AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 112–621

OVERSIGHT OF THE U.S. DEPARTMENT OF HOMELAND SECURITY

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

APRIL 25, 2012

Serial No. J–112–73

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
76–711 PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

HERB KOHL, Wisconsin
DIANNE FEINSTEIN, California
CHUCK SCHUMER, New York
DICK DURBIN, Illinois
SHELDON WHITEHOUSE, Rhode Island
AMY KLOBUCHAR, Minnesota
AL FRANKEN, Minnesota
CHRISTOPHER A. COONS, Delaware
RICHARD BLUMENTHAL, Connecticut

CHUCK GRASSLEY, Iowa
ORRIN G. HATCH, Utah
JON KYL, Arizona
JEFF SESSIONS, Alabama
LINDSEY GRAHAM, South Carolina
JOHN CORNYN, Texas
MICHAEL S. LEE, Utah
TOM COBURN, Oklahoma

BRUCE A. COHEN, *Chief Counsel and Staff Director*
KOLAN DAVIS, *Republican Chief Counsel and Staff Director*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont	1
prepared statement	217
Grassley, Hon. Chuck, a U.S. Senator from the State of Iowa, prepared statement	209

WITNESSES

Napolitano, Janet, Secretary, U.S. Department of Homeland Security	4

QUESTIONS AND ANSWERS

Responses of Janet Napolitano to questions submitted by Senators Whitehouse, Sessions, Franken, Grassley, and Leahy	44
Question 12, December 15, 2011, Final Report	116
Question 27, Memorandum of Understanding	200
Question 31, I–765 Application for Employment Authorization	202

SUBMISSIONS FOR THE RECORD

Napolitano, Janet, Secretary, U.S. Department of Homeland Security, statement	219
Peacock, Nelson, Assistant Secretary for Legislative Affairs, Homeland Security, Washington, DC, April 24, 2012, letter	243

OVERSIGHT OF THE U.S. DEPARTMENT OF HOMELAND SECURITY

WEDNESDAY, APRIL 25, 2012

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The Committee met, pursuant to notice, at 9:33 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Patrick J. Leahy, Chairman of the Committee, presiding.

Present: Senators Leahy, Feinstein, Schumer, Durbin, Whitehouse, Klobuchar, Franken, Coons, Blumenthal, Grassley, Sessions, Kyl, Graham, Cornyn, and Lee.

OPENING STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Chairman LEAHY. Good morning. We will let the photographers get all their shots, but then I am going to ask you, once you have done that, to step back so we can get started.

OK. I think we can get started. Senator Graham is here. I know Senator Schumer dropped in briefly before from the Rules Committee and will be back. Senator Grassley has told me he is over on the House side—is that correct?—and will be joining us. Senator Kyl is here. Senator Grassley said to go ahead, and we will.

Secretary, you know Senator Kyl is from the State of Arizona, I believe.

Secretary Napolitano. I think we know he is.

[Laughter.]

Chairman LEAHY. Yes, I suspect you do.

I want to welcome Secretary Napolitano back to the Judiciary Committee. We are continuing our important oversight of the Department of Homeland Security. She has testified here before, and I think I can speak for every member of the Committee that she has also been responsive if we have called with questions in between the testimony.

This is our oversight of the Department of Homeland Security and the work that the women and men of the agencies within the Department do every day to keep Americans safe.

Now, much attention has been focused on an incident prior to President Obama's attendance at the recent Summit of the Americas in Cartagena, Colombia. I have spoken a number of times with Secret Service Director Sullivan about this. In fact, we met privately for about an hour yesterday, and we probably have been on the phone half a dozen or a dozen times. I have known the Director from the time when he was an agent. I knew him when President

Bush appointed him as Director of the Secret Service and when President Obama reappointed him. I know that he shares my view that the alleged conduct was unacceptable. I think he is doing all he can to ensure a timely and thorough investigation and accountability for behavior that failed to meet the standards he expects and certainly the standards that the President of the United States and the American people deserve. He has taken action on 12 agents who it is claimed have been involved in misconduct.

Last week, I arranged for a bipartisan briefing for Judiciary Committee staff, Republican and Democratic, with the Secret Service and officials of the Department of Homeland Security's Office of Inspector General. I have asked the Director to be sure he is available to members of this Committee as the investigation continues. He assured me he will be and that he will make sure that we know exactly when they finish the investigation and everything they have found.

Now, I have no doubt you are treating this situation with equal seriousness. Certainly in my conversations with you, you have talked a great deal with the Director during this time. Nobody wants to see the President's security compromised; nobody wants to see America embarrassed.

I pointed out to the Director that not only does the Secret Service protect the President of the United States, but they are also going to be and are protecting the man who is going to be the Republican nominee for President, Governor Romney. I cannot think of anything, aside from the personal tragedy, that would look worse to the rest of the world if something happened either to President Obama or Governor Romney, especially during a Presidential election. I think everybody here would agree with that.

Now, you told us at your first appearance as Secretary you would focus on using limited Federal law enforcement resources in a smarter, more effective manner when enforcing our immigration laws. You and Immigration and Customs Enforcement Director John Morton are following through. The implementation of ICE's prosecutorial discretion policy is a positive step forward. If this new policy has the effect of apprehending more individuals who are legitimate threats to public safety and providing some measure of relief to those who pose no threat, then that is an improvement. And you are standing by your commitment to focus first and foremost on the most dangerous among the undocumented population. Mr. Morton was in Vermont, and we discussed that then, too.

And I think you are doing the best you can in the absence of Congress taking up meaningful and comprehensive immigration reform. As you know, I supported President Bush's efforts for meaningful and comprehensive immigration reform, and I still would like to see that. Even though that has very little impact on my State of Vermont, it has an enormous impact on the rest of the country.

In fact, as we hold this hearing today, the Supreme Court is hearing argument on the constitutionality of an Arizona immigration enforcement law. The Constitution of the U.S. declares that Congress and the Federal Government shall have the power to establish a uniform "Rule of Naturalization. "So national immigration policy is properly a subject we should act upon. It should not be

left to a hodgepodge of conflicting State laws. I hope we can get back to where we can do good, strong, comprehensive, bipartisan immigration policy.

In 2010, we passed an emergency appropriations measure to provide $600 million for border security enhancements. You have reported that we have made significant strides there. I understand that illegal border crossings on the southern border have declined, and we have seen steady increases in the numbers of Border Patrol and Customs and Border Protection officers monitoring our borders. And I take special notice as well that you are working with Canadian officials on the Beyond the Border Initiative, coordinating on our shared northern border, and I am impressed with that.

If I can be parochial—and it is very rare that somebody is parochial in any one of these committees, but in Vermont, many people look forward to our friends from Canada visiting and enjoying all that Vermont has to offer. And at least when I was a youngster, if you just felt like going to a different—another State, it is that easy going back and forth across the border. We take that for granted, and I hope that we can work on that—to protect our security but keep that border as open as possible.

I was pleased to see that the EB–5 Regional Center Program was among your recommendations and those of the President's Council on Jobs and Competitiveness. We have worked with that in Vermont. I look forward to working for reauthorization of this program. Senator Grassley and I have been working together to get this and other expiring visa programs reauthorized in a bipartisan manner. I will continue to work with you and with USCIS Director Mayorkas to strengthen and improve the EB–5 program.

I have raised the issue of screening procedures and technology in our airports. I continue to have questions about these policies, their impact on the privacy and health of Americans, and whether this technology is the most effective use of resources. Obviously, when you see an elderly person in a wheelchair going through all kinds of screening, I am not quite sure how that is keeping us safer, but we can talk about it.

I want to make sure that as we go to national cybersecurity we protect our rights and civil liberties. And, finally, I want to commend the women and men who work in the agencies of your Department. I have met so many of them, all different branches. I know they work very, very hard and care about our country. Many are Vermonters who are working hard to adjudicate immigration benefits at the Vermont Service Center, but that can be said of all our States. We will expand the workforce in St. Albans, Vermont, the Vermont Service Center, but I just am constantly impressed every time I see the men and women that work there.

In the absence of Senator Grassley, Senator Kyl, did you wish to make an opening statement before we go to the Secretary?

Senator KYL. No, Mr. Chairman. I think we want to hear from the Secretary, and then we will all have questions, but thank you.

Chairman LEAHY. Well, Madam Secretary, the floor is open to you, and then we will go to 7-minute rounds. We will rotate in the usual manner from side and side in the order in which people arrived.

Secretary Napolitano, please go ahead.

STATEMENT OF HON. JANET S. NAPOLITANO, SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY

Secretary NAPOLITANO. Thank you, Chairman Leahy and members of the Committee. I am pleased to be with you today, and I thank the Committee for your support of the Department over these past 3 years and, indeed, since the Department was founded more than 9 years ago.

Before I begin, I want to address the allegations of misconduct by Secret Service agents in Colombia. The allegations are inexcusable, and we take them very seriously.

Since the allegations first surfaced, I have been in close touch with Director Sullivan. The Director took immediate action to remove the agents involved, and a full and thorough investigation is underway to determine exactly what transpired and actions we need to take to ensure that this kind of conduct does not happen again.

Director Sullivan has the President's and my full confidence as this investigation proceeds. The investigation will be complete and thorough, and we will leave no stone unturned.

Thus far, the investigation has implicated 12 Secret Service personnel. Eight individuals are now separated from the agency. The Secret Service is moving to permanently revoke the security clearance of another, and three of the employees involved have been cleared of serious misconduct but will face appropriate administration action. At this time, therefore, all 12 Secret Service personnel identified in the investigation have either faced personnel action or been cleared of serious misconduct.

Let me be clear. We will not allow the actions of a few to tarnish the proud legacy of the Secret Service, an agency that has served numerous Presidents and whose men and women execute their mission with great professionalism, honor, and integrity every single day. I have nothing but respect for these men and women, many of whom put their own lives at risk for the President and many other public leaders.

We expect all DHS employees, in the Secret Service and throughout the Department, to adhere to the highest professional and ethical standards, and we will continue to update the Committee as the investigation proceeds and more information becomes available.

Let me now move to the Department's progress since 9/11. Ten years after the terrorist attacks of September 11, America is stronger and more secure today thanks to the support of the Congress, the work of the men and women of the DHS, and our Federal, State, and local, partners who work across the homeland security enterprise.

As I have said many times, homeland security begins with hometown security. As part of our commitment to strengthening hometown security, we have worked to get information, tools, and resources out of Washington, D.C., and into the hands of State and local officials and first responders.

This has led to significant advances. For example, we have made great progress in improving our domestic capabilities to detect and prevent terrorist attacks against our people, our communities, and

our critical infrastructure. We have increased our ability to analyze and distribute threat information at all levels through fusion centers, the Nationwide Suspicious Activity Reporting Initiative, the National Terrorism Advisory System, and other means.

We have invested in training for local law enforcement and first responders in order to increase expertise and capacity at the local level. We have supported preparedness and response across our country through approximately $35 billion in homeland security grants since 2002. And we have proposed important adjustments to our grant programs for fiscal year 2013 to continue to develop, sustain, and leverage these core capabilities.

Our experience over the past several years has made us smarter about the terrorist threats we face and how best to deal with them. We have learned that an engaged, vigilant public is essential to efforts to prevent acts of terrorism, which is why we have continued to expand the "If You See Something, Say Something" campaign nationally.

We have also expanded our risk-based, intelligence-driven security efforts across the transportation sector, the global supply chain, and critical infrastructure. By sharing and leveraging information with our many partners, we can make better informed decisions about how to best mitigate risk.

Over the past several years, we also have deployed unprecedented levels of personnel, technology, and resources to protect our Nation's borders. These efforts, too, have achieved significant results, including historic decreases in illegal immigration as measured by total apprehensions and increases in seizures of illegal drugs, weapons, cash, and other contraband. In fact, illegal immigration attempts are at their lowest levels since 1971 while violent crime in U.S. border communities has remained flat or has fallen over the past decade.

We also have focused on smart and effective enforcement of immigration laws while streamlining and facilitating the legal immigration process. Last year, ICE removed record numbers of illegal aliens from the country, 90 percent of whom fell within our priority categories of criminal aliens and repeat immigration law violators, recent border entrants, and immigration fugitives. We have focused on identifying and sanctioning employers who knowingly hire workers not authorized to work in the United States.

We have made important reforms in our immigration detention system so that every individual in custody is treated in a fair, safe, and humane manner consistent with ICE detention standards. And we have worked to reduce bureaucratic inefficiencies in visa programs, streamlined the path for entrepreneurs who wish to bring business to the United States, and improved systems for immigration benefits and services.

In the critical area of cybersecurity, we also continue to lead the Federal Government's efforts to secure civilian government networks while working with industry, State, and local governments to secure critical infrastructure and information systems. We are deploying the latest tools across the Federal Government to protect critical civilian systems while sharing timely and actionable security information with public and private sector partners to help them protect their own operations. With these partners, we are

also protecting the systems and networks that support the financial services industry, the electric power industry, and the telecommunications industry, to name just a few.

We stand ready to work with the Congress to pass legislation that will further enhance our ability to combat threats in the cyber domain. Specifically, we support legislation that would, among other things, establish baseline performance standards for the Nation's critical core infrastructure; remove barriers to information sharing between Government and industry so that we can more quickly respond to and mitigate cyber threats or intrusions; ensure robust privacy oversight to ensure that voluntarily shared information does not impinge on individual privacy and civil liberties, including criminal penalties for misuse; and provide DHS with the hiring flexibility to attract and retain the cybersecurity professionals we need to execute our complex and challenging mission.

Mr. Chairman, threats against our Nation, whether from terrorists, criminals, or cyber adversaries, continue to evolve. And DHS must continue to evolve as well. I look forward to working with you and members of the Committee to build on the progress we have achieved across these and many other mission areas. We remain ever vigilant to threats as we continue to promote the free movement of goods and peoples essential to our economy and protect our essential rights and liberties.

Thank you, Mr. Chairman.

[The prepared statement of Secretary Napolitano appears as a submission for the record]

Chairman LEAHY. Thank you, and, of course, we will put your full statement in the record.

As I told you, with our jurisdiction over the U. S. Secret Service, we did want to ask you some questions there. I am, of course, like all Americans, concerned about the safety of our President, whether it could have been jeopardized by this kind of behavior, just as I am concerned about the safety of any of the protectees. I mentioned Governor Romney, but there are several others.

The misconduct we have heard about, did that pose any risk to the President's security when in Colombia or to national security?

Secretary NAPOLITANO. Mr. Chairman, that was my first question to Director Sullivan when he called me, and the answer is no, there was no risk to the President.

Chairman LEAHY. And you made that assessment?

Secretary NAPOLITANO. Yes, based on the information supplied to me by the Director.

Chairman LEAHY. And is the Secret Service coordinating its internal investigation with the Department of Defense or any other U.S. agency that might have been involved in Cartagena preparing for the President's arrival?

Secretary NAPOLITANO. Mr. Chairman, we are coordinating the investigation with the Inspector General. We have an existing MOA with the IG, between the Secret Service and the IG, so they are, in effect, supervising the investigation even though it is being done by Secret Service agents.

Chairman LEAHY. And was there any evidence that the President's advance team was involved in this misconduct?

Secretary NAPOLITANO. I have not been informed of any such evidence.

Chairman LEAHY. And as we continue to look at this, we know the agents are trained as to what is acceptable and what is unacceptable. Are there standards in place governing appropriate conduct for agents on foreign trips and how they may interact with locals when they are on foreign assignments? And if there are such standards, how are they conveyed to the agents?

Secretary NAPOLITANO. There are standards. They are conveyed through training and through supervision. But one of the things we are doing, Mr. Chairman, is looking at the standards, the training, the supervision to see what, if anything, needs to be tightened up, because, again, we do not want this to be repeated.

Chairman LEAHY. Well, is there training given to agents relating to private or intimate contact with foreign nationals when traveling for security work?

Secretary NAPOLITANO. The training is focused on professionalism, on conduct consistent with the highest moral values and standards, and I think that would include your question.

Chairman LEAHY. Well, Madam Secretary, I know that when we travel, when Members of Congress travel to different countries we go to, we are given security and foreign intelligence threat advisories. I have been in some countries where, for example, we will leave all our communication gear dismantled with U.S. security officers and so forth. Are agents given training in security and foreign intelligence threats for a particular country they might go into?

Secretary NAPOLITANO. I think that is part of the advance process, Mr. Chairman.

Chairman LEAHY. So if they thought there was an intelligence threat in a particular country, they would be advised of that?

Secretary NAPOLITANO. Yes.

Chairman LEAHY. And I began my career here during the cold war period. Some of the assessments we were given then are somewhat different than they are today, but then some of the assessments today because of our increased types of communication gear and electronic gear are different. I assume that is geared based on today's real threats?

Secretary NAPOLITANO. Yes. You mean how to secure our communications equipment and the other types——

Chairman LEAHY. I mean what things an individual must look for. Is this a country that—are they going to be a threat from agents of another country?

Secretary NAPOLITANO. The agents are informed as to what the intel is, what country-specific measures need to be taken. And, again, in this instance, Mr. Chairman, there was no impinging on the security of the President and no access to any secure information by the people involved.

Chairman LEAHY. You know, like you, I have been in many occasions where the Secret Service is around. I have watched very professional men and women. I have traveled with several different Presidents over the course of my career and have watched the Secret Service, again, with very professional men and women there. So when I heard the number of the agents involved in this, I found

it particularly alarming when I got my first call at home from the Director and then as my staff looked into it and the bipartisan staff of the Committee looked into it. I found the numbers shocking.

Do you know, is this the first time something like this has happened, or have you had reports of similar incidences in the past?

Secretary NAPOLITANO. Mr. Chairman, I asked the same question, and over the past 2½ years, the Secret Service Office of Professional Responsibility has not received any such complaint. Over that same period, the Secret Service has provided protection to over 900 foreign trips and over 13,000 domestic trips. So from that standpoint, there was nothing in the record to suggest that this behavior would happen, and it really was, I think, a huge disappointment to the men and women of the Secret Service to begin with who uphold very high standards and who feel their own reputations are now besmirched by the actions of a few.

Chairman LEAHY. Well, and to the extent that any of them are listening to this hearing, I would hope they will not be distracted from their jobs, those who are protecting Governor Romney and those who are protecting President Obama, and all the other protectees. That is going to be their first responsibility.

But then you and the Director have the job of seeing where we go from here. Can you assure us that it will be made very clear to Secret Service agents in their training elsewhere that this kind of conduct will not be condoned?

Secretary NAPOLITANO. That is our goal, Mr. Chairman. There are really three things that I immediately discussed with the Director: one was to make sure the President's security was never at risk; two was to make sure that we instituted a prompt and thorough investigation into the actual allegations in Colombia; and, three, what other steps we need to take for the future to make sure this behavior is not repeated.

Chairman LEAHY. On a different matter, we are going to turn to the reauthorization of VAWA, the Violence Against Women Act. A provision in this year's reauthorization would modestly increase the number of U-visas, the temporary visas available to immigrant victims who have cooperated with law enforcement officers in the prosecution of criminal offenses. Sometimes they are our best sources of information, including domestic violence and sexual assault cases. I have heard from law enforcement all over the country saying they support this.

Does the Department of Homeland Security support this provision of this increase of U-visas for the purpose of cooperating in criminal cases?

Secretary NAPOLITANO. Absolutely.

Chairman LEAHY. Thank you. And I have told you—and I realize I have gone over my time, but we have the question I have raised with you before about the technology used for screening. I was very concerned about the earlier ones that the X-ray type machines that, in effect—my words, not yours—did a virtual strip search of people with very graphic images of the people going through.

Now, those first machines, how much did DHS spend on acquiring them?

Secretary NAPOLITANO. Well, Mr. Chairman, the machines themselves are at a unit cost of approximately $175,000.00 and we can

get you the exact number, but I think the expenditure is probably total, with some installation and other things, about $130 million.

Chairman LEAHY. And then the changes, I am told the changes, after the reaction on the original ones, the retrofits, that upgrades cost about $12 million?

Secretary NAPOLITANO. Well, I am not sure they cost that much because part of the criteria with the vendor was as the software changed, the hardware would be able to accept the software. But I will verify if it was $12 million or not.

Chairman LEAHY. What companies were awarded contracts to provide this?

Secretary NAPOLITANO. Rapiscan and L–3 are the two major vendors.

Chairman LEAHY. Senator Graham, I apologize for taking the extra time. Please go ahead, sir.

Senator GRAHAM. Welcome, Madam Secretary. I have really enjoyed working with your office on things unique to South Carolina and the country's security issues as a whole. My experience with the Secret Service is very similar to what Senator Leahy said. Really, it is basically the time I traveled with Senator McCain during the last Presidential election, and I was very impressed by the people, very hard-working, a lot of time away from families and long hours. So anytime you have military discipline problems, you do not want to paint with a broad brush the 99 percent, and let us start with that baseline.

Secretary NAPOLITANO. I concur, yes.

Senator GRAHAM. But just like in the military, Abu Ghraib and other situations, systems obviously fell then, and obviously there is a system failure here. The likelihood that this was the first and only time that such behavior occurred, do you think that is great or not so great?

Secretary NAPOLITANO. Well, I think part of our investigation is confirming that this was an aberration or not. But I agree with you, Senator. The Secret Service does a marvelous job. I have worked closely with them and——

Senator GRAHAM. The only reason I suggest that we need to maybe look at little harder is because we are lucky to have found out about this. If there had not been an argument between one of the agents and, I guess, a prostitute, for lack of a better word, about money, we would probably have never known about this. So the point is that I think you have got a good order and discipline problem.

Do you believe the agent were confused that their conduct was wrong?

Secretary NAPOLITANO. They should not have been.

Senator GRAHAM. No, I do not think it is a lack of training. I do not think anybody——

Secretary NAPOLITANO. You know, I think the conduct was unacceptable, it was unprofessional.

Senator GRAHAM. Right.

Secretary NAPOLITANO. And as I said in my statement, I think that the people who are most disappointed are the other men and women of the Secret Service.

Senator GRAHAM. I could not agree more, but, you know, human beings being human beings, we all make mistakes, and sometimes organizations can get loose. Being a military lawyer for 30 years, one of the first things that we would advise new commanders, a new squadron commander, is: You have got a bunch of young people in the military for the first time away from home. Go to the barracks 1 day they least expect you to go. Show up at 3 in the morning with the first sergeant, and word will get out pretty quick you have got to watch what you do in the barracks because you never know when the commander is going to show up.

Is there any similar program where supervisors from the home duty station would go out and visit people in the field on a random basis?

Secretary NAPOLITANO. You know, I am not aware of that, which is not to say there is not one. I just do not know the answer. That is one of the reasons that we are continuing our work and want to continue to brief the Committee.

Senator GRAHAM. Could I suggest that you may look at a program very similar to what the military does where people from the command, the central body, would show up on an unannounced basis throughout the world and just let people know that somebody back home is watching. It might do some good in the future.

Is there any exit interviews done for people who are leaving the organization when you ask them, "Does anything bother you, have you seen anything during your time that bothers you?" Because we do that in the military trying to find out how the unit actually works when people are leaving.

Secretary NAPOLITANO. Right, in a civilian agency. Senator, I know there are exit interviews done. Whether that specific question is asked or something like it, again, I do not know the answer, but I can find the answer out for you.

Senator GRAHAM. I would just suggest that maybe we look at changing the system a bit so that people who are away from home never really believe they are away from home, that somebody is always watching.

Secretary NAPOLITANO. Senator, we are looking at this from the aspect of, as I said earlier: one, was the President's security impinged; two, discipline for the agents involved; and, three, what do we need to do to tighten any standards that need to be tightened. So I take your suggestions very seriously.

Senator GRAHAM. Right, and I think this is a bipartisan—you, know, Mr. Sullivan, I have never met the MA, but everybody who knows him seems to have nothing but good things to say about him, and we want to get this behind us and not have the problem emerge again.

Homegrown terrorism, you mentioned that in your opening statement. Would you agree that probably the idea of homegrown terrorism and attack from within is greater today than it was, say, maybe 5 years ago, the radicalization?

Secretary NAPOLITANO. I think that is right. I think we have seen—when I say terrorism continues to evolve, that is one of the evolutions that we are seeing, radicalization—radicalization to the point of terrorist violence—and we have seen several episodes across the United States in the past several years.

Senator GRAHAM. Let us go to the recent tragedy in France where you had a young French citizen, a Muslim, who went to, I think, Pakistan to study at a madrassa there, came back to France and engaged in horrific acts of terrorism. Do you worry about that happening here in the United States?

Secretary NAPOLITANO. One of the things we did in the wake of the Merah incident in Toulouse was to analyze what happened in that case and were there any early signs, indicators, anything that would give us an early tripwire that somebody in the United States was getting ready to do the same thing.

Senator GRAHAM. Well, I think some of these terrorist organizations are actually trying to come to our country and recruit within our own. Is that a fair statement?

Secretary NAPOLITANO. I think there is recruitment. It does not really require a visit. You can do it online.

Senator GRAHAM. That is exactly right. You do not have to come here. But you can talk to our people through the Internet and through the cyber world to try to recruit them to their cause. And, unfortunately, there are some takers, and we need to be vigilant about that.

Now, immigration is—we have got a case before the Supreme Court today. Each person can make their own mind up about, you know, South Carolina, Arizona, and the laws and what we need to be doing. But President Obama in his campaign in 2008 promised comprehensive immigration reform in his first year. Do you believe there was a real genuine effort to make that happen?

Secretary NAPOLITANO. As someone who spent a lot of hours visiting Members of Congress on the Hill to see if there was any room for negotiation of a comprehensive bill, I would say, yes, there was a serious effort.

Senator GRAHAM. So it is Congress' fault?

Secretary NAPOLITANO. Senator, I think all of us have a responsibility to deal in a bipartisan way with a national problem.

Senator GRAHAM. Well, we did not deal in a bipartisan way with health care. Not one Republican in the Senate voted for the health care bill. You had 60 U.S. Senators on the Democratic side. You had a huge majority in the House. So I guess my point is that I do not believe there was much of an effort to deliver comprehensive immigration reform in the first year, and I do not think it is Congress' fault. I think the President failed the country by not making this a priority. He had a large majority he could have worked with, and he chose health care over immigration. And here we are. So not to say that my party is blameless. We are not. But I just want to understand that when people talk about this issue that we remember exactly what happened—60 Democratic Senators, a large majority in the House. Do you remember any bills coming out of the House of Representatives dealing with immigration reform?

Secretary NAPOLITANO. You know, Senator, I am not familiar with any, and I obviously disagree with kind of how you are putting the issue, but I think we can both agree that at some point we are going to have to deal with comprehensive immigration reform.

Senator GRAHAM. Thank you very much for your service.

Chairman LEAHY. Thank you. I would just note parenthetically, I sat in on the meetings with former President Bush on immigration reform. I strongly supported his efforts. I sat in on the bipartisan meetings that President Obama had with some of the same people who were at the President Bush ones in the follow-up, and I recall being told, "Do not bring it up because it is not going to go anywhere. "But I hope, and I still hope, at least while I am still in the Senate, that we will have comprehensive immigration policy. We need it.

Senator Feinstein.

Senator FEINSTEIN. Thank you very much.

Madam Secretary, I am one that thinks you are doing a very good job.

Secretary NAPOLITANO. Thank you.

Senator FEINSTEIN. In an agency that is perhaps too large. I think it is 22 departments and over a couple hundred thousand people. It is a very big job.

I wanted to concentrate my questioning on three areas. The first is student visa and fraud, and earlier last year, I joined in a letter with Senator Schumer on this program, and I am concerned that ICE is not adequately certifying each educational institution. In May of 2011, we have a case of Tri-Valley University in Pleasanton, a sham school certified for 30 students, bringing 1,555 students in, making $4 million. The head is now being prosecuted.

To make a long story short, the United States Immigration and Customs Enforcement, known around here as ICE, wrote an interesting letter on May 3, 2011, saying this: "The student SEVP does not have the statutory authority to close noncompliant schools immediately, nor does it have the authority to restrict DSO access to SEVIS." And it goes on to say they have done a risk analysis of the 6,487 SEVP-certified schools with active records, and they had schools fitting into low-, medium-, or high-risk categories.

Here is the breakdown: Low risk, 4,794, 74 percent; medium risk, 1,276 schools, 20 percent; and then there is high risk, 417 schools, or 6 percent of all the schools examined.

Now, here is what they say: "Many of the noncompliant schools are already the subject of criminal investigations, forestalling any administrative action to limit access to SEVIS to issue the Form I–20. Please know that SEVP can begin immediately such assessments and site reviews once cleared to do so." Can't they be cleared to do this early on?

Secretary NAPOLITANO. I think——

Senator FEINSTEIN. Let me just say one other—I think we have to remember the 9/11 hijackers came in on student visas, went to schools that taught them how to fly but not to land, and nobody thought it was unusual.

So I am really concerned about sham schools and that we have a good sense of who is coming in under a foreign student visa, whether they are attending the school at all. I have been at this, Madam Secretary, for about 12 years, and, you know, initially everybody objected to it. Then they began to do it. Now I see it easing up. And so I wanted to bring it to your attention.

Secretary NAPOLITANO. I share that concern. These sham schools should not be allowed to operate. We have increased our efforts

against them. That particular letter I suspect is that we are coordinating with U.S. Attorney offices in the relevant districts, and they have asked us to postpone administrative action until their criminal case was ready to go. But I will follow up on that.

Senator FEINSTEIN. Can you take a look at it?

Secretary NAPOLITANO. Absolutely.

Senator FEINSTEIN. And let me know.

Secretary NAPOLITANO. Yes.

Senator FEINSTEIN. OK. The second thing is agriculture enforcement audits. Obviously, I have a bias. We have 81,000 farms in California. Virtually all of the labor is undocumented. What happens is in harvest season, canning season, ICE swoops in. We have got a problem. I have tried for 10 years to get an ag jobs bill through, and I cannot get it through. The fact of the matter is that if we want American produce, the labor is generally undocumented, and we have to find a solution to this.

So I am hopeful—and I know that you are doing aggressive I–9 audits of ag employers. I am very concerned that these are going to decimate on-farm and farm-dependent jobs. Do you have any thoughts?

Secretary NAPOLITANO. Yes. I think the base of the problem is that there is no provision under the current immigration law that enables more agricultural workers to be documented. And so we have some employers—and we try to pick those who are really knowingly and intentionally violating the law when they have other options. We are trying to focus on them through the audit process. But the underlying issue goes back to the immigration law itself.

Senator FEINSTEIN. Senator Schumer just murmured to me that most do not have any other options. California is a State that cannot use the H–2A program, the visitor program. So it depends on a large, skilled, rotating, generally undocumented coterie of about 600,000 workers for 81,000 farms. If ICE swoops in, farmers cannot plant, they cannot harvest, they cannot can. And this has been happening. I want to bring it to your attention. You know, it is a hard problem. But if this body will not take action, we are going to put ag out of business, and I am really concerned about it. So if there are any thoughts you might have, I would very much appreciate them.

And the last point I wanted to raise with you is another longstanding issue of mine, and it is the Visa Waiver Program and biometric exit. For many years I have been trying to get data on visa overstays for each country, to no avail thus far. Last month, DHS Assistant Secretary David Heyman informed me that by June of this year, DHS will have a fully operational biographic exit system in place. It is going to provide real-time information on those who exit United States airports. This new exit system is expected to allow you to calculate overstays per country by May of this year. Here is the question. I think this is very important because we have got 15 million people that come in every year, and we do not know whether they leave or not on a visa waiver. Is DHS on track to have a fully operational biographic exit system by June of 2012?

Secretary NAPOLITANO. Senator, I believe we are. The final plan is in the clearance process with OMB, but that is our intent.

Senator FEINSTEIN. Good. Will DHS be able to provide overstay rates per country by May of 2012?

Secretary NAPOLITANO. We should be able to provide some of that information, if not all.

Senator FEINSTEIN. Good. Thank you.

Chairman LEAHY. Thank you, and what we will do now, we will go to Senator Grassley. Senator Kyl would have been next, but—no, we will go to Senator Kyl next. Senator Grassley would have been next, but he is yielding to Senator Kyl, which is fine with me, and then we will go to Senator Schumer.

Senator KYL. Thank you, Mr. Chairman. Thank you, Senator Grassley.

This is not the first time that Senator Feinstein and I seem to have been thinking about exactly the same thing, so let me just quickly touch on the three things that she mentioned, which were also of concern to me.

On student visas, I think it is not just a matter of the sham schools but also the failure of ICE to follow up with students who have overstayed their visas and the very poor record of schools providing information to ICE.

Second, on the ag workers, the H–2A regs could be reformed. It is not just a matter of our failure to pass legislation here. H–2A regulations were reformed toward the end of the Bush administration. They were more workable, I am told. That was then changed with the Obama administration. If we could work more toward the kind of regs that existed toward the end of the Bush administration, I think that might be at least a help for some.

And on the visa overstays and the exit system, I was going to ask about that. I think your budget actually was denied $30 million by the Appropriations Committee because of its frustration with the lack of a plan. We need to get that plan implemented as well as up here.

Let me go on to——

Secretary NAPOLITANO. If I might, Senator.

Senator KYL. Yes, sure.

Secretary NAPOLITANO. Can I talk about the visa overstay issue with you a bit?

Senator KYL. Sure.

Secretary NAPOLITANO. One of the things that we have done over the last few years is we have added data bases and been able to link them so that before visas are issued, there is a check against our data, NCTC's data, and certain NSA data. We have done now the same thing. We have gone backwards to find visa overstays, and we have looked at and prioritized those that provide any kind of public safety or security risk. And we have now looked at the entire backlog, and I will give you the inventory of what we have found, and we are prioritizing those visa overstays within ICE.

Senator KYL. I understand that. What is your estimate now, just approximately, of the number of the visa overstayers as a percentage of the total of illegal immigrants in the country today as opposed to those who have crossed the border illegally? The number you usually hear is around 40 percent. Is that——

Secretary NAPOLITANO. That may be a high number because what we have found is a lot of people who were marked as visa overstays had, in fact, left.

Senator KYL. So 40 percent might be too high an estimate? That is the number that is usually given when we complain about the lack of security at the border. They say, well, remember, 40 percent of the people here illegally is actually overstayed visas. You think that number is a little high.

Secretary NAPOLITANO. It may be a little high.

Senator KYL. All right. In either event, it is a big problem, and it is fine to prioritize for criminals, but that is a very small percentage of the people who have overstay visas.

Secretary NAPOLITANO. Senator, what we have done is say, look, we have to make the best use of those ICE resources we have and pick up——

Senator KYL. Well, that is fine, Madam Secretary. Excuse me for interrupting, but every year I say if you need more resources, ask for them. "No, we have got everything we need." And then the excuse of not moving forward on something is, "We do not have enough resources." You cannot have it both ways. If you need more resources, ask for them.

Secretary NAPOLITANO. Senator, thank you. As you know, we are all working under the constraints of the Budget Control Act. That is the deal that was struck. But to your point, yes, and to Senator Feinstein's point, yes, we believe visa overstays are a keen interest.

Senator KYL. So do we, and we appreciate that.

Another very parochial but very important point, and I know you appreciate this. Every time I go to the border, the first thing people talk about is not illegal immigration. It is the incredible delays at the ports of entry. We need a lot of things, including more officials at the border on the American side. That is not the total solution to the problem. A lot has to do with the inadequate link-up on the Mexican side of the border. But at the Mariposa point of entry and San Luis, both of which I know you are intimately familiar with, we need more agents. That is what they tell us down there. And yet that was not in the budget request.

I would just ask you to please either ask for the agents that we need there—and this is just to facilitate commerce between the two countries.

Secretary NAPOLITANO. Yes.

Senator KYL. And to make life a little bit easier for people that have to cross every day. Either ask for it in the budget or find some other place where we can get it or make a recommendation to us as to how we can move money around to provide for those additional agents. The estimate at Mariposa, for example, is about 250. It does not seem like that many. We ought to be able to find the money for that. Would you agree to help try to work with us on that?

Secretary NAPOLITANO. We will definitely work with you on that, Senator.

Senator KYL. I appreciate it, because I know you know the problem.

Secretary NAPOLITANO. Very well.

Senator KYL. And it is not a partisan problem. We all agree we need to resolve it.

Secretary NAPOLITANO. Well, and we want to facilitate that trade and commerce.

Senator KYL. Absolutely.

Secretary NAPOLITANO. There are a lot of jobs depending on it.

Senator KYL. Absolutely. Now, the last point that I wanted to make, 6 months ago you were written a letter, and then another 3 months ago, about the lack of enforcement of Federal detainers, specifically, for example, in Cook County. Last night, at 6:30, we finally received a response to our letter, and it certainly is a good response in terms of pointing out the problem. Where I fail to see the response is in what you are doing about it other than writing letters.

This letter, dated April 24th, from Nelson Peacock, I will ask unanimous consent to put in the record because, as I said, I think it lays out the problem from ICE's perspective and your perspective very well.

[The letter appears as a submission for the record.]

