modification was made to the original NSN form released on November 29, 2004; a new box—"IBIS HIT (Notification Only)"—has been added. A copy of the revised form accompanies this memorandum (it is still a fill-able Word document). It will also be distributed and available on the FDNS website.

[2] *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.

[3] It is critical to remember to use only the FDNS forms created specifically for the NSN process. See the FDNS website.

[4] The division of the National Security branch within HQ FDNS that is devoted to background check resolution and policy formation is the Background Check Analysis Unit (BCAU).

[5] To assist adjudications in utilizing information obtained through background check resolution processes, USCIS recently created FOCUS, a headquarters review board within Field Service Operations. USCIS offices may refer cases to FOCUS for adjudication guidance at any time following the receipt of background check resolutions. HQ FDNS will refer some cases directly to FOCUS. The Office of Refugees, Asylum and International Operations (ORAIO) will not participate in the FOCUS review process. Field Service Operations will release further FOCUS details at a later date.

C. Clearance Process for Adjudication—How BCAU Interacts with FOCUS

Once an IBIS National Security Case Resolution Record is received at HQ FDNS, it will be reviewed for completeness; the submitting office will be informed if it must be revised and resubmitted. After the Case Resolution Record has been deemed complete by the BCAU, the BCAU will notify the submitting office either that it may forward the case to adjudications, OR that the case has been referred to FOCUS by BCAU[6].

When cases are referred to FOCUS, the submitting office must not release the case for adjudication until it is cleared by FOCUS. During the period of review by FOCUS, any follow-up by the submitting office should be made directly with FOCUS. Once FOCUS has completed its impact assessment, FOCUS will contact the FDU or IO holding the case file directly. At this point, after receiving a response from FOCUS, the FDU/IO will forward the case file containing both the IBIS national security resolution and the FOCUS impact assessment to adjudications.

IL Other FDNS Clarifications and Modifications

A. The role of the Regional FDNS Immigration Officer in IBIS National Security Resolution

As part of the overall effort to streamline the National Security/Terrorism IBIS resolution process, it has been recognized that offices lacking an FDNS Immigration Officer (IO) may not be best positioned to resolve National Security/Terrorism-related IBIS hits. Superseding the November 29, 2004 memorandum, and effective immediately, adjudicators in Field offices without an FDNS Immigration Officer will no longer resolve National Security/Terrorism-related IBIS hits. Instead, adjudicators will e-mail their National Security IBIS hits for resolution (via the form IBIS-National Security Case Resolution Request, released with the November 29, 2004 memorandum) to their corresponding Regional FDNS Immigration officer for resolution. It will also be the responsibility of the designated FDNS IO to review each submission, e-mail an NSN to HQ-FDNS, and e-mail the resolution record to HQ-FDNS once complete.

As indicated in the November 29, 2004 memorandum, the Regional FDNS IO also functions as the regional coordinator for the resolution of IBIS National Security/Terrorism-related positive hits for their respective field offices. The Regional FDNS IO is available to assist field FDNS Immigration Officers with general questions and resolution issues. The Regional IO will, in turn, seek the general assistance of HQ FDNS, or request HQ FDNS assume certain resolutions.[7]

---

[6] The Office of Refugees, Asylum and International Operations (ORAIO) will not participate in the FOCUS review process. The BCAU will refer all National Security Case Resolutions deemed complete to the HQ Asylum Quality Assurance unit. During the period of review by HQ Asylum QA any follow-up meetings by the submitting office should be made directly with HQ Asylum QA

[7] *The Regional IOs are 1) Central: Jeff T. Boyd; 2) Eastern: Robert M Salyer; 3) Western: Kenneth N. Takeda*

B. <u>Instructions Regarding Pending IBIS "SIR" Cases</u>
Until further notice, no USCIS office is to perform resolution on any pending "SIR" Remember the "SIR" process terminated with the November 29, 2004 memorandum; all outstanding "SIRS" are now part of the backlog of "SIR" cases at the National Security and Threat Protection unit (NSTP—the component of ICE that assumed national security IBIS resolution activity from the INS National Security Unit). The ONLY National Security/Terrorism-related IBIS resolutions to be conducted by USCIS offices are those associated with the National Security Notification (NSN) process created with the November 29, 2004 memorandum. When confronted with litigation, an office with a pending "SIR" should contact the FDNS for assistance. FDNS will request expedited processing from the NSTP for those cases ONLY.

C. <u>Contact with the Central Intelligence Agency (CIA)</u>
All contact with the CIA will be coordinated by HQ FDNS. Should any background check require contact with the CIA, request the assistance of HQ FDNS through the **<u>FDNS-IBIS@dhs.gov</u>** mailbox.

FDNS will be conducting FDU and field regional teleconferences to discuss these new procedures. We ask that any questions be directed through the appropriate chain of command to the National Security Branch staff at **<u>FDNS-IBIS@dhs.gov</u>**.

cc: Don Crocetti
Director, Fraud Detection and National Security

Terrance O'Reilly
Director, Field Service Operations

Fujie Ohata
Director, Service Center Operations

Joseph Langlois
Director, Asylum