

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

National Security Nightmare

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.”

National Security Nightmare

- 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.

National Security Nightmare

- 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.

National Security Nightmare

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

National Security Nightmare

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 breaches 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 underfunded, 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 October 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.

National Security Nightmare

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 inquiries 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,

National Security Nightmare

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.*

National Security Nightmare

[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.

National Security Nightmare

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.

National Security Nightmare

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:

National Security Nightmare

“ 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.

National Security Nightmare

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:

National Security Nightmare

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).

National Security Nightmare

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 all national-security related IBIS hits since March 2005.”

⁹ Attachments 7 and 8: FOCUS emails.

National Security Nightmare

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.

National Security Nightmare

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.

National Security Nightmare

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 breach 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.