Senator KYL. Cook County is simply not abiding by Federal law in detaining officials who have criminal records that you have asked them to detain. For example, since the ordinance was enacted, ICE has, according to this letter, lodged detainers against more than 432 removable aliens in Cook County's custody who have been charged or convicted of crime, including serious and violent offenses. Cook County has not honored any of these 432 detainers, and they point out a case of particular gravity recently reported in the Chicago Tribune. And Mr. Peacock notes that this probably violates Federal law.

The only action that I can see taken here is that two letters have been written, and Cook County has been encouraged to change its policy and has been advised that if it continues this policy, it may result in denial of reimbursement to the State of costs under the SCAP program.

You know, the Federal Government has been very aggressive in filing lawsuits against States that are trying to actually do something about illegal immigration, but it does not look to me like the Government is doing that much to enforce the law that currently exists with respect to detainers. What more do you plan to do with entities like Cook County who are obviously flouting Federal law and jeopardizing American security in the process.

Secretary NAPOLITANO. Yes, I agree. I think Cook County's ordinance is terribly misguided. It is a public safety issue. We are evaluating a lot of options right now. You know, we always start off trying to work with the local authorities and work things out. We to date have had no success there, so we are evaluating all options.

Senator KYL. And I hope more than evaluating, you will take some action pretty soon. Will you report to us as soon as you have decided what kind of action to take, just kind of keep us advised rather than waiting for correspondence from us?

Secretary NAPOLITANO. We will keep the Committee staff—I think that is probably the best way to do it—advised of how we are proceeding there.

Senator KYL. I appreciate that very much.

Thank you, Mr. Chairman.

Chairman LEAHY. Thank you, Senator Kyl.

I would also note that today is Senator Kyl's birthday.

Senator SCHUMER. Oh, happy birthday.

Chairman LEAHY. Happy birthday to you. Please do not sing.

[Laughter.]

Senator KYL. That is one thing you and I can agree on.

Senator SCHUMER. Last birthday as a Senator.

Chairman LEAHY. It is his birthday, and I appreciate him being here.

Senator Schumer.

Senator SCHUMER. Thank you, Mr. Chairman. I wish Senator Kyl a happy birthday. I guess it will be the last one as Senator, so your next birthday may be even happier than this one.

[Laughter.]

Senator KYL. But I will miss you.

Senator SCHUMER. Thank you. Mutually, seriously. Senator Feinstein and I were just mentioning that a second ago.

First, two points of housekeeping. Good news for you. I am not going to ask you any questions on the Secret Service. I have a lot of faith in your ability to get to the bottom of this. All of us are shocked and terribly troubled by it, but I think the kind of investigation you and your Department will do I have a lot of faith in.

Secretary NAPOLITANO. Thank you.

Senator SCHUMER. Second, Senator Feinstein mentioned the student visa issue, and I believe she mentioned—I came in in the middle of her testimony, unfortunately. She and I have asked for a GAO report, which is coming out in about a month, and our Subcommittee on Immigration with the Chairman's permission will have hearings on that GAO report when it comes out. So I will let you know about that.

I have two questions here on other issues in your vast jurisdiction. The first relates to passenger advocates. Over the past several months, there have been an increasing number of news stories about passenger complaints over TSA screening procedures, and these complaints include, for instance, a female passenger being told she could not carry her breast pump on board the plane while the milk bottles were empty, imagine how her child is that way; asking female passengers to submit to repeated inspections through body scanner machines for non-security reasons; asking elderly and disabled passengers to remove critical medical equipment and undergo strip searches prior to clearing security.

I like the TSA, and I think they do a good job, and I was involved in setting them up. It is a hard job to balance security and commerce, but you can always make it better without one impeding the other. TSA's original response at the lower levels here was to first deny wrongdoing and then issue apologies. So in light of these incidences, Senator Collins and I decided to introduce legislation called the Rights Act, and the Rights Act will help curb abuses in the TSA screening simply by requiring the TSA ombudsman office to establish a Passenger Advocate Program to resolve public complaints and conduct training of TSA officers to resolve frequently occurring passenger complaints. It would also require that every Category X airport—is that Category X or 10? Big airport. Let us

strike Category X. It is a funny category. What are A through V? We do not know.

Anyway, every Category X airport to at least have one TSA passenger advocate on duty at all times. So if somebody is faced with the choice, they are lined up, they are asked for an intrusive exam, they think that is uncalled for. I do not expect every TSA agent to be schooled in each thing, but if, you know, at Kennedy Airport, a large airport that handles tens of thousands a week, there is someone who is trained who can just come over within 10 minutes—just one, no new people, no new cost, one of the existing employees who knows about how to do this and can resolve a sticky situation. It avoids the passenger the choice of undergoing an examination that they think is intrusive or humiliating or not going on the flight.

So do you support the creation of passenger advocates at airports? And will you work to roll those out at airports without the need for an act of Congress?

Secretary NAPOLITANO. Absolutely. And if I might, just to go through, first, as you know, TSA I think does a very good job, and it is a very difficult job.

Senator SCHUMER. Right.

Secretary NAPOLITANO. You know, every morning I start my morning with a threat brief of what is facing us in the evolving world of terrorism, and aviation security still remains the No. 1 threat. But we have taken steps to try to make it less onerous. We have taken those over 75, children under 12 out of the routine lines. The breast pump incident you mentioned was not in accord with how we do that, and the employee received appropriate retraining. So we keep trying to do that.

But the idea of having cross-trained advocates among our TSA personnel in the Category X airports is something we support and TSA is already moving toward that goal.

Senator SCHUMER. That is great news. Thank you, and it will avoid Senator Collins and I having to pass legislation, which is good.

Secretary NAPOLITANO. Well, we are happy to keep you informed of——

Senator SCHUMER. Since legislation moves so quickly these days through the Senate.

OK. Second is a parochial issue but of great importance to western New York. It is the Niagara Air Force Base, air base. I want to ask you about the possibility of constructing a new Border Patrol station at Niagara Air Base to replace the existing Niagara Falls Border Patrol station. As you know, the existing station is insufficient for your current needs. We all agree to that given all the new security. We have had terrorists cross over the Buffalo border. It lacks the capacity needed to accommodate the number of agents now housed at the station. It does not have the space and resources your agents need to do the job.

A new station at Niagara Air Base can comfortably accommodate 50 agents, could be modified to accommodate even 75. It will also include critical items that the Border Patrol needs, such as the main administration building will be suited for mustering and training, will include an armory and necessary storage space, ancillary buildings that will house vehicle maintenance, enclosed park-

ing, and kennels. Obviously, we have the dogs at the border, too. This new station would be a win for the Border Patrol and the Niagara Air Force Base, whose mission is being curtailed because of the cutbacks in the military.

Would you support the creation of a new Border Patrol station at the Niagara Air Base?

Secretary NAPOLITANO. Niagara is very much under consideration, Senator. The issue is money for construction of a new facility, but certainly Niagara is under consideration.

Senator SCHUMER. OK. So, in other words, you think it is a good idea to have it there, and we have to find the funds for it.

Secretary NAPOLITANO. That is one way to put it, yes, sir.

Senator SCHUMER. Yes. I like the "yes" part of that answer. Thank you.

Mr. Chairman, I am finished with my—I would yield back my remaining time.

Chairman LEAHY. Senator Grassley.

Senator GRASSLEY. Thank you, Mr. Chairman.

First, just a statement. I wanted to give you an update on some of the—well, first of all, I want to put a statement in the record. I was going to have a long statement.

Chairman LEAHY. Without objection, so ordered.

[The prepared statement of Senator Grassley appears as a submission for the record.]

Secretary NAPOLITANO. Senator, I do not know that your microphone is on.

Senator GRASSLEY. I am not talking into it. That is the problem.

Secretary NAPOLITANO. Thank you.

Senator GRASSLEY. I an surprised you want to hear me, but thank you.

[Laughter.]

Senator GRASSLEY. First, an update. About 99 percent of the time when I write you, I do not get a response directly from you. The response comes Leg. Affairs.

Second, and more frustrating, many times my questions are rarely, if ever, answered.

Third, the delays are unacceptable, and just last night, I received a response from the Department about Cook County 6 months after my initial letter of inquiry. And, also, you just responded to questions we posed at the last Judiciary Committee oversight hearing, which took place last October. That is just to bring you up to date. That is not a question. I do not want a response to that.

Both the Chairman and I want to get to the bottom of this Secret Service matter, and I know the Chairman has covered a lot of the issues I wanted to cover, so I am not going to go back over that, and I thank the Chairman for asking those questions.

I was briefed by the Secret Service Director, and he responded about the Inspector General being involved, and I have asked for that involvement. But he said he was already involved before I asked for it, so I compliment Director Sullivan on that.

Director Sullivan has included the Inspector General in the investigation up to this point, but I want to know if the Inspector General is truly conducting an independent and impartial investigation. I think the same independent investigation is necessary

from the Inspector General in Defense and from the White House to get to the bottom of the story for all the advance team staff that was in Colombia.

In previous answers to questions, you mentioned that the IG is supervising the investigation. Do you agree that the Inspector General should conduct a full-scope investigation to determine if this is a cultural problem routinely occurring in additional cities instead of just reviewing what occurred in Colombia? Question No. 1.

Question No. 2: Do you have any reason to believe that the Inspector General is not receiving full and complete access to the Secret Service investigation?

And, three, you referred to previous answers that, as far as you know, in the last 2½ years this has not been a cultural issue. Why do you keep saying just 2½ years? And don't you think we ought to make sure before 2½ years that it was not a problem as much as not being in the last 2½ years?

Secretary NAPOLITANO. Yes, Senator. Let me address that. I use that timeframe because, you know, we are going back now through all of the records, and we have gone back that far, probably even further at this point.

Senator GRASSLEY. OK.

Secretary NAPOLITANO. In terms of the IG's involvement and supervision of the investigation, I am sure the IG would be willing to answer those questions. But we have an MOA, a Memorandum of Agreement, with the IG and the Secret Service that they are—in these kinds of cases where there is alleged misconduct, they actually—"they" meaning the IG supervising the investigation, but they use the investigatory resources of the Secret Service. That is how we are managing this one, and I believe the IG has been with the Director during the Congressional briefings to confirm that point. So we expect the IG to be conducting a full investigation.

Senator GRASSLEY. OK. On another matter dealing with cybersecurity, specifically one cybersecurity proposal would place at your Department the lead agency in overseeing regulations for covered critical infrastructure. I have concerns about this proposal because it creates a new regulatory bureaucracy. I am also concerned that this new regulatory power giving DHS background on overseeing the chemical facilities security, CFATS program. Congress gave your Department regulatory power over chemical facilities. Regulations were issued in 2007. Five years later, nearly 4,200 chemical facilities have complied with the regulations, but your Department has yet to approve a single security plan, so far spending half a billion dollars and not getting anything approved.

I have obtained a copy of an internal review by Under Secretary Rand Beers by two subordinates that details the problems DHS faces in implementing CFATS. This memorandum is the most candid review of a failed Federal Government program I have seen. This memorandum details failures at an unprecedented level, poor hiring, hiring people not skilled, poor staff morale, management leadership failures, lack of subject matter expertise, union problems, and "catastrophic failure to ensure personal and professional accountability."

The memorandum also states that inspectors lacked expertise to effectively evaluate site compliance with cybersecurity requirements. On top of this memorandum, the Department has failed to implement ten outstanding GAO recommendations.

So taken together, these reports paint an agency that cannot control costs, manage employees, and effectively implement the mission. If it costs DHS $480 million to effectively regulate zero chemical facilities, how much can we expect that it costs the taxpayers for the Department to regulate cybersecurity among thousands of private businesses?

Secretary NAPOLITANO. Senator, let me take those issues, both of them. First, the CFATS, or chemical facilities, yes, we did a candid internal review because we were not satisfied that we were achieving the results that we need to achieve, which is the safety and security of our chemical facilities and the possible security issues with them. We now have a very aggressive corrective plan in place. I would be happy to brief you or your staff on that. We have been approving site-specific plans. If they are not at final approval, they just about are. But that process is really moving forward with great alacrity. So we have learned a lot from CFATS, and we are fixing those problems. We have put new people in charge, done all the things one needs to do to make sure that a program moves forward effectively.

With respect to cyber, this is an area where our deep concern is that the Nation's core critical infrastructure on which farmers depend and small business depend and everyone depends is very susceptible to attack, and the attacks can occur in a variety of ways. And we are seeking some means to, A, have basic performance standards by that core critical infrastructure, have real-time information sharing so that we can swiftly move in to help mitigate and share information if need be, and we are actually asking the Congress to give us some hiring authority so it is easier for us to hire people who are experts in the cyber field.

So as the Congress begins to consider and the Senate begins to consider this legislation, we hope they do it in the sense of what the risk posed is really to the country right now.

Senator GRASSLEY. OK. Thank you.

Chairman LEAHY. Next, Senator Klobuchar.

Senator KLOBUCHAR. Well, thank you very much, Mr. Chairman, and thank you, Secretary Napolitano, for being here and the good work that you have done. I share in Senator Feinstein's views that you have done a good job with very difficult challenges.

I also wanted to thank you for being here to answer questions about what happened in Colombia. In my old job as a prosecutor, I had very positive interactions with the Secret Service, and I am hopeful that the actions of a few will not overshadow all of the good work that they do every single day.

Secretary NAPOLITANO. Indeed.

Senator KLOBUCHAR. But I do want to ask some questions about that because I think it really shook the trust of a lot of people, and I think the way you make sure that the actions of a few do not overshadow the actions of many, the good actions and how they sacrifice their lives every day and put them on the line, is by making sure that we clear up what happened, but also make sure that

it does not happen again, and that we have a clear understanding of what is going on.

I know one of the Senators asked about this, but there was a Washington Post report recently that talked about the fact that this may have been going on before. In fact, one of the—the person is not identified, but one agent that was not implicated in the matter remarked that, "Of course it has happened before. This is not the first time. It really only blew up in this case because the U.S. embassy was alerted." And I just wondered if you could comment on that, how you think we need to move forward, and how—to me, this does seem to create a risk when you are in a country like Colombia and you have people doing things where they could potentially be bribed. If you could just generally comment about that.

Secretary NAPOLITANO. Right. Well, again, the actions were unacceptable, and they were unacceptable taken by themselves. I think every mother of a teenager knows that a common defense is, "Well, everybody else was doing it, you know, so I get to do it. "First, not everybody else was doing it. And, second, this behavior is not part of the Secret Service way of doing business. They are very professional.

But we are going to get to the bottom of this. We are going to make sure that standards and training, if they need to be tightened up, are tightened. And we have moved with great speed to deal in a disciplinary fashion with the 12 agents involved.

Senator KLOBUCHAR. I do not expect you to reveal things that are not public, but have there been other incidences where people have tried to bribe or blackmail agents because they believed or they had some kind of interaction with prostitutes or someone with some kind of illegal activity?

Secretary NAPOLITANO. Senator, I am not aware of any. As I said before, the Office of Professional Responsibility in the Secret Service went back 2½ years. That covers 900 foreign trips and 13,000 domestic trips and did not have in that period any kind of a complaint. That does not, obviously, include the IG. That is an independent entity. But we are looking to see and make sure this was not some kind of systemic problem and, most importantly, to fix it.

Senator KLOBUCHAR. And there was one agent that was in the President's hotel. Is that correct? That was also—that was just identified?

Secretary NAPOLITANO. I believe that is correct.

Senator KLOBUCHAR. OK. Another question on a completely different incident, and I think every employer has had incidences of people posting things on the Internet and pictures of them, like maybe in their boss' chair drinking a beer. That happened to me 5 years ago with an intern. It was innocent, but—I think he never thought we would see it. But these are things that happen. But when they happen with law enforcement, it seems a step above and I think much more of a security risk.

I know that recently one of the Secret Service agents has reportedly posted photos on Facebook depicting himself on duty protecting—I think it was then Vice Presidential candidate Sarah Palin. Could you talk about the Secret Service rules regarding agents sharing details of their assignments, online or otherwise?

And does the Secret Service have policies regarding agents' use of Facebook and other social media websites?

Secretary NAPOLITANO. Yes, we do have a social media policy, and we would be happy to provide you with a copy of that. And, yes, to the extent there was such a posting, unprofessional and unacceptable.

Senator KLOBUCHAR. OK. Very good.

I wanted to ask you a little bit about, you know, we are working very hard on cybersecurity initiatives here going forward, and can you talk about how Homeland Security is currently working with State and local law enforcement to prevent and mitigate cyber threats and discuss the Stop, Think, Connect campaign and your efforts to educate the public on the role that they have to play in this important fight?

Secretary NAPOLITANO. Right. We are trying, just as we have the See Something, Say Something campaign, Stop, Think, Connect is one of our efforts to educate the public about everyone's shared responsibility who is on the Internet. Everyone has a responsibility to have good cyber habits. Just like when you get in a car, you should buckle your seat belt, it should be reflexive above anything else. So we continue to push on that.

With respect to our coordination with State and local governments, we do that quite a bit, Senator. We have the NCIC out of Northern Virginia. We actually have representatives on the floor. That is our 24/7 watch center where cyber is concerned. So we are working with them very extensively on that.

Senator KLOBUCHAR. Very good. And now turning to our borders, I am Chair, as you know, of the U.S.-Canadian Interparliamentarian Group. They are actually coming to Washington next month, and I know you have been working on some cross-border crime issues. But I did want to thank you for an issue that I have been raising for a few years, and that is the issue of the Canadian baggage screening, which has finally been resolved as part of the Beyond the Border Action Plan. So thank you for working on that.

And then I wanted to ask—I know Senator Schumer asked some things about the TSA. Again, I understand that there are always incidences that need to be resolved and new things come up. But overall I think they also, like yourself, have a very challenging job, and I have been proud of the work that they do, at least in the Minneapolis airport where I work with them. You just brought in the PreCheck Pilot Program in our State. Do you know how that has been going?

Secretary NAPOLITANO. The PreCheck Pilot Programs are very popular. This is the domestic branch of the kind of Trusted Traveler programs that we began with the Global Entry Program internationally. So we are expanding that PreCheck Program as rapidly as we can.

Senator KLOBUCHAR. Very good. And then, last, the JOLT Act, I would just call your attention to that. This is bipartisan legislation that we have introduced with Senators Schumer, Rubio, Blunt, Mikulski, Kirk, and Lee, and I think it is very important to move ahead with that. We have appreciated some of the work you have done on tourism, and as you know, we are working with the State Department to improve the visa wait times. But there are also

other things that we can do that are contained in this Act, so we would love to have your help and support with that bill.

Secretary NAPOLITANO. I would be happy to take a look at it.

Senator KLOBUCHAR. Thank you.

Chairman LEAHY. Thank you.

Senator Cornyn.

Senator CORNYN. Thank you. Madam Secretary, good morning.

Secretary NAPOLITANO. Good morning.

Senator CORNYN. Good to see you. We can all stipulate you have an extraordinarily challenging job. I want to ask you a question about DNA testing of detainees, and I know you are a former Federal prosecutor and Attorney General, so you know how powerful a tool DNA can be in a law enforcement investigation.

As a matter of fact, to digress a moment, we are going to have an important Violence Against Women reauthorization on the bill probably this afternoon or tomorrow, and I am offering a bipartisan amendment that will address the 400,000 estimated untested rape kits that currently are sitting in police lockers and elsewhere, which, as we all know, is a powerful tool to help identify what in many instances are serial perpetrators of sexual assault. But let me bring you back to 2005. Senator Kyl and I sponsored the DNA Fingerprint Act during the last reauthorization of the Violence Against Women Act. This legislation gave Federal law enforcement authority to collect small DNA samples from all Federal arrestees and detainees, just like we take fingerprints but, as you know more accurate.

These DNA samples, again as you know, can be checked against the FBI's nationwide DNA data base, CODIS, to determine whether the arrestee or detainee has committed other crimes perhaps in other jurisdictions. So far, CODIS, we are told, has assisted law enforcement officials with more than 169,000 investigations, including 10,000 in my State of Texas. So we have seen it to be a powerful tool.

At your 2009 confirmation hearing, I asked if you would see to it that the alien deportee DNA testing regulations were fully and promptly implemented by the Department, and you replied, appropriately, that DHS will fully comply with the applicable statutory and regulatory framework.

Nearly 3 years after the hearing, how do you feel like that is going?

Secretary NAPOLITANO. Well, I think, Senator, we have deported a record number of individuals, as you know. I will be happy to go back and look at all the regulations governing that to make sure we are in compliance. But we have had a very aggressive plan to deport those who should be removed from the country.

Senator CORNYN. And my question is a little more narrow because what we want to do is identify whether these detainees have perhaps committed other crimes and aid those law enforcement agencies in the course of those other investigations, not just enforce the immigration laws, which is important but is not the complete rationale.

Would you be willing to on a voluntary basis submit to the Committee sort of the Department's evaluation of how it has complied

and handled this requirement of 2005 into the DNA Fingerprint Act?

Secretary NAPOLITANO. I would be happy to supply that.

Senator CORNYN. That would be very helpful.

[The information referred to appears as a submission for the record.]

Senator CORNYN. Let me tell you the reason for my concern. Of course, we know the FBI has used a great deal of taxpayer money and crime lab resources to prepare for hundreds of thousands of DNA samples as a result of the passage of this Act in 2005. We are told that the FBI is prepared for and expected to receive between 120,000 and 240,000 samples from the Department of Homeland Security in the year 2012. To date, they report only having received 4,000 samples. So I hope you will help us——

Secretary NAPOLITANO. Yes, let us get to the bottom of that.

Senator CORNYN.—identify what the disparity is between the number of samples and the number anticipated by the FBI as a result of this, because while I am aware that, for example, in Afghanistan and Iraq, when our military captures high-value detainees, they do get biometric identifiers from them that could be used, can be used by law enforcement agencies and the Department in the United States when identifying people coming across, let us say, the southwestern border without the appropriate visas to make sure that they are not coming in to commit acts of terrorism and other violence. It——

Secretary NAPOLITANO. Senator, if I might, that is a somewhat different question.

Senator CORNYN. It strikes me that this DNA evidence—and I will be glad to let you answer.

Secretary NAPOLITANO. Sure.

Senator CORNYN. That this DNA information would be vitally important and enormously useful not only in assisting your Department in terms of border security and immigration enforcement, but also to help law enforcement, writ large, in terms of identifying people who come into the country and commit crimes that currently are unsolved. Please go ahead.

Secretary NAPOLITANO. Thank you, Senator, and I did not mean to interrupt. But we do run illegal immigrants against a variety of data bases, and I think I should supply you with that information. And then I will look specifically into the issue of DNA with the FBI.

Senator CORNYN. To my knowledge—and I will look forward to your report—that is more in the nature of fingerprint and other biometric identifiers and does not extend—did not extend to DNA testing of detainees until Congress passed the DNA fingerprint law in 2005. So you understand, I know, the issue, and I would very much welcome your response to me and the Committee so we can help get to the bottom of that.

Secretary NAPOLITANO. Good.

[The information referred to appears as a submission for the record.]

Senator CORNYN. Mr. Chairman, I will yield back my remaining time. Thank you.

Chairman LEAHY. Thank you very much, Senator.

Senator Whitehouse.

Senator WHITEHOUSE. Thank you, Mr. Chairman. Welcome, Secretary Napolitano.

Secretary NAPOLITANO. Thank you.

Senator WHITEHOUSE. Just one question on the Secret Service episode. What opportunities did this behavior create for compromise of the President's security, for instance, had the prostitutes had connections with Colombian criminal networks or foreign intelligence services? I am not saying that it did, but it seems like it is the kind of behavior that would render an agent vulnerable to blackmail and influence if criminal networks and foreign intelligence services were aware of it and that is a potential avenue for compromise of the President's security.

Secretary NAPOLITANO. Senator, we are still completing the entire investigation, and there are still interviews to be conducted. But I think we have planned to keep the Committee briefed on what we find and whether there could on a future basis be that kind of risk. But as I testified earlier, the first question I posed to the Director was: Was there any breach to the President's security in this instance? And the answer was no.

Senator WHITEHOUSE. But there was a risk of breach along those lines if those connections existed, correct?

Secretary NAPOLITANO. There may be a risk, and that is why this behavior cannot be tolerated.

Senator WHITEHOUSE. Yes. Let me switch to cyber, and let me thank you for your energetic work and persistence on this issue as we in Congress try to pass the legislation that we need.

There are a variety of different approaches that are being looked at here. Let me ask you this: If we were to pass a bill that failed to protect American critical infrastructure in private hands, like our electric grid, our financial processing systems, our communications networks, and so forth; and, indeed, if that bill even failed to define critical infrastructure or provide a process for defining critical infrastructure so we actually knew what it was and what it was not, how well would that bill have met the threat that you see us facing in this realm?

Secretary NAPOLITANO. Well, it would leave a significant gap given the kinds of attacks we already see. That is why we think the Nation's core critical infrastructure should have some basic performance standards to meet. That is why we think a bill needs to have real-time information sharing in it and incentivize that information sharing. And so those are the kinds of things that really should go into a comprehensive cyber bill.

Senator WHITEHOUSE. And would you be able to say that the national security needs of the United States had been met by a bill that did not include any protection for our critical infrastructure?

Secretary NAPOLITANO. Senator, I would say based on what we know now and the risks that we already see now and the kinds of attacks that we already see now, the failure to address core critical infrastructure would be a significant gap in any legislation.

Senator WHITEHOUSE. Thank you.

My last question on this same subject, but switching from the national security and public safety side of cyber attack to the intellectual property and economic competitiveness side of our cyber vul-

nerability, I said about 2 years ago that I thought we were on the losing end of the biggest transfer of wealth in the history of humankind through theft and piracy because of the attacks on our industrial base and our technological base from overseas for the purpose of industrial espionage and stealing intellectual property. Since then, General Alexander has used virtually the same language. McAfee has issued a report that uses virtually the same language. Mike McConnell has used virtually the same language. This is a very big deal for us from the point of view of economic competitiveness, and you have been an Attorney General—in fact, we were Attorneys General together. You have been a U.S. Attorney. In fact, we were U.S. Attorneys together. You have had a lot of experience with law enforcement, also as Governor and in your role as Secretary of Homeland Security.

I do not yet believe that we are resourced adequately in law enforcement to address that aspect of our cyber liability. And I hear from companies in all sorts of industries that when they can get, for instance, the FBI's attention, they are very impressed with the capabilities that are involved. But it is very rare that you can turn over a case of intellectual property theft to the FBI and say go. They simply do not have the staff. They simply do not have the resources, as much as this part of law enforcement has grown both in U.S. Attorney's Offices and at the FBI.

So I would like to ask that you participate in discussions that we are going to be having around the cybersecurity legislation about how we should better organize our cyber resources. It is both criminal and civil because a lot of what gets done is done through civil law. The Coreflood botnet was taken down by a civil case. A lot of the cleanup on the Net of crooked websites can be done through civil proceedings. But it is a law enforcement function because you are getting rid of very bad actors on the Net who are attacking American businesses and the American economy.

So that was a little bit more of a speech than a question, but what I would like to do is to invite you to, based on your experience, participate in that discussion. I do not know if we need the equivalent of a cyber DEA or ATF, an entire organization, or if we need the equivalent of a cyber OCDETF, a different way of organizing law enforcement activity, or whether we need the cyber equivalent of an Organized Crime Strike Force. Those were set up many, many years ago, and there are a variety of different structures, but I do not think the private sector is getting the support it needs from law enforcement because of lack of resources, and there is an awful lot of money going out the door. We are standing by one of the biggest robberies in history, and I would love to have your support in pursuing that concern.

Secretary NAPOLITANO. Senator, first of all, I agree with your statement of the scope of the problem. It is severe, it is endemic, and it is a transfer of wealth, as you put it. We work with the FBI, Secret Service and ICE all have cybersecurity and do criminal cases in that area as well as some others. So I would be happy to participate as we—I think in the context of comprehensively looking at the protection of the country in cyber, how we organize our law enforcement resources and make sure particularly the FBI has

what it needs to handle some of this work is a good question, and I would be happy to participate.

Senator WHITEHOUSE. I appreciate it.

Chairman, thank you very much.

Chairman LEAHY. Thank you.

Madam Secretary, as you have noticed, we have had Senators on both sides of the aisle that have come in and have left during this hearing because most of us have about three different Committee meetings going on. You do not get that luxury, and I do want to applaud you, one, for keeping your answers as brief and to the point and, I might say, as accurate as you have, which is typical of your appearance, and I appreciate that.

I am going to have to leave. I would just note that Senator Lee will go next. I am going to turn the gavel over to Senator Coons. I am doing this so that we are trying to keep similar hairlines——

[Laughter.]

Chairman LEAHY. Sorry about that. But Senator Coons has worked very, very hard on this subject, and I have asked him to take over as Chair. We will go to Senator Lee next, but I do appreciate what you said.

I would add—and I think I can speak for Senator Grassley and others here—we would want to keep in touch with you and the Director of the Secret Service as this whole matter goes on, not just on what has happened now, but what is happening in the future and what will happen in the future. We will do it because of our obvious oversight interests and the need to do it, the protection of key people, in this case in a Presidential election year, both the President and the Republican nominee, but also because we have so many good men and women in the Secret Service that I hope we will be able to demonstrate that if there are a few bad apples, they are weeded out so that the others who are extraordinarily dedicated, highly trained professionals can continue on the work they do.

Secretary NAPOLITANO. Absolutely.

Chairman LEAHY. Senator Lee, thank you for that. Please go ahead, sir.

Senator LEE. Thank you, Mr. Chairman, and thank you, Secretary Napolitano, for joining us.

In March of this year, John Cohen, who I believe is your Principal Deputy Coordinator for Counterterrorism, testified before a House Subcommittee that the Department should have a biometric exit system designed and ready to go—at least ready to roll out, and announced and described some time within the next few weeks, in the coming weeks. In your written testimony today, I believe you said that a biometric exit system should be ready for deployment and use within 4 years. How confident are you about that timeframe?

Secretary NAPOLITANO. What we are planning—and, Senator, the actual plan is in final clearance with OMB so it should be out shortly. But given our ability now to do enhanced biographic exit, immediately moving and deploying that, and then we will move and use that as the platform for adding on the biometric. But the plan is done from our standpoint. We are just working through the final nuts and bolts with OMB.

Senator LEE. And why does it take so long to get it deployed? Is it just the development of a technology? In other words, the fact that it takes 4 years to get it going, is that——

Secretary NAPOLITANO. Well, it is cost, it is the scope of the issue. We have so many ways that people can exit the United States. We are very different from other countries in that regard. And manpower and other resources, yes.

Senator LEE. What kind of an impact do you think this will have on visa overstays once you get it deployed?

Secretary NAPOLITANO. I think it will help us, although we have already used our enhanced biographic to go backwards to identify overstays and to prioritize those that we want ICE to really focus on finding and removing.

Senator LEE. Can you give us any sort of brief specifics, a brief thumbnail sketch on how the system will work?

Secretary NAPOLITANO. I would prefer to do that in a classified setting, Senator, and we would be able to do that, yes.

Senator LEE. Understood. Understood.

Now, on a different topic, last year John Morton, the Director of U.S. Immigration and Customs Enforcement, issued a couple of memoranda that between them set out certain priorities that would govern the use of—the exercise of prosecutorial discretion within ICE. And within that memorandum, there were a number of considerations outlined which ended up mirroring to a very significant degree the same factors that were outlined in the DREAM Act, the same version of the DREAM Act that the Senate refused to pass a couple years ago. It came up for a vote and did not get the necessary number of votes to pass.

Among those factors that the agents were instructed to consider in exercising prosecutorial discretion included the alien's length of presence in the United States, which mirrored the factor in Section 3(b)(1)(A) of the DREAM Act; the circumstances of the alien's arrival in the United States, particularly if it happened at a time when the alien was a young child, which mirrors what can be found in 3(b)(1)(B) of the DREAM Act; the alien's criminal history, mirroring the factor in 3(b)(1)(D) of the DREAM Act; the alien's pursuit of education in the United States with particular consideration given to those who have graduated from a U.S. high school or who have successfully pursued or are pursuing college or advanced degrees at a legitimate institution of higher education in the United States, and that, of course, mirrors Section 3(b)(1)(E) of the DREAM Act; the alien's age with particular consideration given for minors, mirroring Section 3(b)(1)(F) of the DREAM Act; and whether the alien has served in the military of the United States, mirroring Section 5(a)(1)(D)(ii) of the DREAM Act.

So given these prosecutorial discretion standards which match up somewhat closely to the same factors put forth in the DREAM Act, and given the fact that the DREAM Act was not passed into law, what assurances can you give us or what assurances can I give to my constituents when they approach me and suggest that perhaps there might be an effort under way to back-door these same factors in through regulatory channels that could not be passed through Congress?

Secretary NAPOLITANO. Senator, first let me begin by saying, having worked in this field for decades now, we strongly need overall reform, and we strongly support the DREAM Act as a legislative enactment. You are right it failed by four or five votes to get cloture here. It was passed by the House.

That being said, what we have the capacity or only jurisdiction to do is to administratively close a case. That does not give the person involved any kind of a green card or anything of that sort. It simply means their case is effectively suspended and they can remain in the United States. That is very different from the DREAM Act, which would allow an actual pathway to citizenship, and, you know, one of the things I think we should be doing is really focusing our enforcement resources on those who are real risks to the public safety of the United States. And those who meet the standards of the DREAM Act, if they really meet those standards, are not.

Senator LEE. OK. So the overlap between them is coincidental, and your response to that is essentially that these are two different layers of analysis. One in the DREAM Act would be focusing on a pathway toward citizenship. This is focused on how to allocate scarce prosecutorial and law enforcement resources.

Secretary NAPOLITANO. I think that is an accurate statement.

Senator LEE. OK. And you are not concerned or convinced that these could spill over into something larger?

Secretary NAPOLITANO. We are in the process of looking at all of the cases on the immigration docket to see which, if any, should be administratively closed, and those that meet the criteria you just named are those that we would consider for administrative closure.

Senator LEE. OK. Finally, is there any chance that in my lifetime we will see a time when passengers before boarding a plane do not have to remove their shoes going through TSA?

Secretary NAPOLITANO. Well, Senator, we have already—you know, we are looking at everything from what is the threat and what is the risk, and we have already made changes for passengers over the age of 75 and children under the age of 12 where, except for on a random basis—and we always have to have some unpredictability in the system—they can be expedited through the lines without their shoes being taken off.

From a technology standpoint, the technology still does not exist that allows us to easily identify non-metallic matter in shoes or in liquids, which is why we are doing some of the things we are doing. And it is all based on the intelligence we have about the terrorist threats we face.

Senator LEE. I see my time has expired. Thank you.

Secretary NAPOLITANO. Thank you, Senator.

Senator LEE. Thank you, Chairman.

Senator COONS [presiding.] Thank you, Senator Lee.

Senator Franken.

Senator FRANKEN. Thank you, Mr. Chairman.

Madam Secretary, this week the House of Representatives is considering several cybersecurity proposals, but this morning I want to talk with you about the cybersecurity proposals that are here in the Senate, because while there has been a lot of talk about privacy

and civil liberties implications of the House proposals, and rightly so, fewer people are talking about the two bills here in the Senate. The fact is that, as they are currently drafted, both of the cybersecurity proposals here in the Senate present very serious threats to our privacy and civil liberties. Both bills allow companies the near unfettered ability to monitor the e-mails and files of their customers. Both bills may allow companies to share that information directly with the military. Both bills generally allow the Federal Government to freely share that information with law enforcement. And both bills immunize companies against grossly negligent and knowing violations of the few privacy protections that apply to this process.

In doing all of this, both of these bills sweep aside decades of privacy laws, many of which this Committee wrote, in many cases with Chairman Leahy at the helm. I am talking about the Wiretap Act, the Stored Communications Act, and the pen register statute.

Now, I have been working together with Senator Durbin and with the sponsors of the Cybersecurity Act of 2012, and they have been working with us in good faith, and I sincerely hope that we can fix these problems before the bill even gets to the floor. But I think it is really important that everyone knows that we have real civil liberties problems not just in the House but also here in the Senate bills.

I am saying all of this to you, Madam Secretary, because the administration's cybersecurity proposal from last May does not have many of these problems. It is in several ways more protective of our privacy than either proposal here in the Senate, and I want to use the remaining time I have here to tease out those differences and, frankly, just make the case that we should pay attention to what the administration did in its proposal.

First of all, Madam Secretary, as I mentioned, both the Cybersecurity Act and the Secure IT Act would allow the military to be the initial recipient of any information being shared by a private company, but it is my understanding that it is the official position of this administration that a civilian entity, not a military entity, should always be in the initial recipient of cybersecurity data from the private sector.

Can you explain why this is the administration's position?

Secretary NAPOLITANO. Well, the administration's position mirrors how we have actually organized ourselves in the absence of cyber legislation, and the way we have organized ourselves is that DOD has responsibility for military networks, but DHS has responsibility for civilian and for the intersection with the private sector. We both use the technology resources of the NSA, but we use them under different authorities and with more restrictions, particularly on the privacy side, than you would in an international military sort of context. So the position that we have is to make sure that the statute mirrors what actually is happening on the ground.

Senator FRANKEN. Well, thank you.

Second, Madam Secretary, both of the bills in the Senate give private companies a new authority to freely monitor the communications and files on their systems, many of which would be private. These bills create this new sweeping authority despite exist-

ing provisions in the Wiretap Act that allow companies to perform monitoring to protect their systems.

The administration's proposal does not contain that broad new authority. Can you tell us why it does not?

Secretary NAPOLITANO. What we are looking for and part of the protection of critical infrastructure, we are looking for the code, we are looking for the fact of the attack, the methodology used, the code or signatures that were employed, so that we can then check and see whether that is being done elsewhere and also mitigate and also communicate with other companies about this type of attack. So we are not looking at content. We are looking at the how.

Senator FRANKEN. Great. Thank you.

Why does the administration—let me back up. Third, the administration's proposal only allows the Federal Cybersecurity Center to share the information it receives from private companies with law enforcement authorities if the information constitutes actual evidence of a crime, which I think is good.

In comparison, one of the Senate bills allows the disclosure of information received by the Federal Government to law enforcement if it "appears to relate to a crime." Why does the administration have a heightened standard for disclosures to law enforcement? Was this done to protect civil liberties?

Secretary NAPOLITANO. Senator, I do not know the reason for the difference in the language between those two things. I think what both are getting at is use of information for a non-law enforcement purpose would not be immunized or would not be permitted. But I would have to follow up with you on why the difference between the two phrases.

Senator FRANKEN. OK. Thank you. Let us do that.

I want to thank you, Madam Secretary. Before I finish, I do want to say that I agree with my colleagues who say that we need to do something about cybersecurity. There is no question about that. I just think we need to get the legislation right such that the bill does not unnecessarily sacrifice civil liberties, and I thank you so much for your service and for being here and for your answers.

Secretary NAPOLITANO. Thank you.

Senator FRANKEN. Thank you.

Senator COONS. Thank you, Senator Franken.

Senator Sessions.

Senator SESSIONS. Thank you, Mr. Chairman. Your meteoric rise to the chairmanship exceeds even Senator Franken's.

Senator FRANKEN. Mine was, actually, if you remember, more meteoric.

[Laughter.]

Senator FRANKEN. But that is neither here nor there for the purposes of this hearing. We have the Secretary, and I do not think we should squabble over that.

Senator SESSIONS. We are glad to have both of you fine Senators here.

Madam Secretary, Homeland Security is a big operation. I guess it is the third largest personnel operation, or second, in our Government.

Secretary NAPOLITANO. I think it is the third largest, yes, sir.

Senator SESSIONS. Third? Over 200,000 people. It is cobbled together, and I have got to say I was uneasy about that bill. As I recall, the Democrats said we should consolidate, and President Bush said no, and then he finally said yes and did it, and we passed it without a whole lot of consideration, in my view. So you have a lot of agencies.You have got the Coast Guard, Secret Service, TSA, all sorts of agencies with different histories and cultures. So I know the challenge is hard. I just truly believe you have not—I do not think that it is completely together yet. Do you agree that there is still cultural and bureaucratic efficiencies that could be obtained if focused on today?

Secretary NAPOLITANO. Senator, we continue to—we operate under the caption "One DHS," and we continue to excavate differences in systems, in cultures, in protocols and procedures. There has been a lot accomplished over the past 9 years by my two predecessors and over the past 3-plus years now that I have been Secretary. But given the size and scope of the merger that is underway, it does take time. The Department of Defense took by most accounts 40 years to really become unified as a Department. My goal is to substantially beat that record.

Senator SESSIONS. Well, I think so. I just would say every dollar the taxpayers send us, they need and have a right to expect is wisely spent. And when we have got duplication, mismanagement, and competition unwisely within departments and agencies, it just needs to be confronted, and strong leadership. I will just throw that out. I would suggest that you focus on that.

Senator Kyl I believe raised the question of Chicago and their refusal to honor detainers placed on prisoners, which I find, Cook County's policy at least, is unacceptable. You have written letters about it. I hope that you will follow through on it. They are, I believe, on track to obtain their Secure Communities money and program through 2013. But Alabama, who has been sued by the administration for trying to have laws that help America enforce its immigration laws, not block the enforcement of immigration laws, has had its Secure Communities money stopped or not continued for counties that have asked for it.

Can you tell us where you stand on that? And when can Alabama expect that they would be able to have their Secure Communities funding?

Secretary NAPOLITANO. Well, as I shared with Senator Kyl, I believe the Cook County ordinance is unwise, it is overbroad. We are evaluating all options there. We have been trying to work with the county to see if there is a resolution.

With respect to Alabama, given the litigation and what was enjoined and not enjoined, what we did was simply to stop the expansion of Secure Communities to the final—I think we cover now 75 percent of the foreign-born population, so it is the final quarter. But our plan, Senator, is to complete implementation of Secure Communities nationwide by the end of 2013.

Senator SESSIONS. And that would include Alabama?

Secretary NAPOLITANO. That would include Alabama.

Senator SESSIONS. Well, that is a problem for me, and maybe I will file some written questions to make sure we are clear about where that is heading. I am uneasy about it. It seems to me that

the State was targeted because their law was not popular with the Department, with the President; whereas, you have not taken to date any firm action against Cook County, which clearly endangers, I think, the people of Cook County and the country.

But with regard to the visa exit program, this is a plan that was designed and required by law in 1996. I have observed it and have seen it since I have been in the Senate and the difficulties that have occurred. We have the Visa Waiver Program up and working, the entry program up and working. I do not believe it is that difficult to implement an exit program. I said that when the Bush administration was in office, and I will say it again. I think reports from the Government Accountability Office, GAO, validate that, and I hope that we can make some progress on it.

First, you indicated earlier that you have a biographic plan that has some capabilities. But is it not true that biometric—fingerprint, DNA, or some other such system, fingerprint clearly being the most logical from my perspective—that a fingerprint or other biometric exit system is what is needed to have this system up and working? Otherwise, somebody could walk out without a card that has their name on it and their biographical data, but there would be no way to verify the person holding that card is the person actually exiting?

Secretary NAPOLITANO. Senator, let me offer to have our staff come and brief you personally. It is enhanced biographic. It is not simply a card. But I will make sure that you get briefed on that.

With the biometric, the issue is going to be whether the Congress wants to appropriate the money for whatever margin is left after the enhanced biographic. Our plan, our plan to use enhanced biographic as a platform for that, is in final clearance, and we will share that with you as well.

Senator SESSIONS. Well, I had a long—a year or more—intense discussion on this subject with Secretary Ridge, and they met with international stakeholders, and it went on months and months and months. And I insisted that the only system that really works based on your experience as a Federal and State prosecutor, as I have had that same experience, it is the fingerprints that are in every police officer's file. It is the fingerprint that is taken when a person is arrested somewhere in the United States and becomes a fugitive. And the fingerprint is the basic basis for identifying fugitives.

So when he left, after refusing to commit, he left one bit of advice. He said we should have a biographic system that should be—the biometric system should be the fingerprint, to his successors. And I do believe that that is the system that works.

Is there any plan not to have that?

Secretary NAPOLITANO. No. What we are planning is to go in phases. The first phase is the enhanced biographic, which we are a long way toward implementing right now, and then use that as a platform for the biometric.

Senator SESSIONS. Well, I would just say that in my view it should have been the biometric all along. You should have been working on that, and we would have had that done a lot sooner than 4 years. Otherwise, when you indicate you are not going to look for people who have overstayed, then you basically are saying

we do not intend to take any effort to enforce really an entry-exit system in the United States. And that allows the countries that are approved for visa waiver, I think, to have an unfair, unlimited entry to the United States.

Secretary NAPOLITANO. Senator, we have gone back and looked at visa overstays, and we have racked and stacked them according to biographic information we have about the overstays, turning that information over to ICE to prioritize its enforcement operations. And that work is already underway.

The problem or the logistical—the reason why there is no biometric system at exit, quite frankly, is it is not easy. The lanes and the ports have never—they have always been designed for entry. The architecture has never really been designed for exit. So that is an issue. And then cost and manpower are issues.

Senator SESSIONS. Maybe a briefing from your staff would be helpful to me.

Secretary NAPOLITANO. We would be happy to provide that.

Senator SESSIONS. Thank you, Mr. Chairman. I am over my time.

Senator COONS. Thank you, Senator Sessions.

Senator Blumenthal, I will defer to you.

Senator BLUMENTHAL. Thank you. Thank you, Madam Secretary, for your service and for your very steadfast and effective work on behalf of our national security and your words earlier on behalf of the Secret Service. I think all of us share your view that they do, to use your word, a "marvelous" job of protecting the President and many other law enforcement functions.

I want to follow up on a line of questioning that Senator Graham began in terms of looking forward, the kinds of systems, maybe analogizing the Secret Service to the military, that are used in that context. And I wonder if you have given any thought to additional steps that can be taken to safeguard against but also monitor the kinds of abuses that obviously occurred—or allegedly occurred here.

Secretary NAPOLITANO. We are intent, Senator, on doing a thorough examination of how we do it now and what we need to do to improve, to make sure this never happens again. So all those kinds of options are on the table.

Senator BLUMENTHAL. Thank you.

Switching to a different subject, I was recently approached by a couple, a same-sex couple who are married under Connecticut law. One of them is a citizen of the United States; the other is not. And I wrote to you, and I want to thank you for your assistance in connection with their application for a green card to be held in abeyance. You are probably familiar with the problems that arise under these circumstances. But, eventually, we need a solution like the Uniting Families in America Act that can provide some longer-term solution to this problem.

But I wonder whether we can establish a policy of not deporting or, in other words, holding green cards for same-sex couples, one of whom is here, the other seeking a green card.

Secretary NAPOLITANO. Senator, the legal advice we have been given is that unless and until the law is overturned by the court—and I am talking as to DOMA—which the Department of Justice has urged be done, but until that happens, we cannot unilaterally give green cards based on that. What we have done, however, is

when we have same-sex couples, if they fall within the other criteria of our priority memo, our prosecutorial discretion memo, that allows us to intercede with removal and some of the other actions.

Senator BLUMENTHAL. I am a strong supporter, as are other members of this Committee, of repealing DOMA, the respect for marriage act, which would provide a comprehensive solution. I have been approached by other similar couples who have enormous contributions to make to this country and whose families are every bit deserving of the kind of recognition that we accord to heterosexual couples. And so I hope that I can work with you on this area of trying to devise solutions in the meantime that will enable those couples to continue to be families here, as we need and they deserve. Thank you.

Secretary NAPOLITANO. Yes, absolutely.

Senator BLUMENTHAL. Thank you, Madam Secretary.

Thank you, Mr. Chairman.

Senator COONS. Thank you, Senator Blumenthal.

Senator Durbin, I will defer to you.

Senator DURBIN. Madam Secretary, thank you. I have been trying to juggle schedules, and you have been very patient waiting here. Thank you for your service. I would like to ask you a few questions about the DREAM Act, which you and I have talked about from time to time.

Secretary NAPOLITANO. Yes.

Senator DURBIN. Yesterday Senator Schumer and I held a hearing on Senate bill 1070, the controversial Arizona law, and I talked about seven Arizona residents who would qualify for the DREAM Act, but also would be the targets of the Arizona law. It is beyond reasonable suspicion that they are undocumented. They have stated it publicly. All of them are either attending college or are graduates of Arizona State University with degrees in engineering as an example.

You were asked by a bipartisan group of Senators to suspend deportations of DREAM Act students, and in response, you and the President have established a new deportation policy. And under this policy, as I understand it, it is a high priority to deport those who have committed serious crimes or are a threat to the public while it is a low priority to deport individuals who have been in the United States since childhood, like those who are eligible for the DREAM Act.

Last night, we received updated statistics I requested on the review of deportations that DHS is conducting under your policy. There are currently more than 300,000 pending deportation cases. Of these, ICE has reviewed 219,554. Approximately 16,544 cases—7.5 percent—have been identified as eligible for administrative closure. Of these cases, 2,722, or 1.2 percent, have actually been closed.

Please explain the difference between the 7.5 percent of deportation cases eligible to be closed and the 1.2 percent of cases actually closed. When do you expect the percentage of cases being closed to rise—or do you expect it to rise as the review progresses? And when do you expect the review to be complete?

Secretary NAPOLITANO. Right, I think the difference is primarily attributable to time. You know, we have been doing this case-by-

case review. We just started the pilots right after Christmas, and we have moved now to go across the country since then. So that is part of it. And part of it is that, as we offer administrative closure, oftentimes the recipient of the offer will ask for time to think about it.

So I think that will catch up, and I think we will be closed with the case review by the end of the calendar year, and then we will see what the numbers show.

Senator DURBIN. You and I had another conversation about work authorization, and this to me is a very basic issue which would should discuss in this hearing. Historically, by interpretation of the Department and under the previous President, George W. Bush, in cases where there was deferred action, these individuals were allowed to work, given a work authorization. Now under the new policy, these individuals are offered administrative closure, and your Department has taken the position that individuals whose cases are administratively closed cannot apply for work authorization. It creates a real problem. You are saying to qualified individuals they will not be deported, but they cannot work to support themselves or their families. Many are going to end up in the underground economy, which puts them at risk of exploitation and undercuts the labor market. Only a few thousand people have had their deportations halted so far, so I cannot imagine this will have any significant impact on employment in America.

I ask you then why we are not at least making certain that if we have deferred action or administrative closure that a person is allowed to work.

Secretary NAPOLITANO. Well, first, just to make sure we have a common understanding of the record, we have continued deferred actions and do that before cases get into the administrative system. The administrative closure are cases that are already on the docket and most of which are on the non-detained docket, but a certain number are on the detained docket. And those are the ones we are going through in addition to evaluating new cases as they come in to see that they meet the priorities that we have set.

So with respect to the work authorization, we are going back now, in light of your concerns, and in light of the fact that we now have some numbers to look at as opposed to when we started this whole process, to see if we should make some adjustments. So I would be willing to keep you apprised of our efforts in that regard, but I thought about your concerns after we spoke, and I thought they were serious concerns, and we are exploring how best to address them.

Senator DURBIN. Thank you, Madam Secretary. You and I both know that the President is committed to the DREAM Act. He was a cosponsor when he served in the U.S. Senate, and he has made some important decisions to help these DREAM Act students. So I hope that we can find a way to go further when it comes to giving them an opportunity to work.

I also asked you about the Special Registration Program that was created after 9/11. Arab Americans, American Muslims, and South Asian Americans faced national origin and religious profiling. At least that is what was suggested at a recent hearing I held in this same room 2 weeks ago. The Special Registration

Program targeted Arab and Muslim visitors, requiring them to promptly register with the INS or face deportation. At the time I called for the program to be terminated because there were serious doubts it would even help combat terrorism.

We heard testimony that terrorism experts have concluded that special registration wasted Homeland Security resources and ended up alienating Arab Americans and some Muslims. More than 80,000 people registered, more than 13,000 placed in deportation. How many terrorists were identified by special registration? None.

So last year, DHS terminated all special registration requirements. However, because of special registration, many innocent Arabs and Muslims still face deportation or are barred from applying for citizenship. Last week, you issued a memo to address the situation with these individuals. It provides the individuals who failed to comply that they would not be penalized if their noncompliance was involuntary, unintentional, or otherwise reasonably excusable.

Will you ensure that the standards for noncompliance with special registration are going to be applied fairly and generously?

Secretary NAPOLITANO. Yes, I will, and I will make sure that ICE reports to me how that is being implemented.

Senator DURBIN. I visited an immigration detention facility in my State, the Tri-County Detention Center in deep southern Illinois, and I applaud ICE for issuing its revised detention standards recently. I am in the process of looking those over. I am still concerned about some of the conditions I noted. Some of them will take a deep investigation before I can say with any certainty that there are violations that need to be addressed.

But there was one thing that was very basic that caught my attention, and that was lack of access to the telephone. It turns out many of these people who are being detained, not charged with a crime but being detained, are basically 200 or 300 miles away from family. It may seem like a small issue, but to these immigration detainees, it is not. Currently, these immigration detainees do not have the right to an appointed attorney, and approximately 80 percent go forward without one. And basically none of them have access to e-mail, unlike Federal prisoners. And many of them are in remote facilities such as the one I visited.

They repeatedly raised with me the concern about their inability to communicate with the outside world, including their family. They said they could not afford the phone calls that cost well upwards of $1 or $2 a minute that they are being charged. These are not wealthy people, you can imagine. They are very poor.

We tried to use the phones, local phones, just to see how they would work, and they did not. So there was spotty service and high cost. A large number of county jails with which ICE contracts actually profit by taking a cut of the exorbitant fees that phone companies charge detainees, commissions of 30 to 60 percent on phone call charges. My office has been working with your staff to come up with a solution. Do you have any report of progress on this issue?

Secretary NAPOLITANO. Not as I sit here, but I will follow up. You are right to raise the concern, so let me follow up with our staff, and I will be happy to get back to you.

Senator DURBIN. Thank you. Thanks for appearing today, and thank you, Mr. Chairman.

Senator COONS. Thank you, Senator Durbin.

Madam Secretary, I think I have the honor of the last questions of the oversight hearing today, and I appreciate your patience and your diligence before the Committee today. I was reminded in your opening testimony just how challenging your job is by the fact that you casually referenced that you have a daily threat brief. You supervise the third largest Federal agency. You have a scope of responsibility that I think is awesome. And the challenge that you and your leadership team face of striking an appropriate balance between security, privacy, and commerce is a very difficult and delicate balance, and I just want to start by thanking you for your service. I have known you since you were an Attorney General and have always been impressed with your record of service.

First, just on the Secret Service scandal, if I might, there has been some suggestion in the press today, I think in the Washington Post, that this is actually part of a longstanding pattern or practice. In my previous role, I had the honor of supervising a local law enforcement agency, and I know how devastating to morale and even to operations such incidents can be. This particular incident is very troubling, and I know that there is an aggressive and far-reaching investigation underway.

But have there been allegations of comparably serious misconduct related to the Office of Professional Responsibility in the past? And what steps specifically have you directed Secret Service Director Sullivan to take to ensure that this particular type of misconduct does not occur again?

Secretary NAPOLITANO. To my knowledge, there have been no similar type incidents reported to the Office of Professional Responsibility. I cannot speak to the Inspector General, that is a separate department, but not as to OPR.

What the Director is doing is really reviewing training, supervision, going back, talking to other agents, really trying to ferret out whether this is a systemic problem. If it is, that would be a surprise to me. I must say, as someone who has been the Service Secretary for 3–1/2 years now, I have found the men and women I work with to be extremely professional and the men and women I come into contact with to be extremely professional.

But we want to make sure that we get to the bottom of this, that we deal strongly with those who committed the misconduct and gave the report—that has already been dealt with quite a lot of speed—and that we ferret out any other problems, because, you know, the men and women of the Secret Service do not deserve to have their reputations besmirched.

Senator COONS. I want to commend you for how swiftly the investigations proceeded. I just wanted to reassert what I think we share, which is a conviction that it needs to be not just this incident but a far-reaching investigation that can reassure the American public that this is not somehow an agency where this was routinely tolerated or broadly practiced, that this truly is an outlier incident.

I also at the outset just want to thank you. The last time you were before us, I asked a question about Customs and Border Pa-

trol and the interdiction of counterfeit or allegedly counterfeit materials. You have just implemented a new administration policy that allows CBP agents, when they seize goods at the border that are believed to be possibly counterfeit, to share that information with the rights holders. And I think that is a good and strong advance. I had introduced legislation, but given how swiftly legislation is moving here, I am glad that the administration has embraced that change in practice and policy.

I wanted to dedicate most of our time to cybersecurity. I share Senator Franken's deep concerns about privacy and how we strike an appropriate balance, but also Senator Whitehouse's grave concerns that if we fail to effectively legislate in this field, we leave our critical national infrastructure gravely vulnerable and at risk. I note that in your fiscal year 2013 budget, cybersecurity gets a nearly 75-percent increase in funding while the rest of the Department overall stays flat, so I just want to commend that you are, in fact, prioritizing delivering appropriate resources.

First, if I could, we talked about partnerships, fusion centers. US-CERT is an impressive DHS cyber resource, and I wondered how you see State and local resources in the law enforcement community, in the National Guard. As we have discussed before, Delaware and Rhode Island have network warfare squadrons in the National Guard that I think can and should play a positive role here.

What sorts of resource constraints do we have in terms of effectively responding in the law enforcement community and in the first responder community? My concern about a cyber threat is that it will emerge—well, A, it is very broad and a very serious threat today, but, second, a critical infrastructure threat will emerge very quickly and require very rapid response.

Secretary NAPOLITANO. I think a couple of things, Senator. I think obviously I share your concern. Working with State and locals who are on the floor at the NCIC, the 24/7 watch center, but it is helping with training, it is providing lots of information. I think we provided 5,000 actionable bulletins last year. CERT responded to 106,000 incidents itself. And so training, information sharing, and then across the country in certain locations we have Centers of Excellence, which are helping us refine what we are doing, but also think ahead, what is the next thing that is going to happen in the cyber world.

Senator COONS. I also am familiar with the CFATS program, which has had some challenges. I think it has been successful in promoting site safety at those sites that deal with dangerous chemicals but really has significantly underperformed, particularly in cybersecurity, and I just wanted to encourage attention on that particular area that was brought up in previous questioning by Senator Grassley.

Given the evolving cyber attack risk to our Nation's critical infrastructure and given the debated provisions in different bills, please just, if you would, explain for us the particular strengths that DHS has regarding its capability and capacity to administer potential regulations and protect our infrastructure. Are you confident that DHS has the capacity, as opposed to NSA or DOD, required to handle this critical national threat?

Secretary NAPOLITANO. Yes, and, in fact, as you noted, the budget increase has been requested. We have had multiple additions in the cyber area over the last 3 years. We already are the Department that deals primarily with the private sector and with critical infrastructure, and those mechanisms with which to do that are already in place. And so on the civilian side and on the dotcom side, as it were, DHS already has that systemic protection role.

I think General Alexander testified to that several times. DOD has it, of course, as to the dotmil environment.

So the resources are there. The experience is there, meaning at DHS. We do have lessons learned from CFATS, no doubt, but those lessons have been learned, and those lessons learned give us greater confidence that we can administer this properly.

Senator COONS. Last, if I could, some concerns about privacy and then about bringing the public into this conversation. I think it was Senator Lee who previously asked about future attribute screening technology and its development, something I would be happy to get a briefing on about its trajectory. Recognizing that a lot of what is going on in the dialog between the administration and Congress about the cyber threat is occurring in secure briefings and that a lot of the information that at least I, and I think many other Senators, have received that makes it clear to us just how big a threat this is and just how much loss there is here of intellectual property and how much potential risk there is, most of that critical information is shared with us in a secure setting.

My concern is that this Committee previously legislated on intellectual property theft through the PROTECT IP Act and a comparable committee in the House legislated, some would argue overreached, in the Stop Online Piracy Act. And there was a very broad and unexpectedly strong national response to that by engaged and motivated citizens who were deeply concerned, with some legitimacy, that there was some real threat to their privacy and to the vibrancy of the Internet.

My real concern here is that if we are not sufficiently bringing the public along in striking an appropriate balance here between privacy, security, and commerce, we may face a comparable unexpected, abrupt national backlash against these legislative efforts. And given how rarely we legislate on issues this critical, I am deeply concerned that we not then lose a moment, that we not create a moment of real vulnerability when you have worked so hard to craft a structure that works.

Senator Franken asked you previously about how the administration in its proposals maybe has done a stronger job of recognizing and validating privacy concerns. Any advice for me about how we can, while recognizing the limitations of information that must be held secure, more effectively engage the public in this dialog on the balance between security and liberty?

Secretary NAPOLITANO. Well, we have tried to do it by sharing information with the public through a variety of means. I think it is significant that when there have been briefings in a classified setting, you had sitting there the head of the Joint Chiefs, the head of the NSA, the head of the FBI, the second in charge of the DNI, the second in charge of the DOJ, and myself, all saying the same thing: This is a big risk, it is on us. We need some way to protect

the Nation's core critical infrastructure. We need some way to have information sharing. We need to update and streamline some of the statutes that exist now.

In terms of privacy, I think that was built into particularly the Collins-Lieberman bill, the bipartisan bill in this chamber, providing for privacy, for independent privacy oversight, limitations on how information can be used, and the like. I think we just need to continue to emphasize the differences between that and some of the other approaches.

Senator COONS. I agree with you. Those secure briefings have been successful. They have been in my case hair raising, at times alarming. But the unified and broad engagement by this administration in ensuring that the Senate is briefed is commendable. I just am concerned that when I go and talk in my home State of Delaware, I do not hear the same level of broadly shared understanding of just how real, just how constant, and just how present a threat this is to our intellectual property, to our critical infrastructure, and to the vibrancy of our Nation.

Let me just ask a last question or area, and that would be immigration. I was struck—there was a recent Pew report that came out, I believe, saying that for the first time in 30 years there are more illegal immigrants returning to Mexico from the United States than coming here, and I think that is in part due to strengthening of the economy there, but it is also, I think, the unprecedented action of this administration to hire more border guards, deport more undocumented workers than ever before, and really bear down and engage in strong, smart, and effective border security and enforcement. And I wondered if you had any comment on that.

Secretary NAPOLITANO. I do. In fact, I looked at the Pew study yesterday, and what it is talking about are long-term migration trends, and what it identifies is exactly what you said: that the trend now is more out-migration than in-migration. And it attributes at least part of that to the record amount of personnel and technology infrastructure put on the border, in part because there was bipartisan agreement by the Congress to appropriate an additional $600 million to let us do that job.

Our efforts now are sustaining that and making sure we stay ahead of any surge or movement in illegal traffic along that border and keep that border as safe and secure as we can.

Senator COONS. I think you have done a commendable job on this, and it is, I think, important that the general public realize that my side of the aisle, which is sometimes mischaracterized as not being sufficiently vigorous in our support of enforcement, shares that, that this was a bipartisan effort. I hope you will make real progress in the enhanced biographic exit program, and there was some real dialog about that, but I do think I am cautiously optimistic we will find a new common ground on a host of immigration issues, whether the DREAM Act—I am a cosponsor along with Senator Durbin—H–1B reform, STEM immigration, or uniting families.

Last, just a question on FEMA response. I think that retaining airlift capacity in local National Guards and State National Guards was critical in the State of Vermont, represented by the real Chair-

man of this Committee, as well as my State in the past when there were hurricanes or flooding or other issues. I wondered if you had any comment about how the President's funding request might affect the ability of State National Guards to play an active, supportive role in disaster response.

Secretary NAPOLITANO. Senator, let me get back to you on that because—are you asking about how our request with respect to reforming the grants overall would affect first responders? Are you asking specific to the National Guard?

Senator COONS. I think this is more a National Guard capacity within the branch issue. So I may have asked a question that is not directly in your——

Secretary NAPOLITANO. Yes, I think that is probably more appropriately addressed to the Department of Defense. But I will say our entire work with FEMA has been to be a team with local and State responders as opposed to the Feds being in charge. And I think that teamwork approach has been well received and has worked very effectively.

Senator COONS. I would agree, and I hear all the time from our first responder community in Delaware how grateful they have been for the shared training, the equipment, the grants programs. I actually helped one of our local volunteer fire companies write their annual grant in a memorable all-nighter, and I just wanted to close by thanking you for your strong leadership of the Department and for the Department's sustained and significant contribution to the security and liberty of the people of the United States.

Thank you very much for your testimony, Madam Secretary. We will leave the record open for a week for members of the Committee who were not able to join us but might want to submit additional questions for the record.

Secretary NAPOLITANO. Thank you, Chairman.

Senator COONS. This hearing is adjourned.

[Whereupon, at 11:59 a.m., the Committee was adjourned.]

[Questions and answers and submissions for the record follow.]

QUESTIONS AND ANSWERS

Question#:	1
Topic:	NPG
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Sheldon Whitehouse
Committee:	JUDICIARY (SENATE)

Question: The FY 2013 budget request for the Department of Homeland Security proposes significant changes to FEMA's homeland security grant programs. Under the new plan, 16 state and local homeland security grant programs would be consolidated into one state block grant program called the National Preparedness Grant (NPG) program. Please explain how FEMA plans to ensure that the capability areas that were developed under each of the previous 16 individual grant programs will be sustained under the current program. Specifically, please describe how communities will continue preparedness activities that were previously funded under the State Homeland Security Program, the Metropolitan Medical Response System grants, the Port Security Grant Program, the Regional Catastrophic Preparedness Grant Program, the Citizen Corps Program, the Urban Areas Security Initiative and the Transit Security Grant Program.

Response: As we look ahead, in order to address evolving threats and make the most of limited resources, FEMA proposed a new vision for homeland security grants in the FY 2013 President's budget that focuses on building and sustaining core capabilities associated with the five mission areas within the National Preparedness Goal (NPG) that are readily deployable and cross-jurisdictional, helping to elevate nationwide preparedness. This proposal reflects the lessons FEMA has learned in grants management and execution over the past ten years. Using a competitive, risk-based model, this proposal envisions a comprehensive process to assess gaps, identify and prioritize deployable capabilities, limit periods of performance to put funding to work quickly, and require grantees to regularly report progress in the acquisition and development of these capabilities.

Consolidating grant programs will support the recommendations of the Redundancy Elimination and Enhanced Performance for Preparedness Grants Act (REEPPG) and streamline the grant application process. This increased efficiency will enable grantees to focus on how federal funds can add value to the jurisdiction's prioritization of threats, risks and consequences while contributing to national preparedness capabilities. In addition, all states and territories receiving homeland security grant funding are required to complete a comprehensive Threat Hazard Identification and Risk Assessment (THIRA) which provides an approach for identifying and assessing risks and associated impacts across their state/territory. The coordination element described in the new grants vision will assist grantees in their efforts to address the gaps identified in their THIRA, while building important statewide and national capabilities.

The Department believes that the increased flexibility offered by NPGP, along with the emphasis on building and sustaining core capabilities, will provide states, tribes, and communities with ability to maintain the capability gains achieved to date and provide opportunities to expand those capabilities that need additional funding to grow.

Question#:	2
Topic:	THIRA
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Sheldon Whitehouse
Committee:	JUDICIARY (SENATE)

Question: According to the new guidance for FEMA's homeland security grant programs, each state and territory will receive a base level of funding allocated in accordance with a population driven formula, and additional funds will be distributed competitively based on a risk assessment by each state called a Threat Hazard Identification Risk Assessment (THIRA). The THIRA also provides the basis for determining a jurisdiction's current level of capability for the risks it faces and identifying goals for improvement and capability gaps. According to a GAO report entitled 'Managing Preparedness Grants and Assessing National Capabilities: Continuing Challenges Impede FEMA's Progress', which was released on March 20, 2012, "nearly a year after the THIRA concept was first introduced as part of the fiscal year 2011 grant guidance, grantees have yet to receive guidance on how to conduct the THIRA process." The report also outlines concerns about local participation stating, "[q]uestions also remain as to how local stakeholders would be involved in the THIRA process at the state level." I would like to know what steps FEMA is taking to ensure that local communities are part of the assessment process and how FEMA intends to ensure that each state has the resources it needs to develop its THIRA consistent with Department guidance?

Response: The comments in the GAO report cited have been since addressed and resolved by FEMA. In April, FEMA released Comprehensive Preparedness Guide 201: Threat and Hazard Identification and Risk Assessment (THIRA) Guide, which outlines a five-step process for identifying and assessing risks and associated impacts on communities. That guidance expands on existing state, local, tribal, and territorial Hazard Identification and Risk Assessments (HIRA) and other risk methodologies by broadening the factors considered, and incorporating the whole community throughout the entire process. Step one of the THIRA process—identifying threats and hazards of concern—specifically identifies local fire, police, health departments, and local hazard mitigation offices as sources of data and information.

In conjunction with CPG 201, FEMA also released a document entitled "Use of Threat and Hazard Identification and Risk Assessment for Preparedness Grants." That document outlines validation criteria for the state THIRA, specifically alignment with CPG 201. To that end, as part of the submission, states will identify the local departments and agencies, as well as other whole community partners, who participated in the development of the THIRA. FEMA Grant Programs Directorate Information Bulletin #385a was issued on June 1, 2012 which specified that all 56 states and territories and all 31 urban areas eligible for funding under the FY 2012 Urban Area Security Initiative are required to complete a THIRA by December 31, 2012. The

Question#:	2
Topic:	THIRA
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Sheldon Whitehouse
Committee:	JUDICIARY (SENATE)

Information Bulletin also encouraged tribal nations to also complete a THIRA by the same date.

In order to ensure that the states have the resources they need to complete a THIRA in accordance with Comprehensive Preparedness Guide (CPG) 201, FEMA has taken several steps to provide assistance. First, along with the guidance itself, FEMA released a CPG 201 Toolkit that provides resources and information, data sources, and templates to support the conduct of a THIRA. Second, FEMA streamlined the THIRA and State Preparedness Report (SPR) processes. Recognizing that the steps of the THIRA feed directly into the steps of the SPR, the SPR tool has been aligned to begin with the capability targets identified in the THIRA to reduce reporting burden and duplication of efforts. Third, FEMA conducted 10 technical assistance deliveries on the THIRA process for all states and territories between May 8, 2012 and June 15, 2012. Lastly, FEMA is developing an Independent Study course on THIRA that will allow states, locals and tribes to access training on conducting a THIRA online and at their own pace.

Question#:	3
Topic:	aliens 1
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Jeff Sessions
Committee:	JUDICIARY (SENATE)

Question: After your appearance before the Judiciary Committee last October, I submitted a question to you regarding those aliens whose cases have been administratively closed under the Department's prosecutorial discretion policy. Part of my question asked whether any analysis was conducted to determine the effect that providing work authorizations to these individuals would have on the job market and American workers. You stated in response: "Individuals whose cases are administratively closed, the preferred mechanism for exercising prosecutorial discretion in the case-by-case review initiative, are not eligible to receive employment authorization on the basis of the administrative closure alone." Your answer did not address the question asked. Has your Department or any other agency of the federal government done any analysis to determine how the work authorizations issued to illegal aliens whose cases are administratively closed will affect the job market and American workers? If so, please provide the details of that analysis.

Response: Aliens for whom DHS has decided to exercise prosecutorial discretion do not automatically qualify for an Employment Authorization Document (EAD). Pursuant to longstanding regulations such as 8, C.F.R. § 274a.12 which lists the classes of aliens eligible to apply for work authorization and accept employment, individuals whose cases are administratively closed are not eligible for employment authorization solely on the basis of the administrative closure. DHS has not conducted a labor impact study to determine the effect of issuing EADs to aliens whose cases are administratively closed in the exercise of prosecutorial discretion.

Question#:	4
Topic:	aliens 2
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Jeff Sessions
Committee:	JUDICIARY (SENATE)

Question: In implementing the prosecutorial discretion policy, how many incoming immigration cases have been reviewed, and how many have been administratively closed?

Response: As of September 24, 2012, U.S. Immigration and Customs Enforcement (ICE) had reviewed 376,094 pending detained and non-detained immigration cases. Of the cases that were reviewed, 9,716 non-detained cases have been administratively closed, 16 detained cases have been dismissed, and 26,980 have been identified as appropriate for closure.

Question: How many of the illegal aliens who have had their case administratively closed have ever been convicted of a crime?

Response: Prior to considering whether to file a motion for administrative closure, ICE conducts both national security and criminal background checks. The ICE Office of the Principal Legal Advisor's (OPLA) Offices of Chief Counsel carefully evaluate the results of criminal background checks to ensure that aliens who fall under our civil enforcement priorities are aggressively pursued for immigration enforcement. In some circumstances, aliens with a criminal conviction may still be considered eligible for prosecutorial discretion on a case-by-case basis, after weighing all of the factors present in the alien's case.

To determine how many of the 9,732 aliens who have had their cases administratively closed have been convicted of a crime, ICE needs more time to review its records as it requires a case-by-case review.

Question: Has your Department established a way to keep track of the aliens whose cases are administratively closed?

Response: Once an immigration judge administratively closes a case, OPLA annotates the case file and transfers the case file to ICE's Office of Enforcement and Removal Operations (ERO). This administrative closure information is then manually entered into ICE's Enforce Alien Removal Module (EARM) records management system.

Administratively closed cases will remain in the Executive Office for Immigration Review (EOIR) system, although in an inactive status. EOIR requires aliens to maintain an updated address and contact information for cases that are administratively closed.

Question#:	5
Topic:	ICE agents
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Jeff Sessions
Committee:	JUDICIARY (SENATE)

Question: How much in total has the Department spent on implementing the prosecutorial discretion policy, including the cost of training ICE agents and attorneys, establishing a working group with members from the Departments of Homeland Security and Justice, conducting a nationwide review of all incoming cases, and the pilot programs that have been launched to implement this policy? If you do not know the exact dollar amount, please provide an estimate.

Response: The implementation of the prosecutorial discretion initiative has not required additional funding. In all of the 26 ICE Offices of Chief Counsel (OCCs), the review of pending immigration cases for the exercise of prosecutorial discretion is an ongoing part of the case preparation process for anticipated immigration court hearings. In the two OCCs where the two-month pilot programs were completed earlier this year, the functions and duties in the offices were shifted, but no additional expense was incurred by ICE. Similarly, there were no extra expenditures incurred in training on prosecutorial discretion as ongoing training on any Department initiative is part of standard attorney and managerial development.

Question#:	6
Topic:	biometric 1
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Jeff Sessions
Committee:	JUDICIARY (SENATE)

Question: You have testified that establishing a biometric exit program has proven more challenging for DHS, "largely because infrastructure present at ports of entry is completely absent on departure." What infrastructure changes are necessary to complete the system? What is the estimated cost to implement a completed biometric exit system?

Response: Unlike in many other countries, U.S. airports were not built for the control of the departure of aliens—there are no statutory or regulatory requirements to provide to the government space at no cost from which to collect information on aliens departing the United States (as is the case for arrival). Accordingly, U.S. airports currently are not built to separate international passengers from domestic passengers, and often have international flights co-mingled with domestic flights in the same terminal. Because any biometric air exit system must be able to tell with a high level of certainty that an alien actually departed the United States, it must collect biometric information at the closest point of departure, which is the airline gate. DHS has found it challenging to develop cost-effective ways to collect this information while also not interfering with the airlines' existing business processes. DHS estimates that a biometric air exit system would cost $3 billion over ten years, and that economic analysis is publicly available as part of the DHS Notice of Proposed Rulemaking ("Collection of Alien Biometric Data upon Exit from the United States at Air and Sea Ports of Departure" 73 Fed. Reg. 22065 [April 24, 2008], RIN 1601-AA34) on biometric exit. Similarly, building biometric exit at land border ports of entry would also pose a significant cost increase due to the number of land ports and the infrastructure challenges at land ports of entry that are not applicable to air and sea ports. Official cost estimates for a land biometric exit program using current technology are not available, but have been estimated at tens of billions of dollars.

The Secretary has charged the DHS Science and Technology Directorate with researching and exploring emerging technologies to facilitate a more cost effective biometric exit system. This work is ongoing as the Department continues to implement the enhanced biographic exit program. This program was explained in a DHS report to the House and Senate Appropriations Committees in May 2012, and will enhance the ability of DHS to identify and sanction those who overstay their lawful period of admission in the United States. Aspects to the plan include development of an entry/exit system on the northern land border through cooperation with the government of Canada, to be complete in mind-2013, and enhancements to the existing Arrival-Departure Information System (ADIS) that currently matches entry and exit records using biographic information.

Question#:	6
Topic:	biometric 1
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Jeff Sessions
Committee:	JUDICIARY (SENATE)

As DHS develops its enhanced biographic exit program, it will also continue to research ways to collect biometric exit data upon exit from the United States in a cost-effective ways, and is already exploring several different options. DHS will continue to respond to Congressional inquiries regarding this issue. The Secretary of Homeland Security has authority to designate airports as able to accept foreign nationals seeking admission to the United States. *See* 8 U.S.C. § 1224; 8 C.F.R. § 234.4. Pursuant to these authorities, the Commissioner of U.S. Customs and Border Protection (CBP) may designate air ports of entry for the inspection of aliens if necessary or advisable and adequate facilities have been or will be provided at no cost to the federal government.

Question#:	7
Topic:	biometric 2
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Jeff Sessions
Committee:	JUDICIARY (SENATE)

Question: You estimated that implementation of a biometric exit system would cost around $3 billion over 10 years. Nearly 170 million foreign visitors enter the country each year. If these numbers remain unchanged, in ten years, around 1.7 billion foreign visitors will enter the country. Each of these visitors must register their fingerprints upon entry and would do so upon exiting if an exit program is established. Do you agree that if each foreign visitor was charged a fee, those funds could be used to pay for a biometric exit system? In your estimation, how much would that fee have to be in order to cover the cost of a biometric exit system?

Response: The Secretary has charged the DHS Science and Technology Directorate with researching and exploring emerging technologies to facilitate a more cost effective biometric exit system. This work is ongoing as the Department continues implementing its phased approached of an enhanced biometric exit program.

Question#:	8
Topic:	Visa Waiver
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Jeff Sessions
Committee:	JUDICIARY (SENATE)

Question: In the interest of national security, DHS is required to evaluate all Visa Waiver countries at least every two years and report their findings to Congress. Currently, the Department has completed evaluations and reports on only half of the required countries. Nine reports are more than a year overdue and two are four years overdue. Why has DHS failed to submit these reports to Congress and when do you plan to submit them?

Response: Since May 2011, the Department of Homeland Security has submitted 19 reports on Visa Waiver Program (VWP) countries' reviews to Congress pursuant to the statutory reporting requirements of Section 217 of the *Immigration and Nationality Act* (INA). These submissions include a number of reports that the Government Accountability Office (GAO) reported were overdue in their May 2011 VWP audit.

To address the issue the GAO identified in their May 2011 audit, the DHS Visa Waiver Program Office (VWPO) developed a reporting timeline to address delays in completing VWP reviews and associated reports. The VWPO also conducted outreach to DHS and interagency partners that are involved in the review process to ensure their awareness of the reporting timeline and to discuss related workflow issues. Lastly, the VWPO has identified a mechanism by which to inform Congress of potential delays in a particular VWP Report to Congress. The reporting timeline and notification process will be fully implemented in 2013.

Question#:	9
Topic:	detainers
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Jeff Sessions
Committee:	JUDICIARY (SENATE)

Question: You testified that that the first step that DHS takes to address problems caused by the actions of local governments is to attempt to work with them directly. You testified that you were taking this approach in dealing with Cook County's refusal to honor ICE detainers. What steps were taken by DHS to work with the counties in Alabama that requested and expected Secure Communities to be implemented by the end of last year to address the Department's concerns as you have expressed them to this Committee?

Response: Secure Communities is currently active in 37 of 67 Alabama jurisdictions with an estimated 76 percent of Alabama's non-citizens residing within jurisdictions where Secure Communities has been activated. ICE plans to activate Secure Communities in the remaining Alabama jurisdictions no later than Fiscal Year 2013. ICE is evaluating the recent decision by the U.S. Court of Appeals for the Eleventh Circuit. ICE will continue to operate Secure Communities in each of the Alabama jurisdictions where interoperability has already been activated and will enforce federal immigration law in Alabama in line with our priorities.

Furthermore, ICE's Criminal Alien Program conducts outreach with law enforcement officials in Alabama and continues to enforce federal immigration laws against criminal aliens and others who fall within ICE's civil immigration enforcement priorities.

Question#:	10
Topic:	training
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Al Franken
Committee:	JUDICIARY (SENATE)

Question: Last year, the Federal Bureau of Investigation (FBI) disclosed that some of the training materials it was using for its agents contained bigoted and racist descriptions of Arabs and Muslims. For example, presentations described Muhammad as a "cult leader" and said that Muslims are likely to be terrorist sympathizers. Meanwhile, in April 2012, the Defense Department (DOD) suspended a training course for military officers when it realized that the course relied on inflammatory and inaccurate materials, including a presentation which said that the United States is at war with Islam. The FBI and DOD materials not only are offensive, they compromise federal law enforcement's relationships with minority communities. What is the Department of Homeland Security doing to ensure that its training materials are free of racist, bigoted, offensive, and inaccurate statements about Arabs, Muslims, and other minority populations? Is the Department of Homeland Security conducting a review of its training materials? Has the Department of Homeland Security adopted standards for its training materials?

Response: DHS is committed to ensuring that DHS supported training is accurate and helps foster strong partnerships at the local level, which are critical to preventing crime. To this end, DHS has taken a number of steps to: 1) develop accurate and professional training for Federal, State, Local, Tribal, and Correctional Facility law enforcement at the recruit and management level; and 2) communicate best practices and standards for CVE training to State and Local entities.

The Department is working closely on multiple interagency efforts and with state, local, tribal, and territorial and correctional facility law enforcement to develop CVE training curricula and ensure that these trainings are compliant with USG and DHS CVE approaches. Over the past year, DHS has worked closely with State and Local partners, including the State and Provincial Police Academy Directors (SPPADS), the International Association of Chiefs of Police (IACP), the Major City Chiefs Association (MCCA), the Major County Sheriff's Association (MCSA), as well as NCTC, DOJ, and the FBI to develop training for Federal, State and Local, and Correctional Facility law enforcement officers, as well as a training block for State and Municipal Police Academies. The key goal of the training is to help law enforcement recognize the indicators of violent extremist activity and distinguish between those behaviors that are potentially related to crime and those that are constitutionally protected.

The Department has hosted four workshops to receive feedback from frontline officers on the State and Local CVE training materials. Workshops were also conducted to review the CVE training curriculum for Correctional Facility law enforcement. Additionally, the

Question#:	10
Topic:	training
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Al Franken
Committee:	JUDICIARY (SENATE)

Department has held multiple review sessions with the State and Provincial Policy Academy Directors and IACP to receive input on the training materials focused for State Academy Training facilities.

DHS is now in the final stages of reviewing and implementing this CVE training for State, Local, Tribal, Federal, and Correctional Facility law enforcement officers, as well as a training block for State Police Academies. Through the DHS CVE Working Group, the Department is working to ensure that all of these training materials and content are being reviewed by the appropriate CVE representatives, including the Office of Intelligence and Analysis (I&A), the Office for Civil Rights and Civil Liberties (CRCL), the Science and Technology Directorate (S&T), the Office of Policy (PLCY), the Office of the General Counsel (OGC), the Office of Privacy (PRIV), and other members of the CVE Working Group for accuracy and compliance with civil rights and civil liberties. DHS also co-chairs a bi-monthly Sub-IPC Working Group on CVE Law Enforcement Training with NCTC. This group works to ensure that trainings are consistent and in accordance with the standards outlined in the USG and DHS CVE approaches. DHS aims to make all of the CVE training materials available to law enforcement online through a Homeland Security Information Network (HSIN) CVE portal by September, 2012.

We are also working with the IACP, SPPADS, FLETC, and other DHS Components to plan a "Train-the-Trainer" session for state and local training authorities across the country on the CVE training resources that have been developed. DHS has actively worked to develop a set of best practices and standards for CVE training, and to communicate CVE training priorities and best practices to State and Locals and grant recipients in three key ways. First, in response to reports of inappropriate and inaccurate training, CRCL released its *CVE Training Guidance and Best Practices* which specifically outlines that training should focus on behavior and not appearance or membership in particular ethnic or religious communities, and should support the protection of civil rights and civil liberties. This guidance was incorporated into a FEMA Information Bulletin that was distributed to all State Administrative Agency (SAA) Heads, State Homeland Security Directors, State Emergency Management Agency Advisors (HSAs), and Tribal Nation Points of Contact nationwide in October 2011. This FEMA Bulletin emphasized the importance of ensuring that all grant funds, training, presentations, and speakers on CVE are consistent with the Department's CVE guidelines. Moreover, CRCL regularly trains state and local law enforcement on issues related to: 1) understanding violent extremism; 2) cultural differences; and 3) community engagement.
Second, DHS is also working closely with interagency partners, and law enforcement associations, such as the MCCA and senior law enforcement officials nationwide to

Question#:	10
Topic:	training
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Al Franken
Committee:	JUDICIARY (SENATE)

improve CVE training standards. In January, 2012, the MCCA adopted a motion to ensure that all CVE training is operationally appropriate and accurate. DHS has expanded FY2012 grant guidance to include funding for CVE training, partnerships with local communities, and local CVE engagement in support of the White House's *Strategic Implementation Plan to Empower Local Partners to Prevent Violent Extremism in the United States.*

Third, the Department is working to develop an accreditation process for CVE trainers and develop a train-the-trainer program by FY 2013. FLETC, FEMA, and the CVE Working Group are working to achieve the following three goals: 1) Ensure Federal training provided by Components meets DHS and the USG's CVE standards; 2) Ensure that grantees and State and Locals using DHS funds for training are utilizing trainers that are certified with specific qualifications and meet DHS and the USG's CVE standards; and 3) Disseminate our DHS training through specific accredited partners.

Question#:	11
Topic:	grant program 1
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Al Franken
Committee:	JUDICIARY (SENATE)

Question: I am concerned about security at rural and suburban courthouses. In December 2011, a man shot a prosecuting attorney and a witness in the Cook County courthouse in my home state of Minnesota. There has been about one courthouse shooting per month over the past two years. In response to an inquiry that I sent to you in February, the Assistant Administrator of the Grants Program Directorate sent me a letter stating as follows: "The costs associated with some security enhancements at courthouse facilities are allowable under the [State Homeland Security Grant Program]. Allowable physical security enhancement equipment commonly used for courthouse security includes, but is not limited to, camera-based security systems, access and intrusion control technology, remote sensing devices, and impact resistant systems for doors and gates. In addition, [State Homeland Security Grant Program] funds may be used to conduct risk assessments and provide training for key personnel to perform homeland security related activities. However, the cost associated with hiring personnel to secure courthouse facilities is not authorized." Does the letter that I received from your Assistant Administrator for the Grants Program Directorate reflect your views about allowable uses under the State Homeland Security Grant Program?

Response: Yes, the information that you received in February is correct.

Question#:	12
Topic:	corruption
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: On March 30, 2012, the Department of Homeland Security's (DHS) Assistant Inspector General for Investigations, Tom Frost and the Deputy Assistant Inspector General for Investigations, John Ryan were placed on administrative leave pending the conclusion of an investigation by the Federal Bureau of Investigation and the Department of Justice's Public Integrity Section into allegations of obstruction of justice.

Since its inception, CBP has more than doubled. While this growth is a positive step, with it has come increased corruption. For example, in just one year, from FY 2010 to FY 2011, open or assigned cases of CBP corruption almost doubled from 103 to 205. This is particularly true of agents on the southwest border. For example, of the current 570 open or assigned cases DHS OIG is investigating related to CBP agents, 338 or 59% relate to corruption. Problems in prosecuting CBP corruption also appear to be at the root of this dispute between the FBI and DHS OIG, including a large backlog of CBP corruption cases. What steps are you taking to make sure that DHS OIG has the resources sufficient to investigate these cases?

Response: The Department is committed to ensuring that every allegation of misconduct is swiftly and fully investigated. On August 12, 2011, the OIG and CBP entered into a Memorandum of Understanding (MOU) whereby CBP will augment the OIG's investigations of corruption allegations against CBP personnel by detailing CBP Internal Affairs (IA) agents to the OIG's Office of Investigations. Under the terms of the MOU, CBP IA has 13 agents currently detailed to the OIG. In addition, the OIG is in the process of transferring approximately 47 percent of its existing caseload to ICE OPR agents who will investigate the cases with the support of CBP IA. DHS expects these efforts will lead to a significant acceleration in the investigation of corruption allegations.

Question: Why didn't DHS do a better job of screening CBP agents on the front end of the hiring process?

Response: CBP applicants undergo a stringent pre-employment process including a background check and interview through multiple layers of review. This robust candidate screening has been enhanced through the Anti-Border Corruption Act of 2010 (Pub. L. No. 111-376), which requires CBP to conduct polygraph examinations on all law enforcement officer applicants.

Question: Please provide all reports prepared for DHS by the Homeland Security Institute related to combating CBP corruption or the backlog of CBP corruption cases.

Response: A copy of the Final Report produced by the Homeland Security Institute entitled "U.S. Customs and Border Protection (CBP) Workforce Integrity Study" is attached.

Question#:	13
Topic:	Ninth Circuit Order I
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: On February 6, 2012, the Ninth Circuit put five deportation cases on hold and asked the government how the illegal aliens in the cases fit into the administration's immigration enforcement priorities. In relevant part, the order in each case states:
In light of ICE Director John Morton's June 17, 2011 memo regarding prosecutorial discretion, and the November 17, 2011 follow-up memo providing guidance to ICE Attorneys, the government shall advise the court by March 19, 2012, whether the government intends to exercise prosecutorial discretion in this case and, if so, the effect, if any, of the exercise of such discretion on any action to be taken by this court with regard to Petitioner's pending petition for rehearing.

On March 1, 2012, House Judiciary Committee Chairman Lamar Smith and I sent a letter to you and Attorney General Eric Holder expressing concern about the Ninth Circuit's order. Moreover, the letter asked the DOJ and DHS to respond to questions about how they were handling cases before immigration judges, the Board of Immigration Appeals (BIA) and the federal courts of appeals. In particular, our letter contained four specific questions or requests for information:

For each of the cases that is subject to the order(s) issued by the Ninth Circuit on February 6, 2012, identify the following: (a) the date the case was commenced before an immigration judge or trial judge, (b) the date the appeal to the Ninth Circuit was filed, (c) the date the government's merits brief in the Ninth Circuit was filed, (d) the status of the case in the Ninth Circuit, (e) whether the government has argued that the Ninth Circuit should affirm a removal order, (f) the number of hours worked on the case by government attorneys before the case reached the Ninth Circuit, (g) the number of hours worked on the case by government attorneys since the case was filed in the Ninth Circuit, (h) an estimate of the number of hours worked on the case by immigration judges, BIA judges and federal judges and (i) the amount of tax payer dollars spent on the case to date, including the portion of the salaries of the government attorneys, judges and court staff who have worked on the case.

Does the government seek to have immigration judges enter removal orders even though those orders may subsequently be disregarded pursuant to prosecutorial discretion? If so, how does the administration justify wasting millions in taxpayer dollars and wasting the time of the government attorneys working to achieve removal orders and the immigration judges presiding over the cases?

Question#:	13
Topic:	Ninth Circuit Order 1
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Response: The U.S. Department of Homeland Security (DHS) does not initiate removal proceedings before an immigration judge with the intention of eventually having those proceedings suspended or dismissed. Facts may come to light during the litigation or adjudication of an immigration case that may warrant the exercise of prosecutorial discretion. DHS is committed to continuing this Administration's enforcement priorities which ensure that we optimize our resources by targeting for removal those aliens who pose a danger to public safety or pose a threat to national security, including convicted criminals, as well as repeat immigration violators, recent border crossers, and immigration fugitives.

Some of the specific questions asked in your March 1, 2012 letter were addressed in DHS Assistant Secretary for Legislative Affairs Nelson Peacock's April 23, 2012 letter to you. Between the months of April to June 2012 the U.S. Courts for the Ninth Circuit issued mandates in all five civil cases, dismissing each of the plaintiffs' lawsuits. DHS did not track the specific number of hours worked by the attorneys involved in each part of the litigation process or the costs associated with litigating each case as was requested in your March 1, 2012 letter.

Question#:	14
Topic:	Ninth Circuit Order 2
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: Does the government seek to have the BIA affirm removal orders even though the affirmances may subsequently be disregarded pursuant to prosecutorial discretion? If so, how does the administration justify wasting millions in taxpayer dollars and wasting the time of the government attorneys working to achieve removal orders and the BIA judges presiding over the cases?

Does the government seek to have federal courts of appeals affirm removal orders, even though those orders may subsequently be disregard pursuant to prosecutorial discretion? If so, how does the administration justify wasting millions in taxpayer dollars and wasting the time of the government attorneys working to achieve removal orders and the federal judges presiding over the cases?

Response: The U.S. Department of Homeland Security (DHS) does not initiate removal proceedings before an immigration judge with the intention of eventually having those proceedings suspended or dismissed. Facts may come to light during the litigation or adjudication of an immigration case that may warrant the exercise of prosecutorial discretion. DHS is committed to continuing this Administration's enforcement efforts, while ensuring that we optimize our resources by targeting for removal those aliens who are convicted criminals, pose a threat to national security, pose a danger to public safety, repeat immigration violators, recent border crossers, or immigration fugitives. DHS defends removal orders before the Board of Immigration Appeals with the intention of ultimately executing the removal orders.

Question#:	15
Topic:	Ninth Circuit Order 3
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: According to some reports, there are at least 1.6 million immigration cases pending before immigration judges, the BIA and the federal courts of appeals. Also, according to reports, the DHS and/or DOJ are "reviewing" 300,000 or more cases under the "prosecutorial discretion" initiative.

The DOJ and the DHS are supposed to be prosecuting these cases and seeking to have illegal aliens deported. As part of that effort, line attorneys from the DOJ and DHS spend thousands of hours working on these cases. Simultaneously, immigration judges and federal judges, assisted by court staff, spend hundreds of hours adjudicating these cases. Tens of millions of taxpayer dollars, if not more, are spent to pay the salaries of those attorneys, judges and court staff.

The answer to the Ninth Circuit's question set forth in the government's pleadings was nonresponsive. The government's pleadings tell the Court that the government does not presently intend to use prosecutorial discretion with the cases, but that the matter is totally within the discretion of the Executive Branch. If the government decides to use prosecutorial discretion while any of the cases are pending, it will inform the Court. What is unwritten is that the Obama administration can still use prosecutorial discretion after a case is concluded, even if a Court has issued a deportation order and after all the time, effort and money has been expended.

The DHS responded to the March 1 letter with a one-page letter dated April 23, 2012 and signed by Nelson Peacock, the Assistant Secretary for Legislative Affairs. The April 23 letter does not answer the four specific questions or requests for information in the March 1 letter.

Did you review the April 23 letter before it was sent?

Did you authorize the April 23 letter?

Is the DHS refusing to answer the questions and requests for information from the March 1 letter? If so, what is the legal authority for the DHS's refusal? If the DHS is not refusing to answer, how do you explain the April 23 letter's failure to answer the questions?

Question#:	15
Topic:	Ninth Circuit Order 3
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Provide complete and detailed answers to the all of the questions and requests for information from the March 1 letter, which are quoted above.

Response: As the Department explained in its letter of April 23, 2012, U.S. Immigration and Customs Enforcement (ICE) must retain its flexibility to exercise prosecutorial discretion as appropriate at any stage of the enforcement process. In cases where prosecutorial discretion is appropriate, ICE aims to exercise it as early in the enforcement process as possible in order to conserve the greatest number of resources. However, ICE retains the authority to exercise prosecutorial discretion at later stages of the enforcement process, including after federal courts have completed review of a case. Even when an individual has received a final order and a federal court has reviewed his or her case, additional resources must be expended to execute that order and remove that individual from the United States. As a result, the exercise of prosecutorial discretion in appropriate cases at later stages of the enforcement process also helps conserve agency resources, which permits ICE to focus those resources on cases that are enforcement priorities, including convicted criminals, public safety or national security threats, repeat immigration violators, recent border crossers, and immigration fugitives. Nevertheless, prosecutorial discretion is purely a prerogative of the Executive Branch and, as a result, is not a matter appropriate for a court's consideration – a point which the Department of Justice made clear in its filings in the U.S. Court of Appeals for the Ninth Circuit.

Question#:	16
Topic:	FOIA
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: On March 30, 2011, the House Committee on Oversight and Government Reform released its 153-page report on its investigation of the DHS's political vetting of requests under the Freedom of Information Act (FOIA). The Committee reviewed thousands of pages of internal DHS e-mails and memoranda and conducted six transcribed witness interviews. It learned through the course of an eight-month investigation that DHS political staff has exerted pressure on FOIA compliance officers, and undermined the federal government's accountability to the American people. The report by Chairman's Issa's Committee reproduces and quotes email from political staff at the DHS. The report also quotes the transcripts of witness interviews. The statements made by the political staff at the DHS are disturbing.

What is your response to each of the findings contained on pages 5-7 of the report?

What is your response to the disturbing statements made by DHS political staff, who are quoted in the report? In particular, what is your response to political appointees in your office referring to a career FOIA employee, who was attempting to organize a FOIA training session, as a "lunatic" and to attending the training session, for the "comic relief"?

What actions, if any, have you personally taken in response to Chairman Issa's report?

Set forth in detail your involvement in the FOIA vetting process implemented by the Office of the Secretary at the DHS in or about July 2009, which was the subject of Chairman Issa's report/investigation and which was described in a July 2010 article by Ted Bridis of the Associated Press?

Did you authorize the implementation of the FOIA vetting process?

If you did not authorize it, when did you first learn of the FOIA vetting process and what was your response at that time?

Chairman Issa's report and a report prepared by the Inspector General of the DHS find that political staff at the DHS lacks a fundamental understanding of FOIA. What, if anything, have you personally done to address this situation? If you have not done anything personally, acknowledge that fact.

Question#:	16
Topic:	FOIA
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Response: The Department respectfully disputes the findings. The Department of Homeland Security's (DHS) Privacy Office administers policies, procedures, and programs to ensure overall compliance with the Freedom of Information Act (FOIA) and the Privacy Act. In fiscal year 2010, less than one-half of 1 percent of more than 138,000 FOIA requests processed were deemed significant by career FOIA officers pursuant to Department standards established in 2006. The significant requests include those related to ongoing litigation, sensitive topics, requests made by the media, and requests related to Presidential or agency priorities. In these relatively few cases, senior department management was and is provided an opportunity to become aware of the contents of a release prior to its issuance to the public through a FOIA notification process to enable them to respond to inquiries from Members of Congress, their staffs, the media, and the public, and to engage the public on the merits of an underlying policy issue.

No one other than career staff made substantive changes to proposed FOIA releases. No information deemed releasable by the FOIA office or the Office of General Counsel, has at any point, been withheld, and responsive documents have neither been abridged nor edited. The Department's Inspector General (IG) provided an independent analysis on this issue which made many critical findings, including that the significant FOIA request review process did not prevent the eventual release of information; no FOIA requesters were disadvantaged because of their political party or particular area of interest; the Office of the Secretary is responsible for overseeing DHS operations, and thus is well within its rights to oversee the FOIA process; and DHS has made important progress in promoting openness, including through proactive disclosure. We concurred with all of the IG's recommendations, and have implemented a series of process improvements to address the recommendations. The Inspector General has closed his six recommendations for improving the efficiency of FOIA processing, acknowledging the steps the Department has taken. The Department remains fully committed to implementing the Freedom of Information Act and Privacy Act effectively and efficiently and with the highest standards for exceptional customer service.

Beginning in 2011, the Chief FOIA Officer directed the Deputy Chief FOIA Officer, to undertake a comprehensive review of departmental FOIA operations, meeting with all Component-level FOIA Officers to discuss the challenges they faced. As a result of these and other reviews on March 16, 2010, the Chief Privacy Officer issued a memo directing the Department to continue to actively implement the Administration's FOIA policy changes. The memo reiterated the importance of the presumption of disclosure and proactive disclosure requirements and noted specific progress in Components' proactive disclosure activity.

Question#:	16
Topic:	FOIA
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

In total in FY 2011, DHS proactively released 8,903 pages of material, a 43-percent increase from the previous fiscal year. In FY 2012, the FOIA Office anticipates additional growth in proactive disclosure, by implementing new recommendations from the pro-active disclosure team.

The Department has made a significant effort in educating and training its workforce on the importance of the Freedom of Information Act and Privacy Act. In its periodic training of new and current employees on the requirements of FOIA, the Privacy Office emphasizes the contents of the President's FOIA memorandum of January 21, 2009, particularly regarding his policy that "[t]he Government should not keep information confidential merely because public officials might be embarrassed by disclosure, because errors and failures might be revealed, or because of speculative or abstract fears." Our components also provide training on these important points. Thus, not only FOIA staff but also DHS personnel, as a whole, are repeatedly advised of these important points.

The Privacy Office also undertook a systematic review of Exemption 5 usage, reviewing current guidance and consistent with Delegation 13001, by memorandum issued to all of DHS on January 31, 2012, the Chief FOIA Officer reiterated that: "[W]e do not assert FOIA exemptions to prevent embarrassment of public officials or possible revelations of errors or failures, or because of speculative or abstract fears."

Question#:	17
Topic:	DHS Policies
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: According to news reports, a 2011 reference guide for DHS analysts monitoring the media reveals that the DHS is tracking opponents of its policies. In particular, the DHS is directing its analysts to identify and monitor media reports (and social media) that reflect adversely on the DHS. Analysts are also apparently directed to track reports on the Obama administration's policy changes in immigration and the term "illegal immigration" in particular.

Is the DHS monitoring, tracking and/or researching U.S. citizens or organizations that criticize or question the policies of the Obama administration or the DHS, solely because of the individual's or organization's criticism/questioning? If so, when did this start? And if so, for what purposes has this monitoring, tracking and/or research been undertaken and what is the justification for it?

Have you authorized the monitoring, tracking and/or researching of U.S. citizens or organizations that criticize or question the policies of the Obama administration or the DHS, solely because of the individual's or organization's criticism/questioning? If so, when did you authorize this and why did you authorize it? Also, if so, what is the justification for this monitoring, tracking or research?

Who is reviewing the information collected by DHS analysts? Are the same political appointees who were involved in the FOIA political vetting process, and who are identified in Chairman Issa's report reviewing the information?

How is the information that is collected being used?

Response: In support of its statutory mission to provide situational awareness and a common operating picture for the federal government and for other homeland security enterprise partners, the National Operations Center (NOC) within the DHS Office of Operations Coordination and Planning (OPS) reviews publicly available traditional and social media postings to gain an enhanced awareness of rapidly emerging or evolving incidents and events concerning homeland security, emergency management, and national health. By examining open source information and comparing it with other sources of information, the NOC provides enhanced situational awareness and greater detail for the common operating picture to DHS leadership and homeland security enterprise partners.
The NOC's social media initiative (Initiative) is not designed to actively collect personally identifiable information (PII) and remains focused on reporting on event

Question#:	17
Topic:	DHS Policies
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

categories that are operationally relevant to DHS. Beginning in January 2011, the Initiative was first permitted to collect PII on seven defined categories of individuals when doing so lends credibility to the report or facilitates coordination with interagency or international partners. The seven categories are: 1) U.S. and foreign individuals in extremis, *i.e.*, in situations involving potential life or death circumstances; 2) senior U.S. and foreign government officials who make public statements or provide public updates; 3) U.S. and foreign government spokespersons who make public statements or provide public updates; 4) U.S. and foreign private sector officials and spokespersons who make public statements or provide public updates; 5) names of anchors, newscasters, or on-scene reporters who are known or identified as reporters in their posts or articles, or who use traditional and/or social media in real time to provide their audience situational awareness and information; 6) current and former public officials who are victims of incidents or activities related to homeland security; and 7) terrorists, drug cartel leaders, or other persons known to have been involved in major crimes of homeland security interest, who are killed or found dead. This PII is relevant to the NOC's reporting because a journalist, government representative or private sector spokesperson creating a public posting in his or her professional capacity is considered to have greater credibility than an individual bystander posting information on a publicly available social media site. Other PII is collected to better ensure public safety and national security.

In addition, the DHS Privacy Office recently completed its fourth Privacy Compliance Review (PCR) of the Initiative. As part of the review, the DHS Privacy Office reviewed the NOC's 2011 Analyst's Desktop Binder and Standard Operating Procedures (SOPs) and found these documents reflected the purpose and scope of the initiative. However, as some language could have been interpreted differently by those outside the Initiative who have not undergone its extensive training, the DHS Privacy Office recommended changes to reconfirm that monitoring of certain activities is outside the scope and purpose of the initiative. The NOC has already implemented these clarifications.

To maintain a capability focused on reviewing incident and event information, OPS trains analysts to review information in compliance with the parameters set forth in the Privacy Impact Assessments (PIAs). OPS uses a layered approach to ensuring unauthorized PII is not included in reports. During the report production process, reports are reviewed multiple times to ensure PII is not inadvertently included. All reports distributed during each 24-hour period are checked by a media monitoring capability senior reviewer, and the media monitoring capability's quality control leads conduct weekly reviews of all distributed reports to ensure any inadvertent PII inclusions are identified and corrective action is taken. The DHS Privacy Office conducts Privacy Compliance Reviews every six months to ensure OPS is complying with the PIAs. This review process is wholly unrelated to Freedom of Information Act (FOIA) processes.

Question#:	17
Topic:	DHS Policies
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

All NOC social media initiative PIAs and PCRs are available to the public at www.dhs.gov/privacy. The report on the results of the fourth PCR of the NOC Publicly Available Media Monitoring and Situational Awareness Initiative (http://www.dhs.gov/xlibrary/assets/privacy/privacy_privcomrev_ops_monitoringinitiative_05082012.pdf) contains Appendices with a random sample of media monitoring reports distributed by the NOC during the review period as well as a February 2012 Media Monitoring Guidance Reminder.

Question#:	18
Topic:	cybersecurity 1
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: You have vocally campaigned for legislation which would designate DHS as the lead agency for cybersecurity and which would grant it extraordinary (regulatory) powers and massive new funding. In addition to concerns about the approach you have advocated, there are significant reservations about the DHS's ability to handle primary responsibility for cybersecurity. One of those reservations is based on the DHS's failure to implement ten fundamental recommendations made by the Government Accountability Office (GAO) in 2008. After four years, the DHS has yet to confirm that it has implemented the GAO's cybersecurity recommendations.

The GAO's recommendations broke down into two categories. In the first category, the GAO recommended that the DHS should address the challenges that impede it from fully implementing key attributes of cybersecurity, including:

Response: As its cybersecurity mission continues to evolve, the Department of Homeland Security (DHS) has increased funding of key programs to keep pace with emerging threats through innovative technologies and services. The President's fiscal year (FY) 2013 Budget request makes significant investments to expedite the deployment of intrusion prevention technologies on government computer systems, increase Federal network security of large and small agencies, and continue to develop a robust cybersecurity workforce to protect against and respond to national cybersecurity threats and hazards.

Since 2010, DHS's National Protection and Programs Directorate (NPPD) has been providing documentation to the Government Accountability Office (GAO) to support the closure of recommendations contained in GAO-08-588. By the end of August 2011, DHS had provided all agreed upon documentation to GAO and has followed up with GAO several times on our submissions. The following summaries relate to each of the 10 recommendations.

Question: Filling key management positions and developing strategies for hiring and retaining those officials

Response: On August 12, 2011, the National Cyber Security Division (NCSD) provided an organizational chart to GAO, which reflected the status of key management positions as of that date. Per GAO's request, NCSD updated the status of key management positions on July 24, 2012.

Question#:	18
Topic:	cybersecurity 1
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: Developing predictive analysis capabilities by defining terminology, methodologies, and indicators, and engaging appropriate stakeholders in other federal and nonfederal entities

Response: In July 2011, GAO and NCSD agreed that the envisioned predictive analysis capabilities require participation from a set of agencies broader than DHS. GAO indicated that it would either eliminate this recommendation or close it as "not implemented."

Question: Identifying and acquiring technological tools to strengthen cyber analytical capabilities and handling the steadily increasing workload

Response: NCSD continues to acquire tools to strengthen cyber analytical capabilities and handle the steadily increasing workload as part of the National Cybersecurity Protection System (NCPS). NCSD's United States Computer Emergency Readiness Team (US-CERT) has grown its analytic capabilities while developing the Cyber Indicators Analysis Platform (CIAP). These and other tools enable automated analytical capabilities, which are especially important as US-CERT's workload increases. During July and August 2011, NPPD provided GAO with samples from CIAP and other tools and products.

Question: Expeditiously hiring sufficiently trained cyber analysts and developing strategies for hiring and retaining highly qualified cyber analysts

Response: Since the issuance of GAO-08-588, NCSD has increased the size of its workforce by approximately 600% with more people in the hiring pipeline. Through our Cybersecurity Workforce Initiative, NCSD is hiring a diverse group of cybersecurity professionals to secure the nation's digital assets, critical infrastructure, and key resources. NCSD seeks prospective hires through a variety of mechanisms and has established Individual Development plans (IDPs) for all new and current employees. The IDPs are unique for each employee and are based on specific skill set that the employee needs to learn or improve to accomplish the cybersecurity mission.

In 2010 and 2011, NCSD provided GAO with updates to the size of its workforce, and on May 25, 2010, and again on February 16, 2011, NCSD provided GAO with documents relating to its IDP requirements for all employees and training and mentoring opportunities available to its employees. In August 2011, NCSD also provided GAO the redacted hiring strategy from the Comprehensive National Cybersecurity Initiative fiscal year (FY) 2009 report, which helped drive NCSD's hiring initiatives.

Question#:	18
Topic:	cybersecurity 1
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: Engaging appropriate stakeholders in federal and nonfederal entities to determine ways to develop closer working and more trusted relationships

Response: Since 2008, NCSD has engaged Federal and non-Federal stakeholders through numerous forums to develop closer working relationships. These include, but are not limited to, monthly meetings of the Cross-Sector Cyber Security Working Group; sponsorship of the Industrial Control Systems Joint Working Group; and increased Federal, state, local, and private sector participation in the Cyber Storm exercises. More recently, NPPD's Office of Cybersecurity and Communications (CS&C) began executing Cooperative Research and Development Agreements (CRADAs) with companies and information sharing organizations, such as Information Sharing and Analysis Centers, to facilitate increased information sharing and to enable state, local and private-sector stakeholders to maintain a presence on the watch floor of DHS's National Cybersecurity and Communications Integration Center (NCCIC).

Question: Ensuring that there are distinct and transparent lines of authority and responsibility assigned to DHS organizations with cybersecurity roles and responsibilities.

Response: When GAO issued its report, the National Cybersecurity Center (NCSC), which was the focus of this recommendation, operated separately from NPPD. The functions and mission of the NCSC are now executed by DHS through mechanisms like the NCCIC. In August 2011, NCSD provided GAO with a copy of July 26, 2011, testimony on the cybersecurity environment and mission, which described the realignment of functions and missions. This is further reflected in NCSD's FY 2012 Expenditure Plan and the President's Budget Request for FY 2013.

Question#:	19
Topic:	cybersecurity 2
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: In the second category, the GAO recommended that to fully establish a national cyber analysis and warning capability, the DHS should address deficiencies in each of the attributes identified for:

response, including ensuring that US-CERT provides assistance in the mitigation of and recovery from simultaneous severe incidents, including incidents of national significance;

Response: The Department of Homeland Security (DHS) worked with its Federal, state, local, and private sector stakeholders to develop and exercise the National Cyber Incident Response Plan (NCIRP), which provides a strategy for rapidly coordinating the operational response activities of Federal, state, local, tribal, and territorial governments, the private sector, and international partners during cyber incidents. The NCIRP is consistent with the National Response Framework and the principle of "unified command" for multi-jurisdictional response activities. In accordance with the NCIRP, the National Cyber Security Division's (NCSD) United States Computer Emergency Readiness Team (US-CERT) has enhanced its ability to provide onsite and remote assistance during cyber incidents. In 2011, US-CERT handled over 106,000 cyber incidents involving Federal agencies, critical infrastructure, and our industry partners. So far in 2012, US-CERT has responded to over 65,000 incident reports, which reflects a 35 percent increase from the same period in 2011. DHS provided GAO with a sample of US-CERT's Quick Response Incident Response Kit in August 2011.

Question: Warning, including ensuring consistent notifications that are targeted, actionable, and timely

Response: DHS shares actionable threat and vulnerability information with a broad set of partners through the distribution of diverse products, such as Early Warning and Indicator Notices (EWINs) and Security Awareness Reports (SARs). US-CERT also reaches end users through products released through the National Cyber Alert System (NCAS), which includes the US-CERT Web Portal. In August 2011, NCSD provided GAO with copies of EWINs and SARs as well as US-CERT Web Portal membership as of July 2011. NCSD also provided GAO with a copy of US-CERT's Standard Operating Procedures on Information Sharing with Law Enforcement and Intelligence.

Question: Analysis, including expanding its capabilities to investigate incidents

Question#:	19
Topic:	cybersecurity 2
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Response: US-CERT has greatly improved its analysis capabilities including developing the Advanced Malware Analysis Center, which analyzes the current state of digital artifacts, conducts static and behavior analysis of malicious code types, and manages the development of the unclassified/classified lab and its evolution support US-CERT's operations and mission. In August 2011, NCSD provided GAO with a copy of the signed program requirements for the Malware Lab's expansion.

In addition, US-CERT provides data and analysis of observed cyberactivity to Federal Agencies and partners by reporting specific incidents and aggregated data to senior cybersecurity officials throughout the Government who maintain awareness of suspicious activity affecting their networks. The DHS Office of Intelligence and Analysis (I&A) also provides attribution support and shares the data from reports, NCPS, and other sources with the Intelligence Community to enhance understanding of tactics, techniques, and procedures as well as supporting US-CERT's development of signatures to better identify malicious activity on U.S. Government networks.

Question: Monitoring, including establishing a comprehensive baseline understanding of the nation's critical information infrastructure and engaging appropriate nonfederal stakeholders to support a national-level cyber monitoring capability.

Response: US-CERT monitors and analyzes intrusion detection system sensor data observed across the dot-gov. For example, EINSTEIN is a system we use to conduct continuous diagnostics of the traffic flowing to and from the Federal civilian enterprise. EINSTEIN helps analysts identify and combat malicious cyber activity that may threaten government network systems, data protection, and communications infrastructure. EINSTEIN 2 has provided US-CERT with a baseline understanding of network flow activity and supplements this data with signature-based alerts when network traffic, indicative of malicious activity, is detected. DHS also derives signatures from numerous sources, such as commercial or public computer security information, incidents reported to US-CERT, information from Federal partners, or independent in-depth analysis by US-CERT.

To support information sharing, DHS regularly shares situational awareness information, threat products, and Liaison Officer (LNO) exchange with the Department of Defense (DOD), which is responsible for the .mil domain. In addition, numerous NPPD components are collocated on the NCCIC watch floor along with other Federal partners, such as members of the law enforcement and intelligence communities. The NCCIC also co-locates Federal staff with non-Federal and private sector stakeholders to fuse situational awareness resulting from independent diagnostics. For example, the Multi-State Information Sharing and Analysis Center (MS-ISAC) provides diagnostics services

Question#:	19
Topic:	cybersecurity 2
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

to state and local governments and contributes to the larger common operational picture at the NCCIC.

In order to close this recommendation, DHS provided GAO with a copy of a legal memorandum titled "The Legality of Intrusion Detection System to Protect Unclassified Computer Networks in the Executive Branch" in August 2011. At the same time, DHS provided GAO with the Privacy Impact Assessment (PIA) for EINSTEIN 2, a copy of the US-CERT Concept of Operations, and the EINSTEIN 2 deployment status as of July 2011.

Question: In addition to GAO report GAO-08-588, DHS also has a number of additional outstanding recommendations related to Cybersecurity. For example, DHS currently has four reports with a total of 19 open recommendations related to Cybersecurity. What is the status of these 19 outstanding recommendations related to Cybersecurity? When does DHS plan to implement these recommendations to satisfy the concerns expressed by GAO?

Response: By the end of August 2011, DHS had provided all agreed-upon documentation to GAO on actions implemented and milestones completed in accordance with DHS's corrective action plan submitted to Congress and GAO for GAO-10-628. DHS has followed up with GAO several times on the submittal, and GAO is continuing to perform analysis.

The other two GAO reports, GAO-12-8 and GAO-12-92, were issued more recently. DHS is on track to implement each of the recommendations pursuant to the corrective action plans, which are included in the associated 60-day letters.

Question#:	20
Topic:	CFATS
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: Congress is continuing to debate Cybersecurity legislation. A number of different bills provide DHS additional authority to regulate the public and private sector networks. Specifically, one proposal would place DHS as the lead agency in overseeing baseline regulations for entities that DHS determines qualify as covered critical infrastructure.

I have serious concerns with this proposal because it creates a new regulatory bureaucracy at DHS. I am also concerned about this new regulatory power given DHS's background on overseeing Chemical Facility Security under the CFATS program.

Congress gave DHS regulatory power over chemical facilities in 2006 and regulations were issued in 2007. However, five years later, nearly 4,200 chemical facilities have complied with the regulations, but DHS has yet to approve a single security plan. Despite failing to approve a single plan, DHS has spent nearly half-a-billion taxpayer dollars to effectively do nothing.

I have obtained a copy of an internal review conducted for Undersecretary Rand Beers by two subordinates that details the problems DHS faces in implementing CFATS. To be honest, this memorandum is the most candid review of a failed federal government program I have seen.

For example, the memorandum states:

- There a "number of people in leadership positions who lack managerial experience/knowledge."

- The Department had hired "people who do not have the necessary skills to perform key mission and essential functions."

- "While the vast majority of employees are talented, hardworking people, there are many numerous exceptions."

- Employees have "demanded that they be paid if we expect them to answer their cell phones during lunch, or to carry their cell phones outside duty hours."

- "There is a catastrophic failure to ensure personal and professional accountability" among agency employees.

Question#:	20
Topic:	CFATS
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

- "Our lack of focus and vision has resulted in problems with how we have spent our money, and how we are managing those funds."

This memorandum details failures of an unprecedented level. The memo cites: poor hiring decisions, hiring workers who lack skills to do the job, poor staff morale, management and leadership failures, lack of subject matter experts, union problems, and a "catastrophic failure to ensure personal and professional accountability."

The memorandum also states that inspectors lack expertise to effectively evaluate site compliance with cybersecurity requirements. This report paints the picture of an agency that cannot control costs, manage its employees, or effectively implement its mission.

If it cost DHS $480 million to effectively regulate zero chemical facilities, how much can we expect it to cost taxpayers for DHS to regulate cybersecurity among thousands of private businesses?

Response: Since the Chemical Facility Anti-Terrorism Standards (CFATS) program was adopted, DHS has made substantial progress in identifying and regulating high-risk facilities. As of July 25, 2012, CFATS covers 4,425 high-risk facilities nationwide; of these 4,425 facilities, 3,662 are currently subject to final high-risk determinations and submission of an SSP or Alternative Security Program (ASP). The remaining facilities are awaiting final tier determinations based on their SVA submissions. ISCD continues to issue final tier notifications to facilities across all four risk tiers as it makes additional final tier determinations.

As of August 16, 2012, the Department has:

- Conducted 14 authorization inspections (AIs), which occur after a covered facility receives a Letter of Authorization for its SSP or ASP, but before DHS issues a Letter of Approval for the facility's SSP. AIs are conducted to verify that the descriptions of measures in the facility's authorized SSP or ASP are accurate and complete and that the equipment, processes, and procedures described in the SSP or ASP meet applicable CFATS risk-based performance standards. ISCD evaluates the AI results to determine whether DHS should issue a Letter of Approval.

- Conditionally authorized SSPs for 63 Tier 1 facilities, although two of those facilities subsequently had their tier reduced. For the remaining 53 Tier 1

Question#:	20
Topic:	CFATS
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

SSPs reviewed, we are either validating results or reaching out to these facilities to obtain additional information.

- Conducted more than 1,060 Compliance Assistance Visits (CAVs) at regulated or potentially regulated chemical facilities. CAVs are visits at regulated or potentially regulated chemical facilities that seek to provide compliance and technical assistance.

Since the inception of CFATS, more than 2,700 facilities have eliminated, reduced, or otherwise made modifications to their holdings of potentially dangerous chemicals and are now no longer considered high-risk. These actions have helped reduce the number of high-risk chemical facilities located throughout the Nation and have enabled facilities to take actions that minimize their requirements under CFATS.

The cost of not taking action to better secure our Nation's most critical networks is unacceptably high. Private-sector estimates range from $28 billion to $340 billion in annual losses from cyber attacks. However, this estimate is based on known financial and intellectual property theft and therefore cannot be fully reflective of unreported incidents. The potential cost of a significant disruption to one or more of our interdependent critical services, such as electricity, communications or transportation, would be much higher. For example, in the cybersecurity scenario the Administration presented to the Senate on March 7, 2012, which reviewed the federal response to a three-day power outage in a large metropolitan area, the impact to GDP was estimated at $1 billion per day. However, this scenario was contained to one metro area; losses would be much greater if additional parts of the country were impacted and the duration of the attack, extended. While there will be a cost of securing these facilities, DHS believes it will be significantly less than the expected losses that could be suffered if action is not taken.

Question: Given the documented failures highlighted by this memo, why do you feel that DHS can handle the additional responsibilities you have advocated for in Cybersecurity legislation?

Response: While DHS does not agree that the internal memorandum highlights "failures" in the CFATS program, the Department is working to remedy programmatic and management challenges in the CFATS program. Some areas of progress include the following:

Question#:	20
Topic:	CFATS
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

- *Hiring*: The Infrastructure Security Compliance Division (ICSD) is leading an internal analysis to ensure that the proper staffing and qualification needs of the Division are met.

- *Training and Inspection*: In June 2012, ISCD finished updating its internal inspections policy and guidance materials for inspectors. ISCD also began providing additional training that focuses on the updated policy and guidance materials to prepare Chemical Security Inspectors to resume authorization inspections at facilities with authorized or conditionally authorized Site Security Plans (SSPs). As a result, as of July 16, 2012, ISCD has resumed authorization inspections at Tier 1 facilities. This is a vital step for moving the CFATS program toward a regular cycle of approving SSPs and conducting compliance inspections for facilities with approved SSPs.

Question: It has taken four years and DHS has yet to regulate any chemical facilities. How long would it take to regulate thousands of businesses under a cybersecurity bill?

Response: The timeline for implementing a process to designate covered critical infrastructure and establishing risk-based performance requirements would be determined by the Department's engagement with other partners. Establishing new frameworks for critical infrastructure would be a collaborative process that enhances the existing public-private partnership for securing critical networks. In order to leverage the expertise of stakeholders, the Department of Homeland Security believes that close interaction will be necessary going forward.

Question: When will DHS approve all 4,200 site security plans? How much more taxpayer money will it cost to achieve 100% approval?

Response: There are a number of variables with regard to authorizing and approving facilities' site security plans (SSPs), including ensuring that ISCD continues to have sufficient resources to review SSP submissions and continuing to train our inspector cadre to conduct authorization and compliance inspections.

The SSP review, inspection, and approval process has several steps that must occur before an SSP can be approved. First, DHS must review the SSP to preliminarily determine whether the SSP is sufficient to satisfy applicable risk-based performance standards and, when necessary, work with a facility to improve its SSP. Once DHS preliminarily determines the SSP is sufficient to satisfy the applicable standards, as appropriate for the facility's tier assignment, DHS can authorize, with or without conditions, the SSP. Not every SSP submitted to DHS necessarily meets these

Question#:	20
Topic:	CFATS
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

requirements. With regard to the SSPs that do not warrant authorization, DHS first works with the facility to revise the SSP so that it meets applicable risk-based performance standards; but if these efforts are not successful, DHS may ultimately have to disapprove the SSP.

Following an authorization or a conditional authorization of an SSP, an authorization inspection is conducted to verify that the descriptions of current and planned measures in the facility's SSP are accurate and complete. If, in reviewing/evaluating the results of the authorization inspection and other information, DHS determines that the security plan satisfies the CFATS requirements, DHS then approves the SSP and the facility is notified that it should carry through with the planned security measures and continue to implement existing measures.

Given the dynamic nature of chemical facilities, new facilities can become regulated, and currently covered facilities can add, change, reduce, or remove chemicals of interest, which can lead to changes in their risk tiers or even to becoming unregulated under CFATS.

Since the inception of CFATS, more than 2,700 facilities have eliminated, reduced, or modified their holdings of potentially dangerous chemicals to the point that the facilities are no longer considered high-risk. We believe these actions have reduced the risk from chemical facilities and increased the safety of surrounding communities.

Question: When will DHS conduct the first inspection of an approved chemical facility under CFATS?

Response: In September 2011, ISCD established an Inspector Tools Working Group to ensure the Chemical Security Inspectors have up-to-date and, where appropriate, improved inspections procedures, policies, equipment, and guidance. In June 2012, ISCD finished updating its internal inspections policy and guidance materials for inspectors. ISCD also began providing additional training that focuses on the updated policy and guidance materials to prepare Chemical Security Inspectors to resume authorization inspections at facilities with authorized or conditionally authorized SSPs. As a result, I am pleased to announce that as of July 16, 2012, ISCD has resumed authorization inspections at Tier 1 facilities. This is a vital step for moving the CFATS program toward a regular cycle of approving SSPs and conducting compliance inspections for facilities with approved SSPs.

Question#:	21
Topic:	grant program 2
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: On February 28, 2012 the Government Accountability Office (GAO) released its second annual report to Congress under a requirement that GAO identify federal programs, agencies, offices, and initiatives in the federal government that have duplicative goals or activities. With regard to DHS specifically, the report described the results of a separate, in-depth study of DHS's management of disaster preparedness programs, which have provided more than $20 billion to state, local, tribal, and territorial governments since 2003. DHS's Federal Emergency Management Agency (FEMA) allocated these funds through four programs: the State Homeland Security Program, the Urban Areas Security Initiative, the Port Security Grant Program, and the Transit Security Grant Program. Although no actual cases of duplicative funding were found for Fiscal Year 2011, GAO considered that multiple factors contributed at least to the risk of FEMA funding unnecessarily duplicative projects, including overlap among grant recipients, goals, and geographic locations, combined with the limited project information that FEMA had available regarding grant funding levels, grant recipients, and grant purposes. DHS responded to the finding by noting that it had determined that starting in FY 2013, it will merge all four programs into a single one, to be called the National Preparedness Grant Program. You mentioned this consolidation in your testimony as well as in your responses to my Questions for the Record (QFRs) from your last appearance before the Committee.

Please describe in detail the structure of the National Preparedness Grant Program, including its methods for preventing overlap and duplication of funding (I note that you referred to MOUs among DHS components in your responses to the QFRs; please describe what kind of coordination they require.)

Will this program require authorization from Congress in legislation?

According to DHA OIG audits of grants to California, New York, and Nevada under the Urban Areas Security Grant Program, these states did not prepare contingency plans for funding if federal money was not available for future planned expenditures. OIG stated that several years' worth of funding by DHS "has created a perception that this funding will continue indefinitely as would be the case for entitlement programs, such as Medicare and Social Security." How will the consolidated grant program prevent this from happening?

According to OIG reports on Louisiana, Maryland, Missouri, Pennsylvania, Nevada, New Jersey, New York, South Carolina, and Texas, these states did not have "measurable

Question#:	21
Topic:	grant program 2
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

goals and objectives" for their strategic plans for homeland security, in accordance with DHS's guidance requiring such goals and objectives. How will the consolidated grant program ensure that grantees have measurable goals and objectives for their homeland security strategies?

Numerous OIG audits of states revealed failures to monitor subgrantees' use of grant funds, leading to lack of compliance by subgrantees with appropriate grant management requirements. How will this consolidated program ensure compliance by subgrantees?

Response: The FY 2013 President's Budget outlined a vision for a new National Preparedness Grant Program (NPGP) designed to develop, sustain, and leverage core capabilities across the country in support of national preparedness. DHS has been supporting state, local, tribal, and territorial efforts across the homeland security enterprise to build capabilities for the past nine years, awarding more than $35 billion in funding. Through these federal investments, grantees have developed significant capabilities at the local level to prevent, protect against, mitigate, prepare for, respond to and recover from threats and hazards of all kinds. As we look ahead, in order to address evolving threats and make the most of limited resources, the NPGP will utilize existing governance structures to focus on building and sustaining core capabilities associated with the five mission areas within the National Preparedness Goal (NPG) that are both readily deployable and cross-jurisdictional, helping to elevate nationwide preparedness. FEMA is currently soliciting feedback from our partners on this proposal to help guide further development of the proposal. The Administration looks forward to working with Congress and stakeholders to ensure the NPGP enables the whole community to build and sustain, in a collaborative way, the core capabilities necessary to prepare for incidents that pose the greatest risk to the security of the Nation.

NPGP consolidates current grant programs into one overarching program (excluding Emergency Management Performance Grants and fire grants), which will support the recommendations of the Redundancy Elimination and Enhanced Performance for Preparedness Grants Act (REEPPG) and streamline the grant application process. This will enable grantees to build and sustain core capabilities outlined in the National Preparedness Goal instead of requiring grantees to meet the mandates from multiple individual, often disconnected, grant programs. NPGP also provides grantees with maximum visibility of all of the projects being implemented with federal preparedness grant funding, which reduces overlap and duplication of spending. This increased efficiency will enable grantees to focus on how federal funds can add value to the jurisdiction's prioritization of threats, risks and consequences while contributing to national preparedness capabilities.

Question#:	21
Topic:	grant program 2
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

In addition, all states and territories receiving homeland security grant funding are required to complete a comprehensive Threat Hazard Identification and Risk Assessment (THIRA) which provides an approach for identifying and assessing risks and associated impacts across their state/territory. The coordination element described in the new grants vision will assist grantees in their efforts to address the gaps identified in their THIRA, while building important statewide and national capabilities. This incentivizes grantees to fund areas that are in the greatest need of supplemental homeland security funding, and discourages the practice of continually funding areas that may not need continued funding.

Finally, NPGP requires grantees to match their proposed investments to one or more specific core capabilities and incorporates effectiveness measures that facilitate accountability. To facilitate the sharing of capabilities via mutual aid, the NPGP requires that capabilities built with grant funding be made available for use in a mutual aid system and requires grantees to maintain membership in the Emergency Management Assistance Compact (EMAC).

In response to the other questions, all of the grantees identified in the OIG reports as lacking measureable goals and objectives in their state strategies are required to update their strategies to meet this requirement. Along with the THIRA, grantees will be required to maintain a state strategy and a formalized monitoring process in place in order to ensure their sub-grantees are compliant with all grant requirements.

FEMA/GPD has developed several MOUs with other agencies including the Department of Transportation, DHS/Office of Infrastructure Protection, Transportation Security Administration, and Customs and Border Protection. The purpose of these MOUs is to further establish formal relationships with partnering agencies to identify gaps in funding as well as improve coordination and reduce redundancy.

Question#:	22
Topic:	grant program 3
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: The DHS Inspector-General wrote in its annual report on major management challenges facing DHS. "FEMA faces challenges in mitigating redundancy and duplication among preparedness grant programs...Since grant programs may have overlapping goals or activities, FEMA risks funding potentially duplicative or redundant projects." I was gratified to see that DHS is taking steps to reduce duplication through creation of the National Preparedness Grant Program. However, just as FEMA must be aware of, and avoid, duplicative grant-making within DHS, it must also ensure that its grants and other STTL support do not overlap with those of DOJ (as well as other government departments and agencies). In your responses to my QRFs from your last appearance before the Committee, you refer to discussions between FEMA and DOJ regarding coordination of grant programs and that these discussions "will hopefully lead to a Memorandum of Understanding (MOU)."

What is the status of those discussions and possible MOU?

Is DHS aware of any overlap between SHSP- and UASI-funded activities with similar activities funded by DOJ? Has DHS shared information on these programs with DOJ?

What is the relationship between DHS's training programs funded through the SHSP and UASI and DOJ's State and Local Anti-Terrorism Training (SLATT) Program?

Is DHS aware of any overlap between DHS training activities with similar activities performed through the SLATT Program? Has DHS shared information about its training programs with DOJ?

Response: During the development of the annual Funding Opportunity Announcements (FOA) for each of its grant programs, FEMA conducts regular outreach to Agencies and programs within the Federal Government including DOJ and HHS to ensure that our grant programs are complementary.

FEMA is participating in the DOJ sponsored National Institute of Justice Standards Steering Committee in order to coordinate development of equipment performance standards for law enforcement and corrections responders. The inaugural meeting of this group took place in January.

DHS preparedness grants complement those of the Department of Justice (DOJ) in areas related to law enforcement such as interoperable communications and support to fusion

Question#:	22
Topic:	grant program 3
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

centers. Whereas DOJ grants focus solely on law enforcement, DHS complements those efforts by encouraging the engagement of the entire first responder community including the fire service, emergency management, public health, health care and law enforcement in programs such as the National Suspicious Activity Reporting Initiative (NSI), the See Something, Say Something campaign, etc.

All Homeland Security National Training Program and Continuing Training Grant-provided curricula undergo a rigorous certification process to ensure content accuracy and validity, including cross-agency outreach to ensure courses are not duplicative. FEMA's National Training and Education Division (NTED) coordinate its law enforcement-related training with its training partners at DOJ's Office of Justice Program's (OJP) and the Nationwide Suspicious Activity Reporting Program Management Office. NTED also coordinates training programs with the OJP State and Local Anti-Terrorism Training Program, as well as National Suspicious Activity Reporting Initiative Analytic Training programs. FEMA also maintains the Federal Course Catalogue that tracks available, approved course curricula that may be provided with Homeland Security Grant Program funds. Inter-agency collaboration has allowed numerous agency partner-developed curricula to be added to this central depository, further minimizing the risk of duplicative course development.

Question#:	23
Topic:	fusion center
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: Please delineate precisely the resource contributions of DHS and DOJ to the Fusion Center Technical Assistance Program, including which department provides which services and how those delineations have been determined.

Response: DHS sponsors nine of the thirteen technical assistance services under the joint DHS/DOJ Fusion Process Technical Assistance Program. DHS is responsible for development and delivery of those services that are specifically intended to support the development and operation of fusion centers, including:

- Fusion Process Orientation and Development
- Fusion Center Security
- Fusion Liaison Officer Program
- Fusion Center and Fire Service Information Sharing
- Fusion Center and Emergency Operations Center Information Sharing and Coordination
- Fusion Center Communications and Outreach
- Fusion Center and Health Security Information Sharing and Coordination
- Fusion Center and Critical Infrastructure and Key resources Protection Information Sharing and Coordination
- Fusion Center Exchange Program

In FY 2011, over $1.6 million was allocated to the Fusion Process Technical Assistance Program through partnerships between the Office of Intelligence and Analysis (I&A), the Federal Emergency Management Agency (FEMA), the Office of Infrastructure Protection, the Office of Health Affairs, the Privacy Office, and the Office for Civil Rights and Civil Liberties.

DOJ sponsors the remaining four technical assistance services, which are more narrowly focused on information exchange and encourage the development of common information sharing systems and models, including:

- Privacy Training and Technical Assistance
- State and Local Anti-Terrorism Training
- National Information Exchange Model
- Fusion Center Technology Technical Assistance

Question#:	23
Topic:	fusion center
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

While DHS leads the development and delivery of fusion center specific services, and DOJ leads the delivery of information sharing/information technology services, all activities are jointly coordinated and often include participation from both Departments. Additionally, all materials developed and delivered in support of this program are reviewed through intra- and interagency partners, including the Federal Bureau of Investigation, Office of the Director of National Intelligence, Program Manager for the Information Sharing Environment, and state and local partners through the Criminal Intelligence Coordinating Council.

Question#:	24
Topic:	NSI
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: Regarding the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI):

Please delineate precisely the resource contributions of DHS and DOJ to the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI).

Response: The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) is a collaborative effort between a number of federal, state, local, and tribal agencies and organizations with counterterrorism responsibilities. The NSI strategy is to develop, evaluate, and implement common processes and policies for gathering, documenting, processing, analyzing, and sharing information about activities potentially related to terrorism. The long-term goal is for state, local, tribal, and federal law enforcement organizations, as well as private sector entities, to participate in the NSI, allowing them to share information about suspicious activity that is potentially terrorism-related.

The Department of Homeland Security (DHS) supports the NSI by helping to develop training courses for frontline personnel to recognize behavior potentially associated with terrorism, executive leadership regarding the purpose and function of the NSI, and analysts to better understand indicators of terrorism-related activity and how to vet SAR.

The Department also contributes support to the NSI in three specific areas: assignment of personnel, implementation of the NSI methodology throughout DHS operational Components, and analysis of information within the NSI.

DHS defers to DOJ for their expenditures related to NSI.

Question: How many Suspicious Activity Reports (SAR) have been sent to DHS and DOJ through the NSI?

Response: Suspicious Activity Reporting from NSI partners is made available to the Department via the Federated Search Tool which is managed by the NSI PMO. As of August 10, 2012, there were 28,901 SAR in the NSI Federated Search.

Question: How many SARs have resulted in intelligence products being written for distribution to Fusion Centers or other consumers?

Response: DHS I&A analysts have produced several NSI-derived intelligence products

Question#:	24
Topic:	NSI
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

to date. They include:

- 6 SAR Indicators Roll Call Release (RCR) products. An additional 11 SAR Indicator RCRs are currently in various stages of coordination;
- 2 SAR-related Homeland Intelligence Today (HIT) articles;
- Provided responses to 33 SAR-related Requests for Information (3 external, 30 internal); and
- 3 editions of the SAR Top-Five, which highlights the five behavioral indicators associated with SAR that are of particular interest to DHS I&A at that time.
- 2 SAR Indicator Training Workshops on HS-SLIC Weekly Analytic Chat. An additional 14 monthly presentations are scheduled to occur in the future.

Additionally, since July 2011, a group of DHS analysts in I&A's Homeland Counter Terrorism Division have analyzed approximately 7,600 reports from 27 agencies/fusion centers. This effort will develop a baseline of the reporting in NSI to assess any patterns, trends, tactics, techniques, and procedures. At the end of the project, the analysts will have reviewed and assessed a representative sample of over 7,800 reports that were submitted through the NSI.

Question: How many SARs have resulted in DHS or FBI investigations being opened?

Response: DHS defers to the FBI as the statutory lead for all counter terrorism investigations.

Question: How many of those investigations have resulted in legitimate threats being identified?

Response: DHS defers to the FBI as the statutory lead for all counter terrorism investigations.

Question: How many of those investigations have resulted in criminal indictments being brought?

Response: DHS defers to the FBI as the statutory lead for all counter terrorism investigations.

Question: How many of those criminal indictments have led to convictions or guilty pleas?

Response: DHS defers to the FBI as the statutory lead for all counter terrorism investigations.

Question#:	25
Topic:	CICC
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: Please describe DHS's role in the operations of the Criminal Intelligence Coordinating Council (CICC) and the Global Intelligence Working Group (GIWG), led by DOJ's Bureau of Justice Assistance.

Response: DHS is an active partner with the CICC and GIWG. DHS personnel participate in monthly conference calls and quarterly meetings, including the CICC Privacy Committee and Training Committee meetings. DHS utilizes the CICC and GIWG as a mechanism to provide feedback on the development phase of new services and materials for the joint DHS/DOJ Fusion Process Technical Assistance Program, as well as other interagency resources that are used to standardize training across Departments and agencies (e.g. *Common Competencies for Intelligence Analysts*; *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise*; 28 CFR Part 23 training; etc.).

Question#:	26
Topic:	Fast & Furious
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: When you visited Arizona after Border Patrol Agent Brian Terry's death, you met with individuals from the FBI and U.S. Attorney's office who were aware the guns found at Agent Terry's murder scene were tied to an ongoing Phoenix ATF investigation. Documents produced by the Justice Department suggest that at the DHS press conference announcing Agent Terry's death that morning, FBI Special Agent in Charge Nate Grey advised Tucson Assistant U.S. Attorney Shelley Clemens that the two guns were tied to an ongoing Phoenix ATF investigation. Clemens immediately notified her supervisor, U.S. Attorney Dennis Burke, who confirmed that evening that the guns tied back to Operation Fast and Furious. I understand these events on December 15, 2010, to be two days before your visit to Arizona.

While you were in Arizona, did anyone mention to you any connection between the guns found at the scene of Agent Terry's death to an ATF investigation, even if not by the name Fast and Furious? If yes, please describe in detail all individuals who communicated this information as well as the full substance of what they communicated.

When did you first learn of this connection? Please describe in detail from what source you first learned this information, the circumstances of your learning it, and the full substance of what you learned.

Response: To the best of my recollection, no one mentioned to me any connection between the guns found at the scene of Agent Terry's death to an ATF investigation while I was in Arizona in December 2010. I do not specifically recall when I did learn of this connection. However, I believe I became aware of it in March 2011.

Question#:	27
Topic:	cooperation
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: When my staff was initially briefed on April 20, 2012, Secret Service's Office of Professional Responsibility (OPR) indicated that according to a Memorandum of Agreement with the DHS Inspector General (IG), OPR would be conducting the investigation of Secret Service on their own and only providing summaries of their interviews to the IG. However, when I asked you at the hearing about the IG's involvement, you replied that you "expect the IG to be conducting a full investigation." My staff's understanding is that the IG's entrance conference on the matter did not take place until May 2, 2012.

Please provide the Memorandum of Agreement between Secret Service and the DHS Office of the Inspector General.

Response: Please see attached MOA.

Question: When was the decision made for the IG to conduct a full investigation, rather than merely observing the Secret Service OPR investigation?

Response: April 26, 2012.

Question: When were you informed of that decision?

Response: April 27, 2012.

Question#:	28
Topic:	Cook County
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: There was a lot of discussion during the hearing about Cook County's ordinance, and how your Department was handling the issue. Despite the strong stance taken by you and Director Morton, nothing has changed and the safety of the public is still at risk. Please provide an update on what options are being discussed on how to deal with the ordinance and its impediment on ICE's mission. Also, please outline what discussions have taken place with the Department of Justice about withholding SCAAP funds for places like Cook County.

Response: U.S. Immigration and Customs Enforcement (ICE) is engaged with the Cook County Board of Commissioners on this issue. ICE has discussed several alternatives regarding the ordinance to address Cook County's concerns including the formation of a joint working group, the admission of ICE officers into the Cook County detention facility in exchange for ICE bearing any associated costs, and the assurances that ICE will either assume custody of aliens on their scheduled release date (with 24 hours notice) or, as permitted by law, reimburse the county for prolonged detention expenses (to be negotiated with the Cook County Sheriff). DHS and ICE are committed to ensuring the safety of American communities and will continue to consider all options, both financial and legal, to encourage Cook County officials to honor ICE detainers.

On September 21, 2012, ICE sent a letter to the Bureau of Justice Assistance, within the Office of Justice Programs at the U.S. Department of Justice (DOJ), indicating that ICE has completed its review of the fiscal year (FY) 2012 State Criminal Alien Assistance Program (SCAAP) funding requests. The letter informed DOJ that the agency's ability to accurately verify the immigration status of criminal aliens detained by jurisdictions that restrict ICE's access to information and persons who may be in the country unlawfully is unreliable. Accordingly, while ICE did complete its review of all FY 2012 SCAAP requests received from DOJ, ICE could not accurately verify submissions from Cook County, Illinois, and Santa Clara County, California. Both counties have adopted local policies that greatly restrict cooperation with ICE and prohibit law enforcement from honoring ICE detainers placed on aliens held in county facilities.

Question#:	29
Topic:	detention standards
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: In February, ICE announced changes to its detention standards, providing more accommodations and benefits to illegal aliens. The manual says that transgender detainees who were already receiving hormone therapy when taken into ICE custody shall have continued access. Does that mean taxpayers will be paying for these therapies, or will the costs of the therapy be the burden of the detainee?

Response: U.S. Immigration and Customs Enforcement (ICE) pays for medically necessary expenses of all detainees while they are in ICE custody, including hormone therapy for detainees who were already receiving hormone therapy, and where continued use is determined medically necessary to prevent adverse medical complications. This policy is in line with the policy of the Department of Justice, Bureau of Prisons, and is the accepted industry standard.

The 2011 Performance Based National Detention Standards (PBNDS) state:

"Transgender detainees who were already receiving hormone therapy when taken into ICE custody shall have continued access. All transgender detainees shall have access to mental health care, and other transgender-related health care and medication based on medical need. Treatment shall follow accepted guidelines regarding medically necessary transition-related care."

Question#:	30
Topic:	immigration reform
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: The draft memo written by four USCIS employees in 2010 titled, "Administrative Alternatives to Comprehensive Immigration Reform," included several options "to promote family unity, foster economic growth, achieve significant process improvements and reduce the threat of removal for certain individuals present in the United States without authorization." Please outline which options have been implemented (whether in the form described in the memo or otherwise), and which options are being considered or discussed internally.

Response: DHS does not comment on draft documents that do not and should not be equated as official action or policy, nor does it share internal deliberations which do not constitute official policy.

Question#:	31
Topic:	work authorizations
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: For the last five years, please provide all statistics available regarding employment authorizations issued pursuant to 8 C.F.R. § 274A.12, broken down by class of aliens, including those issued employment authorizations after being granted deferred action, parole, or if their case was administratively closed.

Response: The attached I-765 Approvals by Class Preference workbook contains the information requested. The second tab explains the various employment authorization codes.

Question#:	32
Topic:	L-1 Visa Fraud
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: Please provide a status update on the L-1 Visa Benefit Fraud and Compliance Assessment.

Response: In late September 2011, USCIS awarded a contract to an outside firm, Booz Allen Hamilton, to assess the methodology and scientific rigor of the L-1A visa Benefit Fraud and Compliance Assessment (BFCA) report. In the near future, USCIS expects a draft report from the contractor that will analyze the analytical scope, sample size, and relevance of the earlier L-1A visa BFCA study. Based upon the findings in the draft report about the methodology used in the BFCA, USCIS will determine the appropriate next steps.

Question#:	33
Topic:	Visa Security Program
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: What is the status of the Visa Security Program, specifically how many units are deployed and where are they deployed? Do you believe that the Visa Security Program should be expanded to all 57 visa-issuing posts determined to be high risk by DHS and the Department of State? If so, how much would it cost to expand the VSP to all high-risk posts? Why haven't you asked Congress for that amount as part of your proposed budget?

Response:

LAW ENFORCEMENT SENSITIVE START

[redacted]

Question#:	33
Topic:	Visa Security Program
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

LAW ENFORCEMENT SENSITIVE END

The total estimated initial cost to expand the VSP to all high-risk posts is approximately $79.2 million, with an additional $68.4 million in annual recurring operational costs thereafter; however, VSP deployment depends on NSDD-38 request approval and the approval of chiefs of mission at post. Both of these approval processes can contribute to significant deployment delays, with the entire process taking up to two years for each location.

U.S. Immigration and Customs Enforcement (ICE) continues to conduct multiple joint-site visits with DOS to determine the best opportunities for deployment, including the availability of physical space at post. The estimated costs to expand to additional high-risk posts accounts for $2.2 million required to open each office at the remaining 36 high-risk, visa-issuing posts. Once opened, each post requires estimated recurring costs of $1.9 million each year in order to sustain operations.

There has been significant expansion in the VSP in recent years, and ICE remains committed to fully staffing and equipping the program. The FY 2013 Budget supports efforts to leverage IT solutions and the capabilities of our law enforcement and intelligence community partners to increase ICE's efficiency in screening visa applications in order to identify patterns and potential national security threats. This will establish greater efficiencies to our Visa Security Program, allowing for research and analytic activities to be carried out in the United States and investigative and law enforcement liaison work overseas.

Question#:	34
Topic:	Guatemala
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: The country of Guatemala has officially requested that the administration provide TPS to residents of their country. Are there internal discussions taking place to provide Temporary Protected Status to Guatemalans? Please explain the Department's position on any such proposals.

Response: DHS is in the process of evaluating Guatemala's request for TPS by carefully considering the conditions in Guatemala, including reviewing the information provided by the Government of Guatemala. In addition to its own evaluation of conditions, DHS also consults with the Department of State and considers its independent assessment. DHS may consult with other federal agencies as well. DHS continues to monitor whether it is safe for nationals to return to Guatemala. While DHS completes its statutorily mandated assessment of the conditions in Guatemala in order to make a final determination regarding TPS for Guatemala, Guatemalans affected may be assisted by policies offered by U.S. Citizenship and Immigration Services, a component of DHS. These policies can be found on the "Special Situations" page of the humanitarian section of the website at www.uscis.gov.

Question#:	35
Topic:	misconduct
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Patrick J. Leahy
Committee:	JUDICIARY (SENATE)

Question: I appreciate your commitment to a prompt and thorough investigation of misconduct by U.S. Secret Service agents in Colombia. At the hearing, in response to my question of whether the April 2012 incident in Colombia was the first time something like this has happened, you stated that "over the past 2-1/2 years, the Secret Service Office of Professional Responsibility has not received any such complaint." You also said that the Secret Service Office of Professional Responsibility (OPR) was going back beyond that timeframe and would be going through "all of the records."

The Secret Service has been housed within the Department of Homeland Security (DHS) since the Department was established in 2003. Does OPR have full access to its records prior to 2003?

Response: Yes.

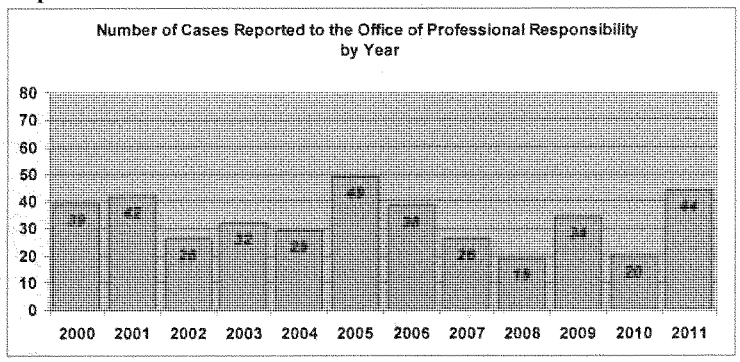
Question: Assuming that OPR currently has full access to its records how far back in time do the records of complaints kept by OPR go?

Response: The Secret Service Office of Professional Responsibility was previously known as the Office of Inspection and was established in 1950. The Secret Service Office of Professional Responsibility currently has cases that date back to 1963 and created a database for these cases in 1997.

Question: What is the breakdown by year of the number of complaints received by OPR?

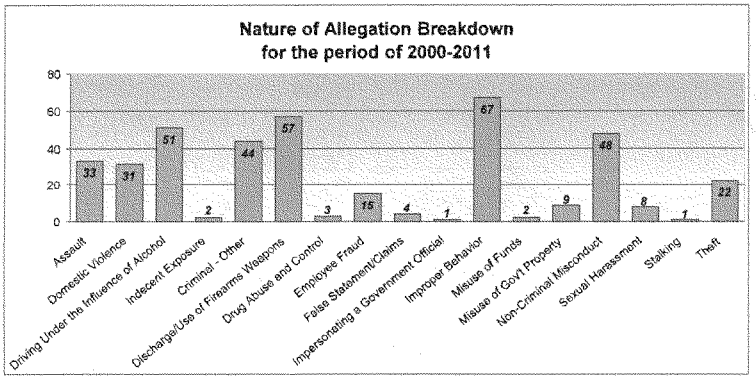
Question#:	35
Topic:	misconduct
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Patrick J. Leahy
Committee:	JUDICIARY (SENATE)

Response:



Question: What is the breakdown by the nature of the allegation of the complaints received by OPR each year?

Response:



Question: What percentage of the complaints received by OPR each year result in disciplinary action? Please specify the action taken.

Question#:	35
Topic:	misconduct
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Patrick J. Leahy
Committee:	JUDICIARY (SENATE)

Response:

Calendar Year	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	Total
Inspection Cases	39	42	26	32	29	49	38	26	19	34	20	44	398
Employee Relations Board (ERB) Cases	17	27	20	19	21	25	23	17	10	19	8	24	230
Percent	43.6%	64.3%	76.9%	59.4%	72.4%	51.0%	60.5%	65.4%	52.6%	55.9%	40.0%	54.5%	57.8%

Actions taken ranged from reprimand to removal from employment, and in some cases employees resigned prior to administrative action being affected.

Question#:	36
Topic:	dispute
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Patrick J. Leahy
Committee:	JUDICIARY (SENATE)

Question: If not for the dispute that an agent reportedly had with a foreign national woman who he brought back to his hotel room, we might have never known about what happened in Colombia. The number of agents found to have brought foreign national women back to their rooms—while only a small percentage of the agents who were in Colombia for President Obama's trip—was shocking.

In addition to reviewing the historical complaints received by OPR, what else is being done to investigate whether there is a cultural problem within the Secret Service that allowed the incident in Colombia to happen?

Response: In April of 2012, Director Sullivan established the Professionalism Reinforcement Working Group (PRWG). The PRWG is conducting a comprehensive review of the Secret Services' values and professional standards of conduct. This process will include evaluation of policy related to employment standards and background investigations; patterns of discipline related to misconduct; ethics training; and all law, policies, procedures and practices related to the same. To facilitate this effort, the PRWG will undergo the following actions:

1) Collect and analyze comprehensive information related to organizational performance and accountability.

2) Identify best practices of other federal law enforcement agencies.

3) Prepare an action plan with recommendations for reinforcing professional conduct.

4) Provide additional ethics training courses for all employees. The goal is to provide enhanced ethics training to all supervisors, mid-level managers and front line field agents, Officers and Administrative, Professional and Technical employees.

Question#:	37
Topic:	press reports
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Patrick J. Leahy
Committee:	JUDICIARY (SENATE)

Question: Following your appearance before the Committee, there were press reports about alleged misconduct by U.S. Secret Service agents in connection with President Obama's visit to El Salvador in March 2011.

Is the Department investigating this allegation as well?

Response: At this time the U.S. Secret Service is unaware if the DHS-OIG will investigate this matter. Respectfully, DHS-OIG would be best suited to answer this question.

Question: Can you assure us that if additional allegations regarding misconduct of U.S. Secret Service agents emerge that those allegations will be fully investigated?

Response: Yes, absolutely. The Secret Service is committed to investigating any allegation of misconduct where witnesses are willing to come forward with facts, provide information, be interviewed and assist Secret Service Inspectors.

If anyone has personal knowledge concerning misconduct by a Secret Service employee, they may contact the OPR directly or the DHS-OIG.

Question#:	38
Topic:	Arizona v. United States
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Patrick J. Leahy
Committee:	JUDICIARY (SENATE)

Question: The Supreme Court is recently heard arguments about the constitutionality of a controversial law enacted in Arizona dealing with state-level immigration enforcement. There has been a lot of rhetoric around the efforts of some states to enact this type of legislation. Much of that rhetoric involves claims that the Federal Government is refusing to deal with immigration. For example, when the Governor of Arizona signed the legislation, she stated that it was needed because the "crisis" of illegal immigration was something the Federal Government has "refused" to fix.

Do you think this is a fair characterization of your efforts as the Secretary of Homeland Security or our efforts in Congress?

Is it an accurate statement of the administration's position on this issue?

Response: We believe the Supreme Court's decision in *Arizona v. United States* serves as an important reminder of the federal government's central role in effective administration of our borders and immigration system. Over the past three and a half years, the Department of Homeland Security (DHS) has dedicated historic levels of personnel, technology, and resources in support of the enforcement of our immigration laws and border security efforts. Most recently, the President's Fiscal Year (FY) 2013 Budget Request continues these efforts by supporting the largest deployment of law enforcement officers to the frontline in our agency's history: 21,370 Border Patrol agents, over 1,200 Air and Marine agents, and 21,186 U.S. Customs and Border Protection (CBP) officers, who work with state, local, and federal law enforcement in targeting illicit networks trafficking in people, drugs, weapons, and money. Over the last year, we have brought greater unity to our enforcement efforts, expanded collaboration with other agencies, and improved response times.

The results of DHS's comprehensive and coordinated efforts are clear. Border Patrol apprehensions—a key indicator of illegal immigration—have decreased 53 percent in the last three years and are less than 20 percent of what they were at their peak. Indeed, illegal immigration attempts have not been this low since 1971. Violent crime in border communities also has remained flat or fallen over the past decade, and statistics have shown that some of the safest communities in America are along the border. From Fiscal Years 2009 to 2011, DHS also seized 74 percent more currency, 41 percent more drugs, and 159 percent more weapons along the Southwest border as compared to Fiscal Years 2006 to 2008.

Question#:	38
Topic:	Arizona v. United States
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Patrick J. Leahy
Committee:	JUDICIARY (SENATE)

DHS has undertaken an historic effort to enforce immigration laws in a way that is smart, effective, and that maximizes the resources to enhance public safety, border security, and the integrity of the immigration system by focusing on the removal of convicted criminals, threats to public safety and national security, repeat immigration violators, recent border crossers, and immigration fugitives.

Immigration and Customs Enforcement (ICE) expanded the use and frequency of investigations and programs, like Secure Communities, that help ICE identify criminals and gang members in our jails and remove them from our streets from 14 jurisdictions in 2008 to 3,074 today, which represents 97% of all jurisdictions, including all jurisdictions along the Southwest border. ICE plans to expand this program to all law enforcement jurisdictions nationwide by 2013. As of July 31, 2012, more than 159,400 illegal aliens convicted of crimes, including more than 58,750 convicted of multiple felony offenses or aggravated felony offenses like murder, rape and the sexual abuse of children were removed from the United States after identification through Secure Communities.

ICE is also committed to ensuring the Secure Communities program respects civil rights and civil liberties. ICE works closely with law enforcement agencies and stakeholders across the country to ensure the program operates in the most effective manner possible.

To further deter individuals from illegally crossing our border, ICE has prioritized the apprehension of recent illegal aliens and repeat immigration violators. Between Fiscal Years 2009 to 2011, ICE made over 30,936 criminal arrests along the Southwest border, including 19,563 arrests of drug smugglers and 4,151 arrests of human smugglers.

Overall, in Fiscal Year 2011, ICE removed nearly 397,000 individuals – the largest number in the agency's history. Ninety percent of these removals fell within one of ICE's priority categories, and 55 percent, or more than 216,000 of the people removed, were convicted criminal aliens – an 89 percent increase in the removal of criminals from Fiscal Year 2008. This total includes more than 87,000 individuals convicted of homicide, sexual offenses, dangerous drugs, and driving under the influence. Of those removed without a criminal conviction, more than two-thirds in Fiscal Year 2011 fell into our priority categories of recent border crossers or repeat immigration law violators.

Question#:	39
Topic:	report
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Patrick J. Leahy
Committee:	JUDICIARY (SENATE)

Question: Two major newspapers reported recently about a report from the Pew Hispanic Center, which finds tremendous decline in migration from Mexico to the United States. The report and articles cited a number of factors, including increased immigration enforcement efforts as responsible for this trend.

Are you seeing evidence that your efforts are making a difference?

Response: Border Patrol apprehensions—a key indicator of illegal immigration—have decreased 53 percent in the last three years and are less than 20 percent of what they were at their peak. Illegal immigration attempts have not been this low since 1971.

Question#:	40
Topic:	Border staffing
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Patrick J. Leahy
Committee:	JUDICIARY (SENATE)

Question: Your department has increased overall security staffing levels along the Northern Border over the past decade. But it appears that the vast majority of these new positions are with the Border Patrol, not with CBP officers and agriculture specialists at the ports-of-entry.

I appreciate the budget constrains you face now – and the increasing demands along the Southern Border – but I remain concerned about the low staffing levels at Vermont's ports-of-entry, where I have received some troubling reports involving overall safety practices, security procedures, and the morale and welfare of CBP officers.

In addition, Autoroute 35, a new highway the Canadians are building between Montreal and the U.S.-Canada border at Highgate Springs, could bring 30 percent more traffic to Vermont's border crossings starting next year.

Are planning efforts underway to address the staffing and infrastructure needs at Vermont's ports-of-entry and at other ports along the Northern Border?

Response: Planning efforts are underway to address the infrastructure needs at land ports of entry (LPOE) along the northern border to include select ports located in Vermont. Though no immediate infrastructure planning activities are in place for the Highgate Springs LPOE, CBP will be closely monitoring a Vermont Agency of Transportation led transportation study to reevaluate the anticipated traffic impact associated with the opening of Autoroute 35. This study, scheduled to conclude in July 2013, will take into consideration the latest cross-border traffic updates from 2011 and evaluate the impact of recent LPOE modernization efforts, to include the replacement of the Pinnacle Road, Vermont LPOE using funds received through the 2009 American Recovery and Reinvestment Act.

Question#:	41
Topic:	prosecutorial discretion
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Patrick J. Leahy
Committee:	JUDICIARY (SENATE)

Question: You and Immigration and Customs Enforcement Director John Morton have developed and are implementing a policy to exercise prosecutorial discretion in some immigration enforcement cases with respect to very low priority aliens. This policy is consistent with your broader policy to use law enforcement resources in a smarter, more effective manner. You have been criticized for this policy, with some suggesting that you are bypassing Congress.

Could you explain how this policy assists your immigration enforcement efforts? Is it fair to say that this policy is primarily directed toward improving the use of law enforcement resources in order to prioritize the worst offenders?

How would you respond to criticism that this policy is an attempt to circumvent Congress in order to provide undocumented immigrants with relief or benefits?

Response: The Department of Homeland Security (DHS) must prioritize the use of its immigration enforcement resources to ensure the removal of those aliens who represent our enforcement priorities, specifically convicted criminals, repeat immigration violators, recent border crossers, and immigration fugitives.

The exercise of prosecutorial discretion is inherent in the execution of our immigration laws and practiced by DHS special agents, officers, and attorneys. For decades, DHS, and previously the Immigration and Naturalization Service, has exercised prosecutorial discretion in order to prioritize the use of its immigration enforcement resources. As the U.S. Supreme Court noted in its recent decision on the Arizona immigration law, "A principal feature of the removal system is the broad discretion exercised by immigration officials." Moreover, the use of prosecutorial discretion, as embodied in DHS's policy guidance, aligns fully with the spirit of the November 4, 1999 letter signed by a bipartisan group of 27 Members of Congress,[1] which referred to the exercise of discretion as a means of alleviating "hardship" and to some deportations as "unfair." It is important to note that this initiative is conducted on a case-by-case basis and provides no legal immigration status.

---

[1] *See Guidelines for Use of Prosecutorial Discretion in Removal Proceedings*, letter to Janet Reno, Attorney General, and Doris M. Meissner, Commissioner, Immigration and Naturalization Service, from Representatives Hyde, Frank, Smith, Jackson Lee, McCollum, Frost, Barrett, Berman, Bilbray, Brown, Canady, Cubin, Deal, Diaz-Balart, Dreier, Filner, E.B. Johnson, S. Johnson, Kennedy, Martinez, McGovern, Meehan, Sensenbrenner, Shays, Waxman, Granger, Green, and Rodriguez (November 4, 1999).

Question#:	42
Topic:	Officers
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Patrick J. Leahy
Committee:	JUDICIARY (SENATE)

Question: In recent reports and congressional testimony, the DHS Inspector General has reported a substantial number of open corruption and other investigations into CBP and Border Patrol personnel. And there have been recent reports of what appears to involve the use of exeessive force by CBP personnel. I recognize and appreciate the very difficult job these officials have, but it is critical that all Federal law enforcement officials maintain a very high level of professionalism and integrity.

Are you concerned about the number of investigations that the Inspector General has reported and is pursuing?

Response: The Department of Homeland Security (DHS) takes seriously allegations of excessive use of force and employee misconduct. We do not tolerate abuse within our ranks. Such allegations are thoroughly investigated, and U.S. Customs and Border Protection (CBP) fully cooperates in investigations involving use of force issues. If employee misconduct is substantiated, timely and appropriate corrective action will be initiated.

All allegations of misconduct are documented and referred to the Office of Inspector General (OIG) for independent review and assessment. Some cases are retained by the OIG for investigation while others are referred back to the component for appropriate handling. The OIG is in the process of transferring 478 cases to ICE's Office of Professional Responsibility (OPR) agents who will investigate cases with the support of CBP's Office of Internal Affairs (IA). In addition, DHS's Office for Civil Rights and Civil Liberties (CRCL) investigates civil rights and civil liberties complaints filed by the public regarding DHS policies or activities, or actions taken by DHS personnel.

Question: What steps have you taken in response to the Inspector General's work to ensure that along with rapid growth in the ranks of CBP and Border Patrol personnel, your screening and training procedures are keeping pace?

Response: In accordance with The Anti-Border Corruption Act of 2010 (Pub. L. No. 111-376), CBP is on track to implement polygraph examinations on 100 percent of law enforcement officer candidates by the end of FY 2012. The Agency will further comply with Pub. L. No. 111-376 by continuing timely initiation of all periodic reinvestigations.

In addition, CBP has a robust integrity training program for all employees. Throughout an employee's career, CBP provides training that focuses on integrity, ethics, and ethical

Question#:	42
Topic:	Officers
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Patrick J. Leahy
Committee:	JUDICIARY (SENATE)

decision making as part of an anti-corruption continuum. When employees initially join CBP they receive training promoting workforce integrity as part of CBP's New Employee Orientation program. Newly hired CBP law enforcement officers receive an expanded level of mandatory integrity and ethics instruction as part of the basic training curriculum.

Recurring integrity training is also an integral part of the advanced and specialized training for CBP employees beyond their initial entry on duty. This training, combined with proper leadership, oversight, and management at all levels of the agency fosters a culture of personal accountability and integrity within CBP. It clearly communicates the standards of conduct with which all CBP employees must comply and identifies the consequences of engaging in inappropriate behavior. Most importantly, periodic in-service training equips CBP employees with the tools they need to recognize, report, and respond to integrity challenges they will encounter both on- and off-duty.

Our focus on integrity is not limited to our non-supervisory personnel. CBP supervisory and leadership training programs such as Supervisory Leadership Training, Incumbent Supervisory Training, the Second Level Command Preparation, the CBP Leadership Institute, and the Department's Senior Executive Service Candidate Development Program incorporate classroom instruction and a series of practical exercises that prepare CBP leaders to guide and direct the workforce in a manner that promotes personal integrity and accountability through critical thinking and integrity-based, ethical decision making.

Question#:	43
Topic:	NCTC
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Patrick J. Leahy
Committee:	JUDICIARY (SENATE)

Question: The Attorney General and the Director of National Intelligence recently released new guidelines governing the acquisition and retention of data by the National Counterterrorism Center (NCTC). Under these new guidelines, it is now conceivable that the NCTC could retain vast amounts of data regarding U.S. persons for up to 5 years – well beyond the six months that was allowed under the previous guidelines. I am concerned that 5 years seems like an awfully long time to be retaining and sifting through data about U.S. persons who may have no connection whatsoever to terrorism.

As DHS could be one of the agencies sharing entire datasets of information with the NCTC, do you agree that such vast amounts of data should be retained for up to five years?

What privacy laws, criteria, and factors will you consider in determining the length of time that DHS will permit NCTC to retain your Department's data?

Response: The Attorney General of the United States recently approved *Guidelines for Access, Retention, Use and Dissemination by the National Counterterrorism Center and other Agencies of Information in Datasets Containing Non-Terrorism Information* (AG Guidelines) that establish an outside limit for temporary retention—that is, retention of data for the purpose of determining whether it is terrorism-related—of five years for U.S. Person information obtained from certain datasets of other federal departments and agencies. These guidelines also preserve my authority to negotiate with NCTC the terms and conditions within Information Sharing Access Agreements (ISAAs) relating to, among other things, "privacy or civil rights or civil liberties concerns and protections."

With this in mind, I tasked a DHS Working Group, chaired by a representative from the Office of Intelligence and Analysis and comprised of representatives from the Office of the General Counsel, the Privacy Office, the Office for Civil Rights and Civil Liberties, the Office of Policy, and the various Departmental data stewards, to establish a framework for evaluating NCTC's data access requests and to make recommendations for the appropriate temporary retention periods for various datasets. The Working Group has settled on six factors for evaluating NCTC's request on a system-by-system basis:

<u>Data Sensitivity Factors</u>

- Factor 1: Circumstances of Collection
- Factor 2: U.S. Citizen and U.S. Legal Permanent Resident Content
- Factor 3: Sensitivity of Data Fields Requested

Question#:	43
Topic:	NCTC
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Patrick J. Leahy
Committee:	JUDICIARY (SENATE)

Operational Factors

- Factor 4: NCTC Operational Mission Benefits
- Factor 5: DHS Operational Mission Benefits
- Factor 6: DHS Steward Dataset Limits

As indicated by our development of this framework, the Department does not reflexively permit our datasets containing U.S. Person information to be held in temporary retention by NCTC for five years.

All sharing between DHS and NCTC must be consistent with both agencies' authorities as well as with the Privacy Act. Last year, NCTC and DHS completed five ISAAs which transferred five DHS travel and immigration benefit-related datasets to NCTC in bulk. The ISAA for each dataset includes express privacy provisions and reflects the Fair Information Practice Principles in a number of ways: establishing the authority of both DHS to share the data and NCTC to receive it; defining which directorates at NCTC could access the data and for what purposes; containing an explicit reference to the applicable Routine Use within the system's Privacy Act System of Record Notice; requiring NCTC to report to DHS on their use of our data; and permitting audits of their compliance with the terms of the agreements. In addition, after the agreements were signed, to enhance transparency, the DHS Privacy Office published Privacy Impact Assessment updates for four of the five impacted systems, disclosing the sharing and the terms and conditions within the agreements that protect privacy. The fifth system already had a PIA providing general transparency of this type of sharing.

I am confident that the continued engagement of both the Privacy Office and the Office for Civil Rights and Civil Liberties will ensure that DHS considers appropriate privacy, civil rights, and civil liberties protections in our information-sharing activities.

Question#:	44
Topic:	287(g)
Hearing:	Oversight of the Department of Homeland Security
Primary:	The Honorable Patrick J. Leahy
Committee:	JUDICIARY (SENATE)

Question: Section 287(g) of the Immigration and Nationality Act permits DHS to enter agreements with state and local law enforcement entities to assist in the enforcement of immigration laws. Following the Justice Department's investigation and findings into the policing practices in the Maricopa County Sheriff's Office, released in December of 2011, you terminated the County's 287(g) agreement.

Could you describe what led to your decision to terminate the County's 287(g) agreement?

You have also announced your intention not to enter any new 287(g) agreements going forward.

What was the basis for this decision?

Response: The U.S. Department of Homeland Security (DHS) has followed closely the U.S. Department of Justice's (DOJ) investigation and findings related to the policing practices of the Maricopa County Sheriff's Office (MCSO) and subsequent lawsuit alleging a pattern or practice of discriminatory and unconstitutional law enforcement practices. Discrimination undermines law enforcement and erodes the public trust. DHS first terminated MCSO's 287(g) task force task force agreement when DOJ initiated its investigation of MCSO, and then terminated MCSO's jail model agreement and restricted the MCSO's access to Secure Communities technology when DOJ issued its findings of unconstitutional and discriminatory policing by MCSO.

Further, ICE is discontinuing the least productive 287(g) task force agreements and will also suspend consideration of any requests for new 287(g) task forces. The basis for this decision is that task force agreements are less efficient than jail model agreements at identifying and removing criminal aliens. For example, for 2011, task force model agreements resulted in an average of 35 removals per agreement, whereas jail model agreements resulted in an average of 450 removals per agreement. DHS will continue to focus our limited resources on enforcement priorities including criminal aliens, recent border crossers, repeat and egregious immigration law violators, immigration fugitives and employers who knowingly hire illegal labor.

U.S. Customs and Border Protection (CBP) Workforce Integrity Study

Final Report

15 December 2011

HOMELAND SECURITY
STUDIES AND ANALYSIS INSTITUTE
An FFRDC operated by Analytic Services Inc. on behalf of DHS
2900 South Quincy Street • Suite 800
Arlington, VA 22206-2233

Prepared for the
Department of Homeland Security
U.S. Customs and Border Protection

TASK LEAD

George Murphy

TASK TEAM

INSTITUTE
Catherine Meszaros
Anita Epstein
Eric Conklin

Michael Parkyn
Division Manager,
Workforce Analysis Division

Richard Kohout
Mission Area Director,
Counterterrorism, Borders and Immigration

HILLARD HEINTZE CONSULTANTS
Arnette Heintze
Terry Hillard
Matthew Doherty
Kenneth Bouche

Senior Leadership Council
Robert Davis
Thomas Streicher

U.S. CUSTOMS AND BORDER PROTECTION (CBP) WORKFORCE INTEGRITY STUDY

Final Report

December 15, 2011

Prepared for
Department of Homeland Security,
U.S. Customs and Border Protection

ACKNOWLEDGEMENTS

The Homeland Security Studies and Analysis Institute – Hillard Heintze study team expresses its gratitude to Major General Michael Lehnert, USMC (Ret.), Senior Policy Advisor in the Office of the Commissioner, who sponsored the project and advocated its objectivity throughout the work. The team also gratefully acknowledges the assistance of Jorge Gonzalez, Senior Policy Advisor in the Office of Policy and Planning, who facilitated information gathering and access to—including interviews with—principals, staff and subject matter experts both within CBP and the federal interagency.

The study team is deeply appreciative of the assistant commissioners, executive directors, division directors and chiefs, and their staffs, both within CBP Headquarters and in the field, who graciously shared their ideas, perspectives, and time with us. We would also like to recognize those officials whom we consulted across the federal interagency. Uniformly, all the professionals the study team spoke with shared the same concerns for workforce integrity and the firm commitment to stem corruption.

The study team expresses a special thanks to the CBP leadership for the opportunity to study and offer its perspectives on ways to promote integrity and counter corruption in the CBP workforce.

HOMELAND SECURITY STUDIES AND ANALYSIS INSTITUTE

Analytic Services Incorporated
2900 S. Quincy Street
Arlington, VA 22206
Tel (703) 416-3550 • Fax (703) 416-3530
www.homelandsecurity.org

Publication Number: RP11-17-04

TABLE OF CONTENTS

Contents

Executive Summary 1

Introduction 3

Background 3

Scope 4

Methodology 4

Report Structure 6

Section I. CBP Operational and Organizational Structure 7

Overview of Findings and Recommendations 7

CBP Workforce Integrity Strategy 7

CBP Disciplinary System 9

DHS OIG – CBP Organizational Structure 14

Border Corruption Task Force 19

Section II. Employee Recruitment and Vetting Process 22

Overview of Findings and Recommendations 22

Recruitment and Vetting Process 22

Suitability Determinations 26

Surge Hiring 28

Entry-Level Polygraphs 30

Section III. Integrity Training Process and Programs 34

Overview of Findings and Recommendations 34

Assessment 34

Ethics and Integrity Training Programs 34

Ethics and Integrity Training Themes 36

CBPnet Content and Messaging 39

Section IV. Metrics and Information Sharing Process 41

Overview of Findings and Recommendations 41

Assessment 41

Data Collection and Reporting 41

Data Analysis 43

Section V. Prevention, Detection, Monitoring, and Investigative Programs and Initiatives 47

Overview of Findings and Recommendations 47

Assessment 48

Random Drug Testing Program 49

Analytical Management Systems Control Office Program 50

Integrity Officer Program 51

U.S. Border Patrol Integrity Advisory Committee 52

Office of Internal Affairs, Integrity Programs Division (multiple programs and initiatives) 52

Integrated Policy Coordination Cell for Integrity 55

Section VI. Conclusions 56

Areas for Further Study 56

Disciplinary Process 56

Ethics and Integrity Training *57*
"Code of Silence" *57*
Surge Hiring *57*
Disciplinary Data Requirements *57*
Early Warning Systems Implementation *57*
Future Threats and Vulnerabilities *58*

Appendix A. Interview Issues and Questions for CBP Headquarters Officials 59

Appendix B. CBP Offices and Activities and Federal Interagency Counterparts Interviewed 61
CBP Headquarters Offices and Divisions 61
CBP Field Activities – El Paso, Texas 62
DHS and Federal Interagency 63

Appendix C. Workforce Integrity and Counter-Corruption Programs and Initiatives 64

Appendix D: Hillard Heintze Profiles 69

Appendix E. CBP Disciplinary Flow Chart 72

Appendix F. Recruiting and Vetting Flow Diagram 73

Appendix G. CBP Training Materials Reviewed and Next-step Recommendations 74
Training Materials Reviewed and Considered in the Study 74
Recommendations for Next Steps 74

Appendix H. CBP Statement of Policy and Intent: Integrity 77

List of Tables

TABLE 1. DHS INVESTIGATIVE RESOURCES AND CASE INVENTORIES 17
TABLE 2. CBP RECRUITMENT ATTRITION RATES 24

List of Figures

FIGURE 1. WORKFORCE INTEGRITY STRATEGY OUTLINE 9
FIGURE 2. TIMELINESS PRIOR TO DISCIPLINE REVIEW BOARD SESSION 11
FIGURE 3. TIMELINESS OF THE DISCIPLINE REVIEW BOARD PROCESS 12
FIGURE 4. DISCIPLINE REVIEW BOARD SESSIONS AND PROPOSALS/ACTIONS FOR FY10 13
FIGURE 5. RECRUITMENT AND VETTING PROCESS OVERVIEW 23

EXECUTIVE SUMMARY

The deployment of Department of Homeland Security (DHS) technology, physical infrastructure, and manpower along the border has made it more difficult now for drug trafficking and other transnational criminal organizations to conduct their illicit activities. This had led these organizations to infiltrate CBP through conspired hiring operations and compromise of the agency's existing officers and agents. Isolated acts of corruption have occurred.

The overwhelming majority of CBP officers and agents demonstrate the highest levels of integrity and perform their duties with honor and distinction every day. The wide range and number of CBP programs and initiatives on workforce integrity and counter-corruption also testify to the concern and attention that the agency places on these matters. But since October 1, 2004, 134 CBP agents and officers have been arrested, charged with, and convicted of mission critical corruption charges, including bribery, alien and/or narcotics smuggling, conspiracy, and fraud. This is a small minority of the workforce, but it represents a threat to our national security.

To address this threat, the Office of the Commissioner, U.S. Customs and Border Protection (CBP), Department of Homeland Security asked the Homeland Security Studies and Analysis Institute (the Institute) to evaluate existing integrity and counter-corruption programs within CBP, provide feedback on their effectiveness, identify areas of vulnerability, and recommend best practices and strategies for improving or replacing existing programs.

The Institute's study team, which included the law enforcement expertise of Hillard Heintze, approached this study according to five focal areas given by CBP: the operational and organizational structure, the employee recruitment and vetting process, the integrity training process and programs, the metrics and information sharing process, and the prevention, detection, monitoring, and investigation process. Through interviews and research of materials, the study team spent six months (the sponsor-directed length of this task) evaluating CBP's efforts, gathering findings on what works, what does not work, and what needs improvement—to help CBP deal better with corruption by better instilling integrity in its workforce.

The following highlights some of the key findings and recommendations of the study team.

- There is no comprehensive guidance for integrity programs and initiatives across the CBP organization. CBP therefore should implement an agency-wide workforce integrity strategy—one that establishes and articulates core concepts, approaches, control mechanisms, roles and responsibilities.
- The CBP's disciplinary system has so many processes that it does not foster timely discipline or exoneration. The agency therefore should rethink its disciplinary system toward more efficiency.

- The number of open cases and the protracted periods until many of them are closed (if ever) attest to the inefficiencies of the present DHS Office of Inspector General (OIG) – CBP organizational structure. The Commissioner should approach DHS leadership to change that structure for more efficient reporting, assignment, investigation and disposition of CBP workforce investigations.

- The FBI-led border corruption task forces (BCTFs) are effective in countering public corruption on the borders, including the corruption of CBP employees. The continued inclusion of CBP Office of Internal Affairs special agents in the national and regional BCTFs will foster effective criminal investigations and introduce efficiencies in combined counter-corruption efforts.

- Follow-on refresher ethics, integrity and counter-corruption training offered in the field take on a variety of forms. CBP should designate one authority on ethics and integrity training to coordinate courseware content and messaging throughout the agency.

- Emphasis in exactly what things CBP wants its employees to be doing in regards to the day-to-day application of ethics appears to be missing from the training materials/lesson plans. CBP should emphasize the practical application of ethics concepts within the day-to-day work of both first-line employees and supervisors, and better inform CBP staff of any organization-wide training.

- There is no comprehensive picture of workforce misconduct and corruption. CBP should consider implementing a central, unified tracking system for all the important disciplinary data that could be used to prevent, detect and deter misconduct and corruption.

- The organization of disciplinary data is lacking in several significant ways (e.g., some types of discipline appear to be missing from the data). CBP Labor and Employee Relations Division (LER) should consider the collection, breakdown and analysis of the disciplinary data sets discussed in this paper, and conduct further study to determine other data requirements.

- The Analytical Management Systems Control Office (AMSCO) has, for the three years since its inception, identified and corrected operational vulnerabilities that would have allowed potential opportunities for employee corruption. CBP should continue to pursue the AMSCO program's full potential.

- The Integrated Policy Coordination Cell for Integrity (Integrity IPCC) has yet to adopt and implement a charter governing its activities—without which there is no clear articulation of the cell's vision, purpose, goals, objectives, structure and methodologies. The Integrity IPCC should develop and implement a charter, including consideration of its activities since inception to broaden the scope of its initial intent.

INTRODUCTION

Since its inception, CBP has been dealing with corrupt individuals within its workforce, despite having an array of programs, initiatives, and other efforts aimed at instilling integrity and stemming corruption. In response to this persistent problem, the Office of the Commissioner, U.S. Customs and Border Protection, Department of Homeland Security asked the Homeland Security Studies and Analysis Institute to examine the nature of the corruption problem within this CBP workforce and existing vulnerabilities. Specifically, CBP asked the Institute to evaluate existing integrity and counter-corruption programs within CBP, provide feedback on their effectiveness, identify areas of vulnerability, and recommend best practices and strategies for improving or replacing existing programs.

The focus of this study is the law enforcement CBP workforce—CBP officers and Border Patrol agents—primarily at and between land ports of entry along the U.S. Southwest border.

Background

CBP is the largest uniformed federal law enforcement agency in the country, with about 59,000 employees. Law enforcement elements comprise the vast majority of this workforce, broken down as follows:

- 20,500 Border Patrol agents between the ports of entry (POEs)
- 20,600 CBP officers at air, land, and sea ports of entry
- 2,300 agricultural specialists
- 1,200 Air and Marine officers[1]

As a component of DHS, CBP is specifically charged with border and port security and administration and enforcement of customs and immigration laws and regulations. CBP employees routinely and frequently are in contact with both U.S. citizens and foreign nationals. In fiscal year (FY) 2009 alone, CBP officers and agents

- processed more than 352 million travelers at POEs;
- apprehended 463,000 illegal aliens at the border;
- arrested more than 84,000 fugitives wanted for crimes including murder, rape, and child molestation;
- seized more than 1.7 million prohibited agricultural materials and by-products; and

[1] U.S. Customs and Border Protection, "U.S. Customs and Border Protection: Fiscal Year 2010 Accomplishments" (briefing, released March 2011).

- intercepted more than $147 million in currency.[2]

The deployment of DHS technology, physical infrastructure, and manpower to counter smuggling along the border has made it more difficult for drug trafficking and other transnational criminal organizations to conduct their illicit activities. This had led these organizations to infiltrate CBP through conspired hiring operations and compromise of the agency's existing officers and agents. The overwhelming majority of CBP officers and agents demonstrate the highest levels of integrity and perform their duties with honor and distinction every day, but isolated acts of corruption do occur. Since October 1, 2004, 134 CBP agents and officers have been arrested, charged with, and convicted of mission-critical corruption charges, including bribery, alien and/or narcotics smuggling, conspiracy, and fraud.[3] This is a small minority of the workforce, but it represents a threat to our national security—hence CBP's move to ask the Institute to study this corruption problem.

Scope

This study focuses on workforce integrity and, more specifically, law enforcement workforce integrity. For the purposes of this study, integrity is regarded as:

> A series of concepts and beliefs that, combined, provide structure to an agency's operation and officers' professional and personal ethics. These concepts and beliefs include, but are not limited to, honesty, honor, morality, allegiance, principled behavior, and dedication to mission.[4]

Given the relatively short six-month duration of the project and resources made available for the work, the study team conducted a high-level analysis across the agency, rather than in-depth case-study analyses on how CBP is handling its workforce corruption problem. Due to these limitations, anecdotal information corroborated by multiple sources was applied to some findings.

Methodology

The study team characterized workforce ethics, integrity, and corruption through research of relevant open source studies, authoritative documentation, and other materials.[5] Interviews with key CBP officials and their interagency partners involved in workforce integrity and corruption issues provided background and context for the work. Those discussions also offered informed perspectives on coordination, interactions, and constraints in dealing with workforce corruption and integrity matters, as well as issues for further exploration. (A list of standard questions used in the initial CBP interviews

---

[2] Ibid.

[3] CBP Office of Internal Affairs, reported as of November 11, 2011.

[4] Stephen J. Gaffigan and Phyllis P. McDonald, Ed.D., "Police Integrity: Public Service with Honor," National Institute of Justice, U.S. Department of justice, NJC 163811 (January 1997), www.ncjrs.gov/pdffiles/163811.pdf.

[5] Much of this research was completed under the Institute's Workforce Integrity and Ethics Analysis core task.

appears in appendix A. A listing of CBP offices and activities, and federal interagency counterparts consulted over the course of the study appears in appendix B.[6])

Based on the initial findings derived from the opening interviews, the team studied and assessed CBP workforce integrity and counter-corruption programs and initiatives to identify vulnerabilities and possible solutions. The team then augmented its preliminary research and findings with further targeted study and consultations with subject matter experts. The aim was to identify relevant best practices and make recommendations regarding how to optimize CBP's programs, processes and technologies for countering corruption and heightening workforce integrity. This final report is a comprehensive summary of the work performed, findings, and recommendations.

The sponsor tasked the study team to direct the aforementioned efforts in the following five focal areas.

1. CBP Operational and Organizational Structure. The initial intra-agency and interagency consultations provided background necessary to examine the existing internal and external CBP organizational structures for maintaining workforce integrity, and investigating and dealing with allegations of misconduct against CBP employees.

2. Employee Recruitment and Vetting Process. The study team explored the process to identify potential vulnerabilities in existing employee recruitment and vetting procedures, including the process, frequency, and types of data collected during background investigations and re-investigations.

3. Integrity Training Process and Programs. The team reviewed existing training programs to determine the content and extent to which ethical behavior, workforce integrity, and counter-corruption themes are integrated into Border Patrol and Field Operations curricula and courseware at entry and supervisory levels. This sub-task also considered continuing professional education as well as messaging programs to reinforce integrity and counter-corruption themes within the CBP workforce.[7]

4. Metrics and Information Sharing Process. The study team evaluated CBP's existing metrics for identifying and determining the level of corruption and measures of discipline in the workforce.

5. Prevention, Detection, Monitoring, and Investigation Process. This broad sub-task considered over forty programs and initiatives across the agency in

[6] The CBP employee labor unions—the National Border Patrol Council and the National Treasury Employees Union—did not reply to the study team's request for interviews in time for this report.

[7] The study team was unable to visit training facilities and witness classroom instruction due to constraints on time and travel.

determining their effectiveness. A listing of those programs and initiatives appears at appendix C.[8]

In order to meet these requirements and attain the desired outcomes, the Institute assembled a team of seasoned analysts, some of whom have law enforcement and vulnerability assessment experience and have worked with CBP officials on related projects. We collaborated with Hillard Heintze, a highly experienced firm of law enforcement (LE) and organizational security professionals uniquely well-suited to partner with the Institute on the study. The Hillard Heintze Senior Leadership Council (SLC) is an independent council of retired federal, state and major city police chiefs and law enforcement executives dedicated to advancing excellence in policing and public safety. SLC subject matter experts focus on law enforcement and security issues ranging from ethics, integrity and public trust to law enforcement technologies, workforce management systems and best practices. In addition to the data collected, we relied heavily on the judgment of Hillard Heintze and its SLC in particular on whether or not a CBP activity constituted a best practice. Appendix D profiles Hillard Heintze and its contributors to this project.

Report Structure

As noted above, the report progresses through the five sponsor-directed focal areas, first offering a brief statement of the team's findings and recommendations in each area. A discussion of each of those findings—how the team arrived at each recommendation (analyzing current practices, efficiencies, etc.)—follows. That discussion of each finding then concludes with a full explanation of each recommendation—actions, strategies, and/or best practices—that CBP should focus on to optimize the agency's workforce integrity and counter-corruption programs, processes, and technologies.

The conclusion of this report summarizes the key findings and recommendations, and suggests areas for further study that were beyond the scope of this project. Appendices E through H offer further detailed listings and ancillary treatments of topics (e.g., the CBP Disciplinary Flow Chart) not accommodated in the body of the report.

[8] Appendix C is an adaptation of a June 2011 "Current CBP Corruption and Integrity Initiatives" matrix developed by the Office of Human Resource Management Labor and Employee Relations Division.

SECTION I. CBP OPERATIONAL AND ORGANIZATIONAL STRUCTURE

We examined the existing internal and external CBP organizational structures[9] for maintaining workforce integrity, and for investigating and dealing with allegations of misconduct against CBP employees. That led the study team throughout the CBP organization and across the federal interagency to broadly survey existing approaches to workforce integrity and counter-corruption measures, and perspectives on efficiencies (and inefficiencies) in various processes. Further research and analysis, plus consultations with subject matter experts, complemented the initial discussions.

Overview of Findings and Recommendations

- There is no comprehensive guidance for integrity programs and initiatives across the CBP organization. CBP therefore should implement an agency-wide workforce integrity strategy—one that establishes and articulates core concepts, approaches, control mechanisms, roles and responsibilities.
- The CBP's disciplinary system has so many processes that it does not foster timely discipline or exoneration. The agency therefore should rethink its disciplinary system toward more efficiency.
- The number of open cases and the protracted periods until many of them are closed (if ever) attest to the inefficiencies of the present DHS Office of Inspector General (OIG) – CBP organizational structure. The Commissioner should approach DHS leadership to change that structure for more efficient reporting, assignment, investigation and disposition of CBP workforce investigations.
- The FBI-led border corruption task forces (BCTFs) are effective in countering public corruption on the borders, including the corruption of CBP employees. The continued inclusion of CBP Office of Internal Affairs (IA) special agents in the national and regional BCTFs will foster effective criminal investigations and introduce efficiencies in combined counter-corruption efforts.

The following is a discussion, in order, of those findings and recommendations.

CBP Workforce Integrity Strategy

Discussion of Findings

In discussing the workforce integrity/counter-corruption enterprise with personnel across the agency, the study team looked for comprehensive guidance on the subject and found none. We learned of many programs and initiatives to address these matters, but saw that

[9] Internal organizational structures reside within the agency; external structures extend beyond the agency.

these ongoing actions were largely distinct and independent of one another. We asked interviewees, "Where is the nexus of the workforce integrity/counter-corruption enterprise within CBP?" and did not get a ready articulation of the answer.

Even the word "integrity" is unclear among CBP personnel. While "integrity" is often mentioned, including in the CBP core values, we did not find an agency-wide definition of this fundamental principle.[10] Our research confirmed that the proverbial "code of silence"—an unwritten rule not to report another colleague's errors, misconducts or crimes—is common within the law enforcement profession.[11] Multiple agency interviewees indicated anecdotally that it exists within CBP. Our review of many CBP papers, pamphlets, and quick-reference cards that address workforce integrity did not address this "code." The "code" presents an insidious challenge to workforce integrity, and requires explicit, targeted and sustained attention.

CBP's sustained attention to workforce integrity activities is itself a challenge. There are over forty workforce integrity and counter-corruption programs and initiatives across the agency.[12] There is no central coordination of these related and dynamic activities. While much communication and information sharing occurs across the organization, many of these exchanges are informal and personality based, and assurances that the right information is getting to the right parties are lacking.

What coordination of the many programs and initiatives does exist is splintered. Formal workforce integrity and counter-corruption training, for example, is administered by no less than five different entities, yet there is no mechanism to ensure that the training themes are consistent across all training efforts.[13] Lines of responsibility are not always clearly defined, which presents the potential for redundancies and unintended interference. For example, it is not clear when the Office of Field Operations (OFO) Analytical Management Control System Office (AMSCO) analysis of a workplace data anomaly ends and the OIA investigation of potential employee malfeasance begins. An articulation of roles, responsibilities, and lines of communication across the workforce integrity – counter-corruption enterprise is necessary.

Discussion of Recommendation

CBP should implement an agency-wide workforce integrity strategy—one that establishes and articulates core concepts, approaches, control mechanisms, roles and responsibilities. The insidious "code of silence," for one, requires explicit, targeted and

[10] A flashcard distributed within the agency listing fifty qualities with definitions that describe an ideal agent or officer does not list or define "integrity."

[11] Neal Trautman, "Police Code of Silence Facts Revealed," Paper for the Annual Conference of the International Association of Police Chiefs, The National Institute of Ethics, 2000, http://www.aele.org/loscode2000.html.

[12] Appendix C contains lists and briefly describes these programs.

[13] Formal integrity and counter-corruption training is developed and provided to the workforce by the following: the Office of Training and Development, OIA Integrity Programs Division; Field Operations (FO) and Border Patrol academies; OIA special agents; DHS OIG special agents; and CBP supervisors and FO integrity officers at shift musters.

sustained attention—the kind of attention that a strategy like this would give the agency's workforce integrity/counter-corruption efforts. The study team recommends that the CBP commissioner consider chartering a cross-agency working group to develop and maintain this strategy.[14] We believe the Commissioner Bersin's March 2011 "Statement of Policy and Intent: Integrity" provides an excellent prologue to such a strategy and, furthermore, establishes that office as the much-needed nexus of the workforce integrity/counter-corruption enterprise. Figure 1 outlines what that strategy might include.

Workforce Integrity Strategy Outline

- Commissioner's Statement
  - Clearly articulated, agency-wide definition of integrity
  - Declaration of organizational culture of integrity
  - Integrity initiatives, goals, and principles
  - Establishment of lines of criminal behavior, strict accountability, and punishment
    - Articulation of "Bright Line" misconduct
    - "Code of silence" unacceptable
- Central coordination of integrity and counter-corruption programs and initiatives
  - Control mechanisms
- Information sharing and communications protocols
- Recruitment and vetting approaches and programs
- Training and education approaches and programs
- Professional development approaches and programs
- Roles and responsibilities

Figure 1. Workforce Integrity Strategy Outline

The cross-agency working group we suggest for developing the strategy might be internal to the CBP Integrity Integrated Policy Coordination Committee (Integrity IPCC), with a dedicated support element.

CBP Disciplinary System

Discussion of Findings

Discipline implies the systematic conduct of an organization's enterprise by its members adhering to essential rules and regulations. Employee behavior is the basis of discipline in an organization, entailing compliance with the organization's code of conduct. Such discipline promotes productivity and efficiency, and encourages harmony and cooperation among the workforce. Key to the effectiveness of an organization's

[14] Incidental to our research, the study team learned that the *CBP Strategic Plan for 2009-2014* calls for "a comprehensive integrity strategy that integrates prevention, detection, and investigation."

disciplinary system is timely action to correct a condition when a breach of the code of conduct has occurred.[15]

The CBP disciplinary system has many processes—each taking time; some less efficient than others—that, in total, do not foster timely discipline or exoneration. The net result is a compromised management tool with detrimental effects not only on workforce integrity but also on employee morale.[16] The CBP Disciplinary Flow Diagram at appendix E depicts the many processes which a disciplinary case may go through. Misconduct incidents that are considered non-reportable under CBP OIA guidelines can be managed efficiently at the local, supervisory level. The nature of these non-reportable offenses warrants non-adverse disciplinary actions.[17] Those instances of misconduct deemed reportable may be subject to a number of processes at the CBP Headquarters level and above.

The reporting of a misconduct incident to the CBP OIA - Immigration and Customs Enforcement Office of Professional Responsibility (ICE OPR) Joint Intake Center (JIC) initiates a number of reviews adding up to a lengthy process. Current guidance requires that all incidents reported to the JIC be referred to the DHS OIG within five days of receipt. Those referrals are forwarded through the ICE OPR Case Management Group (CMG), which screens cases for data integrity and proper classification. Upon receipt of the case file, the DHS OIG will, in turn, notify the JIC within five working days if it will retain the case for investigation or refer it to ICE OPR for disposition.[18] Cases referred to ICE OPR (again through the CMG) are either retained for investigation of criminal allegations or referred to CBP OIA for lesser offenses.[19]

DHS OIG has demonstrated a practice of retaining a broad spectrum of cases of both criminal and non-criminal allegations. Currently, the DHS OIG maintains an inventory of well over 1,000 cases[20] involving CBP employees, some dating back to 2004.[21] This backlog presents the most significant impediment to timely disposition of CBP disciplinary cases. ICE OPR is currently investigating about 140 cases involving criminal allegations against CBP employees in cooperation with CBP IA special agent detailees, and strives to close cases within established CBP OIA goals.[22] CBP OIA's goal for

---

[15] "Employee Discipline and Features of a Sound Disciplinary System," Management Study Guide, http://www.managementstudyguide.com/employee-discipline.htm, accessed on November 25, 2011.

[16] The 2011 CBP Employee Viewpoint Survey rated among the most negative responses: "Steps are taken to deal with poor performers – 28%."

[17] Non-adverse disciplinary actions include letters of reprimand up to a 14-day suspension.

[18] See DHS Management Directive 0810.1, "The Office of the Inspector General," Appendix A, June 2011.

[19] See DHS Delegation Number 7030.2, "Delegation of Authority to the Assistant Secretary for U.S. Immigration and Customs Enforcement," Article 2(E), November 13, 2004.

[20] Case inventory refers to currently open, active investigations.

[21] Interview with ICE OPR – CBP OIA Joint Intake Center staff, October 6, 2011.

[22] Ibid.

investigation of allegations against CBP employees is 90 to 120 days; it currently has 860 active cases of a broad range of malfeasance allegations.[23]

All instances of misconduct reported to the JIC and the results of investigations of CBP employees are referred to the CBP Office of Human Resources Management Labor and Employee Relations Division (HRM LER) for disposition. LER remands cases that do not warrant proposed adverse action to the respective principal field officer/principal headquarters officer (PFO/PHO) for appropriate lesser action. LER prepares any case warranting adverse action for presentation to a Discipline Review Board (DRB).[24] (Figure 2 provides the time frame from the incident date to receipt in LER for review.) DRBs are three-person boards of GS-14, GS-15, and Senior Executive Service (SES) managers and supervisors who serve as a collateral duty under appointment by their PFO/PHO. Boards meet about every four weeks with an average of fifteen cases reviewed per session.[25] (Figure 3 profiles the timeliness of the DRB process.)

TIMELINESS PRIOR TO THE DISCIPLINE REVIEW BOARD SESSION

Of all cases presented to the DRB, the time frame from incident date to receipt in LER for review is as follows:

- **42% cases received within six months of the incident (52% in FY-09)**
- **28% cases received between six months and one year of the incident (29% in FY-09)**
- **17% cases received between one and two years of the incident (14% in FY-09**
- **13% cases received after two years of the incident (5% in FY-09)**

Figure 2. Timeliness Prior to Discipline Review Board Session[26]

[23] Ibid.

[24] Adverse action is defined as a removal, reduction in grade or pay, or a suspension of more than 14 days. For a detailed discussion of the DRB process see "U.S. Customs and Border Protection Discipline Review Board," Directive No. 51751-002A, June 21, 2004.

[25] Office of Human Resources Management Employee Relations Division, *U.S. Customs and Border Protection Discipline Report for Fiscal Year 2010*, slide 35. Due to study time and resource constraints, we could not independently verify the CBP statistics. A more detailed analysis should rely on primary data sources.

[26] Ibid, slide 31.

TIMELINESS OF THE DISCIPLINE REVIEW BOARD PROCESS			
Average Number of days for:	Fiscal Year 2009	Fiscal Year 2010	Change 2009 to 2010
DRB to Counsel	16.8 days	14.9 days	-1.9 days
Counsel Review	13.7 days	16.4 days	2.7 days
DRS to Issuance of Proposal	51.6 days	46.9 days	-4.7 days
DRB to Final Decision	152.1 days	151.6 days	-0.5 days
While there are significant decreases in the amount of time to process a case through the issuance of the proposal letter, there is only a small decrease in the length of time to process a case based on delays caused by union information requests, scheduling oral replies, Douglas Factor discussions, and changes of Deciding Officials.			

Figure 3. Timeliness of the Discipline Review Board Process[27]

Figures 2 and 3 illustrate the protracted amount of time it takes from the date of an incident to the actual meting out of punishment—from months to years. These lengthy periods pose challenges to CBP management in maintaining the security mission, good order, and discipline—that is, this problem challenges workforce integrity, which stands to incite or facilitate corruption. The following explains:

- CBP employees suspected of corruption may remain in critical security positions until allegations are proven or disproven, or criminal investigations gain sufficient evidence or grounds for prosecution.
- CBP employees found innocent of allegations may have had their professional reputations tainted and advancement impeded by lengthy leave and administrative duties, suspension, and/or reassignment.
- Fellow CBP employees aware of a colleague under suspicion and observant of an apparent lack of action on the part of management and law enforcement may consider the enforcement system "broken" and disregard professional responsibilities to report malfeasance.
- Lengthy times may violate norms of speedy disposition of cases and lead to the subject "walking" without receiving final discipline appropriate for the misconduct.

[27] Ibid, slide 32.

Furthermore, the LER-DRB process itself is flawed. Initially established by the U.S. Customs Service in 1999 to service a population of 22,000 employees, the process now deals with a 59,000-member workforce, many of whom operate in a highly volatile border environment. LER staff is overburdened with caseloads. The 151 days in FY10 from "Discipline review Board to Final Decision" shown in Figure 3 reflect the inordinate amount of time it takes to get to the final decision—due to labor union requests, oral replies, Douglas Factor documentation,[28] deciding official penalty changes, and other administrative processes.

Discussion of Recommendation

The agency should rethink its disciplinary processes toward more efficiency. Process improvements should include realistic timelines to ensure that cases are tracked and receive due, timely attention. Reforms should give greater delegation of disciplinary authorities to PFOs/PHOs—to allow more administration of discipline at the local level and lessen headquarters requirements. A review of FY10 DRB sessions and proposals or related actions (see figure 4) suggests that penalties up to and including long suspensions could be administered at the PFO/PHO level to allow more timely discipline in those cases, and to ease the caseload of the LER staff. Cases in which the employee admits to having committed the offense and accepts the penalty offered by the PFO/PHO should be handled at the PFO/PHO level and not require a DRB review.

DISCIPLINE REVIEW BOARD SESSIONS AND PROPOSALS/ACTIONS

- **21 Boards convened (includes 5 special boards)**
- **273 Cases presented to Discipline Review Board**
  - **167 Removals**
  - **7 Demotions/demotions with suspensions**
  - **37 Long suspensions**
  - **34 Short suspensions**
  - **8 Letters of reprimand**
  - **9 Letters of counseling/letters of caution**
  - **11 No action**

Figure 4. Discipline Review Board Sessions and Proposals/Actions for FY10[29]

These delegations would give the senior officials more authority to manage their workforces, and offer significant efficiencies to the process. The local LER and Office of

[28] "Douglas Factors" are criteria established by the Merit Systems Protection Board that supervisors or, in some instances, deciding officials must consider in determining an appropriate penalty to impose for an act of employee misconduct.

[29] Office of Human Resources Management Employee Relations Division, *U.S. Customs and Border Protection Discipline Report for Fiscal Year 2010*, slide 30.

Chief Counsel representatives would continue to advise the deciding official and review case penalties for consistency and propriety.

CBP should undertake a study to consider these and other revisions to the current CBP disciplinary system.

DHS OIG – CBP Organizational Structure

Discussion of Findings

In the initial organization of the Department of Homeland Security in 2003, the "Bureau of Customs and Border Protection" (CBP) brought together approximately 30,000 employees including 17,000 inspectors in the Agricultural Quarantine Inspection program, Immigration and Naturalization Service (INS) inspection services, Border Patrol, and Customs Service. This new bureau focused its operations on the movement of goods and people across U.S. borders, and the enforcement of applicable laws and regulations.[30] A "Bureau of Immigration and Customs Enforcement" (ICE) organized the enforcement and investigative arms of the Customs Service, and the investigative and enforcement functions of the Immigration and Naturalization Service and the Federal Protective Services (FPS). The reorganization involved approximately 14,000 employees to focus on the mission of enforcing the full range of immigration and customs laws within the interior of the United States in addition to protecting specified buildings. By unifying previously fragmented investigative functions, ICE would enhance information sharing with the FBI and develop stronger relationships with the U.S. Attorney's Office.[31]

This early reorganization of DHS border-related functions left CBP—the nation's largest law enforcement agency—without an internal investigative capability.[32] DHS organizers thought, at that time, that CBP's internal investigative needs would be met by other resources. DHS Management Directive 0810.1, dated June 2004, gave the department's Office of Inspector General the authority to accept and retain a broad range of allegations of criminal and non-criminal misconduct of CBP employees for investigation.[33] The DHS Secretary's Delegation Number 7030.2 gave the Assistant Secretary of ICE the authority to investigate allegations of misconduct against officers, agents, and employees of CBP.[34] In practice, ICE OPR investigates allegations of CBP employee misconduct referred by DHS OIG.

The reliance upon external organizations for CBP's internal corruption investigations contravenes the conventional federal law enforcement model for internal affairs. That

---

[30] U.S. Department of Homeland Security, "Border Reorganization Fact Sheet," January 30, 2003, http:/www.xnews/releases/press_release_0073.shtm.

[31] Ibid. ICE has ceded the practice of sharing DHS employee-related information with FBI to DHS OIG.

[32] CBP retained a small staff of about eight persons to conduct internal inspections.

[33] DHS, "Office of Inspector General," MD 0810.1, June 2004.

[34] Department of Homeland Security, "Delegation Number 7030.2: Delegation of Authority to the Assistant Secretary for U.S. Immigration and Customs Enforcement," Article 2(E), November 13, 2004.

model calls for the placement of the internal investigative function within the agency which bears the strongest institutional interest in deterring and detecting corrupt behavior. The Secret Service, Transportation Security Administration, Coast Guard and ICE maintain internal criminal investigative capabilities within their respective organizations. CBP, which operates in a high threat and corruption prone border environment, requires these same capabilities.

In 2003, one of the reasons put forward by then-CBP Commissioner Robert C. Bonner for not splitting off INS and Customs special agents into a separate investigative agency was that such a move would seriously undermine CBP and the commissioner's ability to ensure workforce integrity.[35] This matter was even more vital given the national security implications of a corrupt CBP frontline officer in collusion with terrorists or other criminal elements. The foremost concern was that failure to implement a fully functional internal investigative capability within CBP would likely make it impossible for the commissioner to contain, control, deter, and eradicate corrupt frontline border officers.

The fact that 134 current or former CBP employees have been arrested or indicted on corruption-related charges since October 1, 2004 validates Commissioner Bonner's concerns.

To countermand these threats to U.S. national security and the CBP workforce, CBP's Office of Internal Affairs has, since 2006, hired over 200 special agents to constitute an intra-agency investigative capability. These agents on average possess more than 20 years of experience as investigators in a variety of federal law enforcement agencies. Investigative personnel are stationed at 22 field offices located across the nation.[36] CBP IA special agents work collaboratively with the FBI as part of the National Border Corruption Task Force (NBCTF), participating in 21 FBI-led border corruption task forces and/or public corruption task forces nationwide.[37]

Over the years, CBP commissioners have requested the Department of Homeland Security's permission to delegate to this highly qualified force full investigative authorities, while at the same time complying with prerogatives provided to DHS OIG under the Inspector General Act of 1978, the Homeland Security Act of 2002, and DHS Management Directive 0810.1. In July 2008, then-Commissioner W. Ralph Basham requested permission to convert IA's GS-1801 general investigators to GS-1811 criminal investigators to give CBP those full investigative authorities. Then-Secretary of Homeland Security Michael Chertoff denied that request, reasoning that border-related criminal investigative functions had been vested in ICE, and expressing concerns about potential overlap in ICE and CBP missions.[38] The Secretary noted that "it is axiomatic

[35] U.S. Customs and Border Protection Office of Internal Affairs Study, November 2004.

[36] The CBP Statement of Objectives for this task contains these facts and figures.

[37] This cooperative arrangement is under review as a condition of the "Memorandum of Understanding between U.S. Department of Homeland Security Inspector General and U.S. Customs and Border Protection on Border Corruption Initiative," August 12, 2011.

[38] Department of Homeland Security Office of Inspector General, "CBP Corruption Investigations to the House Appropriations Committee staff" (briefing, 2011).

that border-related corruption will be tied to potential violations of core ICE smuggling and trafficking statues."[39] In the course of the research for this report, the Institute study team did not find any evidence substantiating that assumption. Such a predicament illustrates that, insofar as CBP IA investigative resources lack any authorities they need, the full potential of those resources remains unrealized.

The DHS OIG, meanwhile, remains the more fully vested authority in investigations concerning CBP workforce—and the case load represents a significant backlog. The intent of DHS Management Directive 0810.1 is for the OIG to serve as the primary entity within DHS for investigating all criminal allegations of waste, fraud, abuse and mismanagement, allegations of misconduct against all political appointees and personnel at the level of GS-15 and above, and any allegations that indicate systemic problems within the department or otherwise affect public health or safety.[40] As noted above, the Inspector General Act, Homeland Security Act, and Delegation Number 7030.2 further vest investigative authority in the DHS OIG, with the ICE OPR having authority to investigate those allegations involving CBP and ICE employees referred to it by OIG.[41]

In practice, DHS OIG accepts cases involving both criminal and non-criminal allegations against all grades of CBP employees. The study team could not correlate the OIG acceptance of these cases to any particular pattern or rationale. Of the remaining cases referred by OIG to ICE OPR, OPR retains the cases of criminal allegations and refers the non-criminal cases to CBP OIA for investigation. Table 1 illustrates DHS investigative resources, workforce populations serviced by those resources, and current CBP case inventories.

[39] Ibid.
[40] Ibid.
[41] Ibid.

Table 1. DHS Investigative Resources and Case Inventories[42]

DHS Office	Workforce Population	Agents Assigned	Workforce – Agent Ratio	CBP Case Inventories	Notes
DHS OIG	225,000	213	1,056:1	1,330	Workforce population not inclusive of 200,000 DHS contractors
ICE OPR	79,000	230/256	343:1/309:1	140	Workforce population includes 59,000 CBP employees; assigned agents and ratios reflect without and with 28 CBP detailees
CBP OIA	59,000	210	281:1	860	Criminal and non-criminal cases

As Table 1 illustrates, the inventory of CBP cases that DHS OIG currently holds is exorbitant.[43] These backlogs represent months to years taken to close investigations,[44] presenting significant workforce management challenges for the CBP commissioner.

Some measures have been taken to alleviate CBP case backlogs. In December 2010, the ICE director and CBP commissioner signed a memorandum of understanding (MOU) that allowed for CBP IA agents to augment ICE OPR agents in the investigation of criminal allegations against CBP employees. Under the terms of that agreement, "CBP IA agents are authorized to exercise the full range of their authority as federal law enforcement officers under the direct supervision of the presiding OPR manager...."[45] Since the signing of that MOU, CBP disciplinary functionaries have noted more timely submissions of investigation reporting from ICE OPR.

[42] As a point of reference, prior to the DHS reorganization, the Customs Office of Internal Affairs was staffed with approximately 162 criminal investigators who investigated allegations of corruption within a legacy workforce of 22,000 employees. This represented an approximate ratio of 1 investigator for every 136 employees.

[43] These statistics are derived from cases processed through the ICE OPR – CBP OIA Joint Intake Center (JIC). -These statistics do not include allegations against CBP employees reported directly to DHS OIG for which neither the JIC nor CBP have any visibility or awareness.

[44] See the discussion of disciplinary process investigations on p. 16.

[45] ICE Director John Morton and CBP Commissioner Alan Bersin, "Memorandum of Understanding Between U.S. Immigration and Customs Enforcement and U.S. Customs and Border Protection," December 2010.

Then, on August 12, 2011, the CBP commissioner and DHS Inspector General signed a memorandum of understanding under which CBP IA detailees to OIG field locations will similarly "assist and meaningfully participate in the investigation of each border-related criminal misconduct case in which a CBP employee or contractor is subject to a criminal investigation.... Such participation will be under the supervision and direction of OIG INV (Office of Investigations)...."[46] CBP OIA and DHS OIG are presently engaged in a small pilot program based on this MOU, prior to full implementation of the terms of the MOU. Nonetheless, case backlogs persist.

Both of these MOU arrangements represent patchwork attempts to address the unintended consequences of a DHS OIG – CBP organizational structure developed in 2003 that now, eight years later, has proven to be largely ineffective. The scrutiny applied in the ICE OPR and DHS OIG acceptance of CBP IA detailees bears testimony to their professional qualifications. However, in their "under direct supervision" and "assist and meaningfully participate" roles, IA detailees are constrained in applying their full capabilities and potential. The detailing of CBP IA investigators to other organizations in order to conduct criminal investigations on CBP employees defies the common logic of the federal investigative arena—where, as noted earlier, organizations like the Transportation Security Administration maintain internal criminal investigative capabilities within their respective organizations.

To effectively manage the CBP workforce, including monitoring and addressing integrity and counter-corruption concerns, the CBP commissioner and his management team require full situational awareness, which comes from the reporting of disciplinary incidents and criminal investigations through the JIC. However, as noted above, allegations of CBP employee misconduct may in fact be reported directly to DHS OIG. In such instances, the DHS OIG has not shared that information with the CBP commissioner—who therefore remains unaware of the existence of such cases and their disposition.

Discussion of Recommendation

The Commissioner should approach DHS leadership to change the existing DHS OIG – CBP organizational structure for the reporting, assignment, investigation and disposition of CBP workforce investigations. The number of open cases, for one, and the protracted periods until many of them are closed (if ever) attest to the inefficiencies of the present DHS OIG – CBP organizational structure. Further, the restrictions placed on a highly qualified cadre of CBP IA special investigators who have proven their professional qualifications and skills, cause suboptimal utilization of this valuable counter-corruption asset. Finally, the CBP commissioner, who is ultimately responsible for the workforce and its integrity, should be fully cognizant of the ongoing cases against his employees; to address the workforce corruption problem, he must know

[46] DHS Inspector General Charles K. Edwards and CBP Commissioner Alan D. Bersin, "Memorandum of Understanding Between U.S. Department of Homeland Security Inspector General and U.S. Customs and Border Protection on Border Corruption Initiative," August 12, 2011.

the extent of the problem. The DHS OIG practice of withholding from the CBP commissioner information on CBP corruption cases is not in the best interests of the agency or the department. The DHS OIG – CBP MOU allows CBP IA detailees to report cases involving CBP employees to the commissioner. Its provisions also state, "OIG is committed to providing CBP with full awareness of border-related criminal misconduct cases for which OIG is the lead investigative agency."[47] DHS OIG has yet to demonstrate that commitment.

The CBP commissioner should consider further developing these issues and additional reasoning. The commissioner could then bring forward to DHS leadership the rationale for implementing a fully functional CBP internal affairs office—to include the capability to conduct independent criminal investigations of CBP employees. The provisions of the Inspector General Act, Homeland Security Act, and Management Directive 0810.1 accommodate this proposal.

While previous commissioners at the agency have presented much of the same reasoning in making their cases for such changes to the organizational structure, circumstances have changed. Failing to provide the commissioner the necessary capabilities and situational awareness to eliminate corruption in a workforce that operates in a high-threat environment, the existing DHS OIG – CBP organizational structure has clearly demonstrated, over eight years, that it is ill-suited for present circumstances.

Border Corruption Task Force

Discussion of Findings

The FBI organized border corruption task forces (BCTFs) counter public corruption on the border—including the corruption of CBP employees. That fact alone warrants discussion of CBP IA special agents' participation in the BCTFs to address the agency's corruption problem.

Cooperation among law enforcement agencies at all levels represents an important component of a comprehensive response to terrorism, organized crime and public corruption. The FBI-led task force concept has proven effective in a number of applications, combining federal, state and local resources to leverage one another's unique capabilities and adds synergies to criminal investigations. By combining the assets of multiple law enforcement agencies in a common pursuit, task forces serve as force multipliers.

The task force concept increases the effectiveness and productivity of limited personnel and logistical resources, avoids duplication of investigations and consequent wasteful expenditure of resources in matters of concurrent jurisdiction, and expands the cooperation and communication among federal, state and local law enforcement agencies. Federal elements of the task force allow the application of sophisticated investigative techniques normally associated with complex organized crime and racketeering

[47] Ibid.

investigations. Such techniques are frequently unavailable to other federal, state and local members of the task force.[48]

Conversely, criminal investigations conducted independently of the task force and without full transparency between those agencies and the task force introduce a duplication of effort and lost efficiencies. Parallel, uncoordinated efforts risk exposing informants, compromising investigations and, in worst case situations, causing "blue-on-blue" encounters.[49]

The Attorney General Guidelines read as follows about the FBI's responsibilities regarding investigations—indicating the bureau's prioritization of tackling corruption:

> The Department of Justice has primary responsibility for enforcement of violations of federal laws by prosecution in the United States district courts. The Federal Bureau of Investigation is charged with investigating violations of federal laws. Offices of the Inspector General have primary responsibility for the prevention and detection of waste and abuse, and concurrent responsibility for the prevention and detection of fraud and other criminal activity within their agencies and their agencies programs.
>
> As the primary investigative arm of the Department of Justice, the Federal Bureau of Investigation has jurisdiction in all matters involving fraud against the Federal Government, and shares jurisdiction with Offices of Inspector General in the investigation of fraud against the Office of Inspector General's agency.[50]

Charged with the primary responsibility for investigating fraud, the FBI places particular emphasis on public corruption as their top criminal investigative priority. Corrupt public officials undermine national security, jeopardize safety, erode public trust and confidence in the federal government, and waste billion of dollars.[51]

BCTFs combine CBP IA special agents, the resources of the FBI, Drug Enforcement Administration (DEA), Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), Transportation Security Administration (TSA) Office of Inspections, and state and local

---

[48] *Hearing on Combating Gang Violence in America: Examining Effective Federal, State and Local Law Enforcement Strategies before the Senate Judiciary Committee* [108th Congress] (2003) (statement of Grant D. Ashley, Assistant Director Criminal Investigative Division, Federal Bureau of Investigation), http://www.fbi.gov/news/testimony/the-safe-streets-violent-crimes-initiative.

[49] "Blue-on-blue" is a common term in law enforcement that describes the potential for a tragic act of violence that can potentially occur between law enforcement officers when they are not aware of each other's presence during an investigation.

[50] John Ashcroft, "Attorney General Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority," Office of the Attorney General, U.S. Department of Justice, Washington, D.C., December 8, 2003.

[51] Federal Bureau of Investigation, "Public Corruption: Why It's Our #1 Criminal Priority," http://www.fbi.gov/news/stories/2010/march/corruption_032610, accessed on November 23, 2011.

agencies to investigate public corruption along the borders. Twenty-one BCTFs exist today, thirteen of which are on the Southwest Border alone. Of the 700 FBI agents assigned to public corruption nationwide, approximately 120 of them are located in the Southwest region. Through this regional cooperation, more than 400 public corruption cases were originated, and in FY09 more than 100 arrests and about 130 state and federal cases were prosecuted.[52]

Assertions of the Secretary's "One Face at the Border" axiom applying to independent DHS investigations of criminal misconduct against DHS employees is totally out of context.[53] On September 2, 2003, then-DHS Secretary Tom Ridge announced the "One Face at the Border" initiative, directed toward travelers and commerce crossing U.S. borders. The intent was to eliminate the previous separation of immigration, customs, and agriculture functions at U.S. land, sea, and air ports of entry, and institute a unified border inspection process.[54] In fact, criminal investigations are conducted out of the public eye. When conducted efficiently, they require cooperation and coordination among numerous law enforcement organizations, including BCTF members, DHS, and its components. "One Face at the Border" is not a rationale for DHS and its components to conduct investigations into public corruption against its employees independent of the Federal Bureau of Investigation and other agencies with cross-jurisdiction.

Discussion of Recommendation

The continued inclusion of CBP IA special agents in the national and regional BCTFs will foster effective criminal investigations and introduce efficiencies in combined counter-corruption efforts. The BCTFs have been effective in countering public corruption on the borders, including the corruption of CBP employees. The DHS OIG – CBP MOU on Border Corruption Initiative recognizes CBP OIA's agreements with the FBI's NBCTF and local BCTFs. Under the terms of the agreement (and in the absence of a separate MOU between DHS and the Department of Justice), CBP and OIG will provide the Secretary of Homeland Security with recommendations regarding CBP's continued participation in those task forces. Based on those recommendations, "the Secretary of DHS or her designee will make a decision ... based on the Department's desire to ensure that all allegations of employee corruption are fully and promptly investigated."[55] The commissioner should recommend to the DHS leadership CBP's full participation in the national and regional BCTFs.

---

[52] Federal Bureau of Investigation, "On the Southwest Border – Public Corruption: A Few Bad Apples," http://www.fbi.gov/news/stories/2010/august/southwest-border2, accessed on November 22, 2011.

[53] See Department of Homeland Security Office of Inspector General, "CBP Corruption Investigations to the House Appropriations Committee staff" (briefing, 2011), and DHS OIG – CBP MOU.

[54] Deborah Waller Meyers, "One Face at the Border: Behind the Slogan," Migration Policy Institute, Washington, D.C., June 2005, www.migrationpolicy.org/pubs/Meyers_Report.pdf.

[55] DHS OIG – CBP MOU.

SECTION II. EMPLOYEE RECRUITMENT AND VETTING PROCESS

We looked at the entire recruitment and vetting process to determine how integrity is incorporated into assessments of job candidates. We were interested in determining what, if any, vulnerabilities might exist that would allow corrupt individuals—or those with the potential for corruption—to enter the workforce. We also wanted to identify any limitations in the process, due to either internal or external factors. Finally, with the help of the Hillard Heintze Senior Leadership Council, we sought to determine if there were any best practices for vetting law enforcement personnel that could be useful to CBP in bolstering the candidate selection process.

Overview of Findings and Recommendations

- CBP should follow through with its intent to conduct entry level polygraph examinations prior to the more expensive and time-consuming background investigation. The sequential recruitment and vetting process as a whole appears to be practical, with the relatively less expensive assessment tools that result in the higher fallout rates being on the front end of the process.
- Some CBP officials we spoke with expressed concerns that Office of Personnel Management (OPM) suitability determination guidelines are rather permissive when considering placement of applicants in the agency's national security positions. CBP should open discussions with OPM to address those shortfalls.
- Surge hiring and corruption cases in recent years have led some to associate the two occurrences without certain evidence. CBP should consider conducting a conclusive analysis of the tenure of employees arrested or convicted for corruption—specifically, to consider the most likely career points for this malfeasance and the effects of surge hiring.
- Psychological examinations are not a standard part of the candidate vetting process. CBP should consider implementing pre-employment psychological (and additional) testing.
- There is strong data to support the use of polygraph examinations in vetting CBP law enforcement job candidates. CBP OIA Credibility Assessment Division should continue steadily accumulating a cadre of 85 polygraphers to meet the Anti-Border Corruption Act mandate of testing prior to January 1, 22013 all CBP officer and agent recruits before employment.

The following is a discussion, in order, of those findings and recommendations.

Recruitment and Vetting Process

Discussion of Findings

We found that the sequential process[56] for recruiting and vetting CBP officers and Border Patrol agents is extensive and involves multiple measures that seek to ensure the integrity of job candidates. From the initial application through the written test; the medical, fitness, and drug tests; the scenario-based interview; the polygraph examination; and the background investigation—attempts to assess integrity and ethical behavior are woven throughout the process, both directly and indirectly.

Based on our research and discussions with relevant personnel, we developed a schematic overview (figure 6) of the recruitment and vetting process. (A more detailed version is provided in appendix F.)

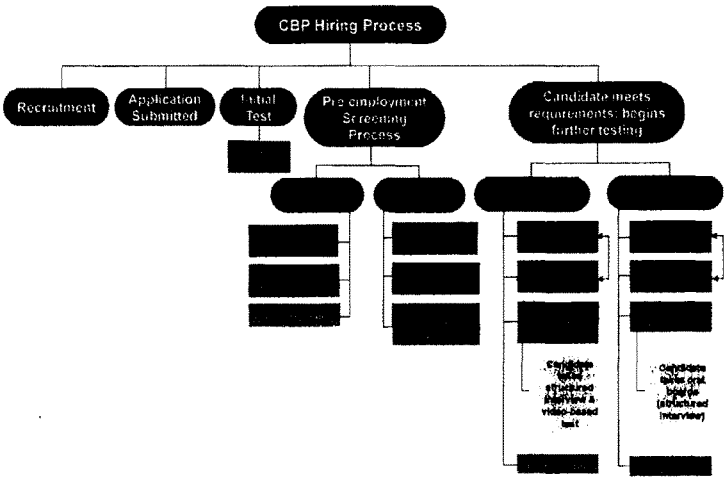


Figure 5. Recruitment and Vetting Process Overview

The recruitment and vetting process takes an average of six to nine months from start to finish, each step of the process having measures designed to identify individuals who may not be fit for duty. On average, it takes 52 applicants for the Border Patrol Agent position to get one candidate through the entire recruitment and vetting process and determined suitable for entry on duty (EOD). It takes 28 applicants for the CBP Officer

[56] The sequential process involves various steps of the process occurring one at a time. A concurrent process involves various steps occurring simultaneously. The trade-offs are time (sequential being longer) versus cost (concurrent being costlier).

position to get one candidate suitable for EOD.[57] Candidates fall out at various parts of the vetting process, as demonstrated by the recruitment attrition rates provided in table 2.

Table 2. CBP Recruitment Attrition Rates[58]

Stage of Recruitment/Vetting Process	Attrition Rates		Cost per Recruit
	Field Operations Officers	Border Patrol Agents	
Written Test	50%	50%	$80
Video-Based Test and Structured Interview	20%	---	Unknown
Oral Hiring Board	---	15%	Unknown
Medical Test	25%	25%	$460
Fitness Test	20%	15%	$270
Drug Test	<1%	<1%	$77
Polygraph Examination*	75%	74%	$800
Background Investigation**	45%	56%	$3200-3600

* Includes no-show rate (i.e., non-pass rate).
** Includes drop-out rate (i.e., non-pass rate) of background investigations completed in FYs 08-10.

Some of the assessment tools used in the vetting process that are explicitly designed to address the candidate's integrity and ethical behavior include the following:

- At the onset of the application process, "Eight Questions" about personal judgment and conscientiousness are used to make an initial decision as to whether the candidate is eligible to proceed to the written test.[59]
- Once candidates pass the written test (which examines the applicant's reasoning skills, writing skills, and experience record), they participate in scenario-based exercises or interviews designed to addresses integrity and ethical decision making.
- Candidates for Border Patrol agent positions are interviewed by the Oral Hiring Board, which is a panel of three trained agents who discuss scenarios that candidates are likely to encounter on the job. The board then assesses each candidate's response to how he or she might handle the situation.

[57] Interview with CBP Minneapolis Hiring Center staff, November 4, 2011.
[58] Minneapolis Hiring Center. "Unknown" denotes that the study team did not receive the information during the course of the discussions, and does not necessarily mean the information does not exist.
[59] The sensitive nature of the content of the initial "Eight Questions" and scenario-based interviews prevented the study team from evaluating (or even having access to) these tools.

- Candidates for CBP positions are required to take a video-based test (VBT), where they are asked to respond to job-related scenarios. Candidates who pass the VBT go on to participate in a face-to-face structured interview with a panel of two trained CBP officers. Both assessments measure competencies that are critical to job success, including integrity. Candidates receive a pass/fail grade for their performance. Those who pass go on to the next step of the vetting process.

- The polygraph examination involves the administration of the Law Enforcement Pre-Employment Test (LEPET). The exam includes questions designed to determine the suitability of the candidate, including whether they are fit to hold a national security position. The exam covers topics such as involvement in serious crimes, illegal drugs, terrorism, and espionage, as well as unauthorized disclosure of classified information or unreported/unauthorized foreign contacts.[60]

- Subsequent to their submission of an SF-86 Questionnaire for National Security Positions, all candidates undergo a background investigation. That investigation covers such areas as finances, drug/alcohol abuse, arrest history, misconduct in prior employment, associations with persons involved in illegal activities (e.g., drug use, trafficking), and demonstrated lack of integrity or honesty in providing complete and comprehensive information about current or past behaviors which may be unfavorable.[61]

CBP is currently building up to a corps of 85 polygraphers to meet the Congressional Anti-Border Corruption Act mandate to conduct pre-employment testing of all candidates by January 1, 2013. While building up to that capacity, some candidates receive polygraphs subsequent to the initiation of the background investigation. It is CBP's intent, once the agency reaches sufficient polygraph capacity, to conduct the less expensive polygraphs before initiating the more costly and time-consuming background investigations.

Discussion of Recommendation

CBP should follow through with its intent to conduct polygraph examinations prior to the more expensive and time-consuming background investigation. The sequential recruitment and vetting process as a whole appears to be practical, with the relatively less expensive assessment tools that result in the higher fallout rates being on the front end of the process.

---

[60] CBP OIA Integrity Programs Division and Credibility Assessment Division, *Final Report: A+ Case File Study: An Exploration of the Statements Made Against Personal Interest in Law Enforcement Applicant Screening Polygraph Examinations*, (March 31, 2009), page 2.

[61] Customs and Border Protection, "CBP Officer Frequently Asked Questions," http://www.cbp.gov/linkhandler/cgov/careers/customs_careers/officer/cass_faq.ctt/cass_q_a.pdf , accessed on September 5, 2011.

Suitability Determinations

Discussion of Findings

CBP adjudicators apply prescribed OPM guidelines to determine the suitability of applicants for employment. Some CBP officials we spoke with expressed concerns that these guidelines are rather permissive. For example, background investigations and follow-up inquiries by CBP Office of Internal Affairs agents discovered some applicants with associations with known felons or suspicious persons. Nevertheless, the OPM guidelines listed below do not regard associations as unsuitable behavior. Per OPM guidelines (5 CFR 731.202), the only factors that can be considered as a basis for finding a person unsuitable are as follows:

- Misconduct or negligence in employment
- Criminal or dishonest conduct
- Material, intentional false statement, or deception or fraud in examination or appointment
- Refusal to furnish testimony as required by Section 5.4 of CFR 731.202
- Alcohol abuse, without evidence of substantial rehabilitation, of a nature and duration that suggests that the applicant or appointee would be prevented from performing the duties of the position in question, or would constitute a direct threat to the property or safety of the applicant or appointee or others
- Illegal use of narcotics, drugs, or other controlled substances without evidence of substantial rehabilitation
- Knowing and willful engagement in acts or activities designed to overthrow the U.S. Government by force
- Any statutory or regulatory bar which prevents the lawful employment of the person involved in the position in question[62]

Additional suitability considerations, if pertinent to the case, include the nature of the position for which the person is applying or in which the person is employed; the nature and seriousness of the conduct; the circumstances surrounding the conduct; the recency of the conduct; the age of the person involved at the time of the conduct; contributing societal conditions; and the absence or presence of rehabilitation or efforts toward rehabilitation.[63]

Another expressed concern is that there are no distinctions made in terms of suitability criteria for different types of job positions. The current qualification criteria are similar

[62] Code of Federal Regulations, "Criteria for Making Suitability Determinations," 5 CFR 731.202, http://frwebgate.access.gpo.gov/cgi-bin/get-cfr.cgi.
[63] Ibid.

across all positions, so that an individual applying for an administrative assistant position would be subject to the same level of investigation as someone applying for a law enforcement or national security position.

Suitability reciprocity is another issue that impacts the vetting process. DHS headquarters' policy accepts suitability determinations from all components, thus minimizing the administrative burdens and costs of separate background investigations and adjudications. However, DHS components perform different types of suitability checks dependent on their varying missions. Consequently, the components do not always recognize one another's suitability determinations. An example provided on multiple occasions was the lack of reciprocity between TSA and CBP, with CBP not honoring suitability determinations made by TSA. This lack of reciprocity forestalls an individual's full employment until a determination can be made by the new component.

The shortfalls continue, as other persons we spoke with who are involved in vetting job candidates suggested that even current DHS policies regarding suitability introduce potential vulnerabilities. They cited, for example, the department's current policy to recognize background investigations previously conducted under another agency for employment within CBP, which presents a loophole for possibly "corrupted" candidates. The following example was offered:

> An individual is hired by DHS Agency X for a management analyst position. A background investigation (BI) is completed with a favorable determination on 1/1/10. The individual is arrested on 6/1/10 on a felony charge of driving under the influence causing bodily injury. Two months later, on 8/1/10, the individual is aware that Agency X may be about to terminate his employment during his probationary period so he applies and is selected for a lateral transfer to CBP. CBP is prohibited by DHS policy from requesting a new BI package. CBP requests the prior investigative file from Agency X. That file does not contain the record of the 6/1/10 arrest since the file was completed prior to the arrest. CBP may run new background checks, but if the felony case has not yet been brought to trial or resolution, it may not have been entered by the arresting police department into the national database. Based on the information contained in the 1/1/10 BI, the CBP adjudicator clears the individual for an appointment. The individual is later convicted of the offense, and CBP now has a convicted felon on its rolls.[64]

Given that example, some interviewees expressed concerns that a follow-on policy requiring acceptance of other components' adjudications could further present potential vulnerabilities.

Recommendation

CBP should open discussions with OPM to address shortfalls in suitability guidelines when considering placement in the agency's national security positions.

---

[64]Interview with OIA, Personnel Security Division (PSD) staff, November 22, 2011.

OPM guidelines for suitability determination may be overly permissive for the types of responsibilities inherent in CBP national security positions. Additionally, the Department of Homeland Security and its components may want to reconsider the current DHS policy of accepting potentially dated prior agency background investigations for intra-departmental transfers, especially for national security positions.

Surge Hiring

Discussion of Findings

The corruption problems that CBP faces today are often attributed, at least in the media, to the surge in hiring that occurred between 2006 and 2008, as the following example attests:

> Critics, including the union representing agents, warned...the agency was moving too fast, shortcutting background checks, lowering hiring standards and truncating the training time at the Border Patrol Academy in New Mexico. They warned one unintended consequence could be more cases of misconduct and *corruption.*[65]

Two compelling points arose in the study team's findings on this subject. First, persons we spoke with for this study disagreed as to whether corruption is actually attributable to the attempts in the 2006 – 2008 time frame to hire more law enforcement officers to meet congressional mandates. Several persons suggested that many of the 134 employees implicated on corruption charges were not hired during the surge, but rather were several years into their careers with the agency. The OIA Integrity Programs Division (IPD) Behavioral Research Branch has studied the tenures of the 134 and demonstrated that nine percent (twelve persons) were surge hires.[66] However, this analysis is inconclusive given the fact that CBP and its IPD analysts do not have any knowledge of cases currently under investigation by the DHS Office of Inspector General.

(There have also been reports in the media suggesting that personnel have been hired prior to the completion of their background investigations. However, persons we spoke with indicated that 100 percent of applicants' background investigations are completed prior to their appointment.)

The other compelling point in the study team's findings is that surge hires have yet to reach that point in their careers where individuals appear to be more likely to become corrupt. For example, further analysis may reveal that corrupt frontline CBP employees typically conduct these felonious acts in the 8-12 year points in their careers. Those surge hires appointed in the 2007-2009 time frame have yet to reach that point in their careers.

---

[65] G. Moran, "Hiring Practices Questioned after Border Agent's Arrest," *Sign On San Diego*, 1 April 2011, http://www.signonsandiego.com/news/2011/apr/01/hiring-practices-questioned-after-border-agents-ar/.

[66] Of the 134 cases, tenures ranged between one year to 33.5 years of CBP (and legacy agency) service at the time of the arrest/indictment, with the mean CBP tenure of 8.75 years and median 7.42 years.

Discussion of Recommendation

CBP should consider conducting a conclusive analysis of the tenure of employees arrested or convicted for corruption—specifically, to consider the most likely career points for this malfeasance and the effects of surge hiring. The agency may wish to defer this initiative until DHS OIG provides CBP with information of the cases it is currently holds. The compiled data may be able to confirm, deny, or otherwise support further development of the hypothesis of a link between surge hiring and workforce corruption. If it is found that a statistically significant portion of the sample was recruited during the hiring surge, additional research should be undertaken to determine if there were any aspects of the vetting process that may have led to some unsuitable candidates being hired.

Psychological Evaluations

Discussion of Findings

Law enforcement agencies commonly use psychological evaluations in vetting job candidates. These evaluations assess the candidate's "psychological suitability," which refers to both the absence of job-relevant risk factors as well as the presence of job-critical personal and interpersonal qualities.[67] A variety of tests seek to ensure law enforcement candidates are able to tolerate the stresses of their work environment, follow rules, use resources responsibly, behave in a trustworthy manner, use good judgment, and refrain from off-duty behavior that would reflect poorly on their department.[68]

CBP candidates do not receive a formal psychological evaluation as part of the applicant screening process. According to the persons we spoke with, the medical examinations required of all recruits do ask some questions about the candidates' mental health. However, we were told that, in order for a psychological evaluation to occur, the candidate must have a history of depression or counseling that comes up as part of the medical examination.

When we asked why psychological evaluations are not a standard part of the candidate vetting process, we learned that the large volume of job candidates as well as resource constraints prevents CBP from administering such evaluations.

Discussion of Recommendation

CBP should consider implementing pre-employment psychological (and additional) testing. Most progressive local law enforcement agencies have been performing pre-screening psychological evaluations on their applicants for decades. The IPD Behavioral Research Branch (BRB) has looked into the use of psychological evaluations for CBP job

[67] Y.S. Ben-Porath et al., "Assessing the Psychological Suitability of Candidates for Law Enforcement Positions," *Police Chief Magazine*, no.78, August 2011, http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=print_display&article_id=2448&issue_id=82011.

[68] Ibid.

candidates and concluded "there is a demonstrated value in assessing the psychological suitability of law enforcement applicants and including it in a multi-layered approach to personnel screening." [69]

The Hillard Heintze Senior Leadership Council also indicated they are firm supporters and advocates for the use of psychological evaluations. The council suggests that the evaluation may be one of the most important phases of the hiring process, as the following explains:

- Many local law enforcement agencies also require internal candidates for some highly sensitive positions to undergo such examinations both going into and coming out of certain types of units, such as Special Weapons and Assault Teams (SWAT) and Child Exploitation Investigation Units.
- Many local law enforcement agencies also reserve management's right to require certain employees to submit to psychological evaluations (sometimes called Fitness for Duty Examinations) under certain circumstances. Instances in which an employee has engaged either in some unusual behavior while at work or actual misconduct may warrant an exam to determine the employee's psychological state.
- The nation's litigious society has come to the point that failure to conduct such examinations on prospective employees, as well as failure to conduct such examinations for current employees under the other circumstances already noted, could open up an agency to "negligent retention" lawsuits.

Any efforts to incorporate psychological screening would benefit from the research already conducted by IPD, as well as from the International Association of Chiefs of Police (IACP) Police Psychological Services. The IACP has developed guidelines for conducting pre-employment psychological evaluations. These guidelines take into consideration various restrictions imposed by the Americans with Disabilities Act, to include the stipulation that psychological examinations can only be conducted after a conditional offer of employment has been made.[70] Other guidelines developed by IACP address the need for the psychologist to be familiar with the specific working conditions of the job and the usefulness of integrating findings from a candidate's background investigation and polygraph examination into the interview process.[71]

Entry-Level Polygraphs

Discussion of Findings

[69] IPD Behavioral Research Branch, "Project Two of the Internal Affairs Best Practices Initiative: Pre-Employment Psychological Evaluations," September 30, 2010, p. 5.

[70] IACP Police Psychological Services Section, "Guidelines for Police Psychological Service," *Police Chief Magazine*, vol. 72, no. 9, September 2005.

[71] Ibid.

The Anti-Border Corruption Act of 2010 established a policy calling for all CBP law enforcement position applicants to undergo a polygraph examination and a background investigation before being offered employment. As noted in the first finding and recommendation here—on doing polygraphs prior to background checks as a way to save time and resources in the vetting process—polygraphs are critical to recruitment for organizations like CBP. Yet, based on our interviews for this study, it was apparent there has been some organizational resistance to entry-level polygraphs. Several of the persons we spoke with at headquarters expressed some level of opposition to such polygraphs, while most of the persons we spoke with in the field expressed support for this assessment tool. There were no apparent correlations to these diverse opinions.

Whether or not the use of the polygraph examination is supported by staff, there is strong data to support its effectiveness in vetting job candidates. Polygraphs have been detecting matters that would not have been exposed through other vetting tools. The IPD BRB *A+ Case File Study* (figure 6) attests to this finding.

The A+ Case File Study: An Exploration of the Statements Made Against Personal Interest in Law Enforcement Screening Polygraph Examinations (2009)

Conducted by: The Office of Internal Affairs, Integrity Programs Division (IPD) Behavioral Research Branch and the Credibility Assessment Division (CAD)

This exploratory study reviewed 24 failed applicant polygraph examinations to describe the nature of information revealed during polygraph exams and identify any common elements.

Findings:

- Study appears to validate the notion that pre-employment polygraphs yielded [illegible]

Figure 6. Findings from the 2009 IPD *A+ Case File Study* about polygraphs[72]

We reviewed data and studies developed by IPD that indicated polygraphs have led to admissions in the following areas:

- organized crime (involvement with drug-trafficking organizations, human smuggling/trafficking, other criminal associations)
- citizenship issues (self or family)
- crimes against persons

[72] *A+ Case Study*, p. 9.

- property crimes
- illegal drug activity
- counterintelligence issues (compromise of classified information)
- countermeasures (attempts to "game" the polygraph or cover up things they have done)[73]

Furthermore, BRB found that, for many of the individuals who have admitted to participating in illicit activities such as those listed above, the activities "were not youthful indiscretions or one-time mistakes, but rather represented a pattern of behaviors."[74]

We also learned from CBP staff that polygraph examinations have identified at least fifteen individuals who were deliberately trying to infiltrate the organization for illicit purposes.

Discussion of Recommendation

The CBP OIA Credibility Assessment Division should continue steadily accumulating a cadre of 85 polygraphers to meet the congressional Anti-Border Corruption Act mandate of being able to, by January 1, 2013, test all CBP officer and agent recruits before employment.

The Test/No-Test Study (2010)

Conducted by: The Office of Internal Affairs, Integrity Programs Division (IPD) Behavioral Research Branch

Using a random sample, the Behavioral Research Branch compared the employment records of persons who did and did not take a pre-employment polygraph examination to identify negative conduct of the employees.

Findings: Analysis revealed the persons who did not take the polygraph were more than twice as likely to be on record with Internal Affairs for negative conduct [illegible] who did take the polygraph.

Figure 7. Findings from the 2010 IPD *Test/No-Test Study* about polygraphs[75]

CBP should also consider periodic polygraphs for its law enforcement employees once the polygraphers' cadre is at full capacity. This testing could be conducted on five-year

[73] Ibid., pp. 6-7.

[74] Ibid., p. 10.

[75] CBP OIA Integrity Programs Division Behavioral Research Branch, *Test vs. No-Test: Pre-Employment Polygraph Exams and Subsequent Record with Internal Affairs*, (September 16, 2010), page 2.

intervals in conjunction with the periodic background investigation (BI) to avert any deceptions in the BI process. If this method exceeds testing capacities, a more strategic approach may be required. An "early warning system" could prove valuable and perhaps more cost-effective by randomly subjecting to such tests those most likely to be experiencing problems.[76] CBP should also consider the testing of specific employee populations, e.g., national security positions, with random polygraph examinations, much like random drug testing.

[76] "Early warning systems" are data-based police management tools designed to identify officers whose behavior is problematic and provide a form of intervention to correct that performance. Samuel Walker, Geoffrey Alpert, and Dennis Kenney, "Early Warning Systems: Responding to the Problem Police Officer" Research in Brief, National Institute of Justice, U.S. Department of justice, NJC 188565 (July 2001), www.ncjrs.gov/pdffiles1/nij/188565.pdf.

SECTION III. INTEGRITY TRAINING PROCESS AND PROGRAMS

The study team assessed existing training programs designed to develop ethical behavior in both Border Patrol agents and CBP officers at the entry and supervisory levels, and the rest of the continuum of an agent/officer's career. We conducted this evaluation through discussions with Office of Training and Development (OTD) leadership, as well as representatives of the Field Operations Academy (FOA), Border Patrol Academy (BPA), and the Advanced Training Center (ATC) who directly oversee workforce integrity/counter-corruption-related academic programs and curricula. We also reviewed associated courseware provided to us by OTD. (See appendix G for a list of that courseware, and recommendations for a comprehensive review of CBP ethics and integrity training programs.) Finally, the team considered "messaging" (how topics are woven thematically into communicative materials) as a subset of continuing training and education by discussing training themes in the field and reviewing CBP intranet (CBPnet) content.

Overview of Findings and Recommendations

- Follow-on refresher ethics, integrity and counter-corruption training offered in the field take on a variety of forms. CBP should designate one authority on ethics and integrity training to coordinate courseware content and messaging throughout the agency.
- Emphasis in exactly what things CBP wants its employees to be doing in regards to the day-to-day application of ethics appears to be missing from the training materials/lesson plans. CBP should emphasize the practical application of ethics concepts within the day-to-day work of both first-line employees and supervisors, and better inform CBP staff of any organization-wide training.
- The CBPnet web content for integrity and counter-corruption is spread across several pages of the website. Integrity and counter-corruption messaging on the CBPnet would benefit by having a central site for all of this information.

The following is a discussion, in order, of those findings and recommendations.

Assessment

Ethics and Integrity Training Programs

Discussion of Findings

CBP provides training focused on ethics, integrity and ethical decision making throughout an employee's career, since—as with any organization—training is essential to establishing and reaffirming an organizations' values, ethos and code of conduct. Entry-level training ingrains in the recruits the fundamental precepts by which the organization conducts itself, and offers standards to which they should aspire.

Supervisory training prepares mid-level managers to lead and look after their personnel, and foster expected performance and behavior. Continuing education and training reinforces and reaffirms organizational goals and standards.

Covering these various levels of training for CBP are a handful of entities. As noted earlier, formal integrity and counter-corruption training is developed and provided to the workforce by OTD, OIA Integrity Programs Division, the Field Officer and Border Patrol Academies, CBP IA special agents, DHS OIG special agents, and supervisors and CBP integrity officers at shift musters. The Office of Chief Counsel also administers ethics training.

The variety of training entities presents a variety of training on ethics. The New Employee Orientation Program, for example, provides at least two hours of workforce integrity training for all CBP personnel. Newly hired CBP law enforcement officers receive expanded ethics and integrity instruction tailored to their workplaces, as part of their basic training curricula.

Beyond their initial entry on duty, CBP employees receive advanced and specialized training which includes integrity elements. CBP supervisory and leadership training programs include Supervisory Leadership Training, Incumbent Supervisory Training, the CBP Leadership Institute, the Command Leadership Academy, and the DHS Senior Executive Service Candidate Development Program. Those programs include seminars, classroom instruction, and practical exercises that prepare CBP leadership to direct the workforce in a manner that advances integrity and accountability through critical thinking and ethical decision making.[77]

The training activities at the Field Operations Academy in Glynco, GA, Border Patrol Academy in Artesia, NM, and the Advanced Training Center in Harpers Ferry, WV, include ethics and integrity modules and themes explicitly and implicitly. In addition, themes such as CBP's core values of "Vigilance, Service and Integrity"; OTD's guiding principles of "MESH (Mission Focused, Esprit de Corps, Sustained Excellence and Honesty)"; and the Border Patrol motto "Honor First" receive prominent treatment. In some courses, Commissioner Alan Bersin's theme, "Corruption is the dagger pointing at the heart of Customs and Border Protection," receives emphasis.

Follow-on refresher ethics, integrity, and counter-corruption training offered in the field take on a variety of forms. Standardized training modules developed by OTD's Training Production and Standards Division (TPSD) and offered online and by local instructors appear to be of high quality and consistency. However, in our discussions in the field, we were told that the quality of the training varies with the organization offering the instruction and the individual instructors.

---

[77] *Hearing on Border Corruption: Assessing Customs and Border Protection and the Department of Homeland Security Inspector General's Office Collaboration in the Fight to Prevent Corruption , Before the Senate Homeland Security and Governmental Affairs Committee, Ad Hoc Subcommittee on Disaster Recovery and Intergovernmental Affairs*, 112th Congress (June 9, 2011) (statement of Alan D. Bersin, CBP Commissioner).

Discussion of Recommendation

CBP should designate one authority on ethics and integrity training to coordinate courseware content and messaging throughout the agency. Covering so many levels of training in any subject, in an organization this large, without a single authority overseeing it all presents the potential for inconsistencies. The consistency of the instruction and themes may suffer when multiple organizations with different interests lecture field-activity personnel.

Ethics and Integrity Training Themes[78]

Discussion

While we note a variety of positive aspects of the training as outlined in the training materials provided, there were also a number of questions that arose during our review that suggest further analysis and consideration - answers to which could serve to enhance the overall effectiveness of CBP ethics training. A few of these concerns follow:

- Universal Definition of Ethics: While it was readily apparent that the CBP courses each dedicated a portion of their training to defining ethics and integrity and to highlighting the importance of ethics to their agencies' work, it was not apparent that there is a universal definition of ethics for the greater CBP organization that is emphasized in each and every CBP course. In other words, it is not clear if each basic academy and advanced training course speaks with one overall CBP voice in terms of an ethics definition and expectations.

  Questions for consideration are:

  - Is there a coordinated effort within each of the CBP's training delivery groups to ensure they are addressing the same ethics concepts, using the same definition, as the other CBP training groups, with a goal to set a CBP-wide standard for ethical expectations and behavior?
  - Are CBP's organization-wide goals and objectives for addressing corruption identified, and if so are they to be found within each training course?

- Root Cause Analysis of Corruption and a Focus on Ethics Application: While a number of the courses did highlight discussions of some real-life cases in which corruption had been identified, the discussion did not seem to do much more than highlight how some corruption cases came to light and how they damaged the

[78] The following is the Hillard Heintze SLC training subject matter experts' (SMEs) initial assessment of how the various materials above interrelate and how they appear to address CBP's current concerns. These are only the initial impressions and opinions of the SMEs—including the recommendations they give at the end of this assessment. Given the gravity of the topic and the complexities of the material, additional review and analysis should be done to yield concrete recommendations regarding training methodologies and their effectiveness.

reputation of CBP. It was unclear if the discussion moved from simply discussing the outcomes of corruption to clearly emphasizing a CBP-wide strategy about how to prevent, detect, investigate and report corruption.

For example, in the Second-Level Command Preparation course, it was apparent that a number of different situations involving ethical lapses were discussed (Abu Ghraib prison, the Rodney King incident, the Kitty Genovese incident, My Lai Massacre, Tailhook scandal, etc.). Yet these course materials did not seem to go much beyond such philosophical discussions. It did not appear that the major emphasis was on what actions CBP supervisors could or should take on a daily basis to prevent, detect, investigate and/or report corruption.

While this particular course's material does discuss paying attention to issues that should lead a supervisor to detect corruption (described at times as "red flag" issues), the material leaves readers with the sense that a relatively small portion of the overall training time focused on this very important component of being a supervisor.

Indeed, even the final essay that the Second-Level Command Preparation Course attendees are required to write—describing a real-life, work-related ethical dilemma each trainee had experienced—seemed to highlight discussion about what could be done to improve the response to the dilemma, rather than proactive measures that could be taken to prevent or detect it. Instead, the essay's emphasis included answering the following questions (taken from page 4-89):

- What is the nature of the ethical problem?
- Was the action taken appropriate?
- If the action taken was not appropriate, what should have happened?
- What lessons were learned?
- Would the information provided in this lesson have been applicable, and would it have resulted in a better/different outcome?

Missing from this course's material were such questions as the following, which emphasize proactive efforts on the part of supervisors to prevent such dilemmas in the first place:

- What actions might I as a supervisor have taken to prevent this ethical dilemma from occurring in the first place?
- Did I share this dilemma with my own supervisor as soon as possible?

- "Bright Line" Behaviors: Because of the concerns that CBP has regarding workforce integrity and corruption within its organization, it would seem extremely important to place the greatest emphasis in its training courses on the specific behaviors it expects from its members. Hence, while there was a great deal of commendable philosophical discussion about the importance of values and ethics in the course overviews and

instructor's guide we reviewed, it was unclear whether CBP has drawn a "bright line" about what is acceptable (and what is not) in terms of ethical behavior. Bright line standards are a means of ensuring that all employees are very clear about some very specific types of misconduct that will result in very specific levels of discipline.

This seems especially important given the fact that there has been such a rapid increase in the number of CBP employees in recent years, and because it appears that so many newer employees are being promoted so much sooner within their careers to keep pace with the organizational growth. Hence, what appears to be missing from the training materials/lesson plans is emphasis in *exactly* what things CBP wants its employees to be doing in regards to the day-to-day *application* of ethics, as well as an emphasis on training supervisors on the nuts-and-bolts, day-to-day tasks that one would expect them to engage in to prevent, detect, investigate and report unethical behavior.

For instance, using the Second-Level Command Preparation Ethics course as just one example, the following might be a few samples of training components of great value that could be incorporated, for the supervisor trainees as well as for the organization itself:

- A description and review of IPD's Corruption Case Study, which discusses employment histories and performance, demographics, social contacts, misconduct and discipline, and other important data points. Simply having a better understanding of what the organization is actually doing to address corruption issues, as well as a discussion of how such efforts can be of use to CBP supervisors on their "home turf," can go a long way in helping the staff feel that there is an organization-wide plan to address corruption issues. It can also help boost morale and instill a sense that they, as supervisors, are part of the organization's solutions to corruption.
- A review of CBP's *Annual Report on Employee Delinquency* would be of value when highlighting what real-time problems are occurring within CBP, which would tend to highlight what supervisors specifically need to be addressing back in their part of the organization.
- An IA investigator's perspective on what they wish CBP supervisors in the field would be doing to address corruption issues on a day-to-day basis, with an emphasis on preventing corruption cases.
- A checklist of specific "red flags," or things to watch out for with employees that might tend to indicate ethical issues when reviewing their subordinates' work-related performance on a day-to-day basis. Small-group discussions could then be initiated in which scenarios could be presented that require the supervisors to determine what ethical problems might exist, what specific steps they would take to address it, and how to communicate the problem with their chain of command.

- A very candid discussion of what their specific roles and responsibilities are as supervisors, with emphasis on the accountability that CBP expects of them. Trainees should leave the course with a very clear understanding of what, specifically, are their roles and responsibilities and what is expected of them regarding CBP's anti-corruption efforts.

Discussion of Recommendation

CBP should emphasize the practical application of ethics concepts within the day-to-day work of both first-line employees and supervisors, and better inform CBP staff of any organization-wide training. This emphasis, in exactly what things CBP wants its employees to be *doing* in regards to the day-to-day *application* of ethics, appears to be missing from the training materials/lesson plans.

The study team further recommends a review more in-depth than the one accomplished here of training issues, to determine what additional steps could be taken to ensure that CBP's ethics/integrity training highlights the practical application of ethics as stated above. Such a review should also inform CBP of what organization-wide efforts can help bolster training efforts to meet the expectations set by CBP management (e.g., Commissioner Bersin's theme implying that CBP "stop the dagger"). Appendix G suggests an approach to this review.

CBPnet Content and Messaging

Discussion of Findings

The study team wanted to determine the extent to which less formal, non-training communications conveyed workforce integrity and counter-corruption themes. To do this they surveyed the agency-wide CBPnet for content and messaging, and noted that CBPnet features the following relevant sites:

- "Commissioner's Message: Assuring the Highest Standards of Integrity"

  The text version of this message, housed on the commissioner's page, was easily accessible. There were also two linked videos related to the written statement: (1) Commissioner Bersin formally presenting the message from a podium at CBP headquarters; and (2) a subsequent video entitled "Integrity Town Hall Meeting".

- "Message from Chief Fisher: Wellton Station Border Patrol Agent Arrested"

  Posted on U.S. Border Patrol Chief Fisher's webpage, the written message offers a basic description of the April 5, 2011 arrest. A linked audio recording from Chief Fisher included after the written message offers a more personal message condemning the agent's actions.

- "Trust Betrayed"

  Located on the CBP Office of Internal Affairs website, the official title of this page is "Trust Betrayed: As Guardians of Our Nation's Borders, We Cannot Afford a Weak Link." The section offers "snapshots" of information related to

individual field officer or Border Patrol officers and agents who have been convicted of corruption-related offenses. It also includes instructions for reporting attempted bribes and other corruption-related behavior.

- "Vigilance, Service, Honor"

  This theme is located in the Office of Public Affairs (OPA) portion of the CBP intranet website. The opening segment of this section states, "Every day, outstanding, CBP courageousness brings respect and honor to us all." It goes on to offer profiles of field officer and Border Patrol officers and agents who have distinguished themselves by acts of heroism and high integrity. Interestingly, if considered as the counterpoint to "Trust Betrayed," this site does not experience nearly as many "hits" as "Trust...."

- Anti-Corruption Training Videos

  Three anti-corruption training videos produced by CBP's Field Communications Branch appear on the Office of Border Patrol page. The first video focuses on on-duty malfeasance; the second deals with a Border Patrol agent using his badge and personal relationship with a bouncer to obtain access to a nightclub; the third addresses debt issues. The videos all offer good overviews of potential corruption pitfalls. They are well made and provide a good tool to bridge the gap between other types of ethics/integrity instruction.

- Video Message from former Border Patrol Chief Ron Colburn

  Posted to the Office of Border Patrol in March of 2009, former Chief Colburn delivers a stern anti-corruption message with a forceful warning to Border Patrol agents that corruption is treason.

The CBPnet content is, overall, informative, interesting, and timely. However, the information is spread across several pages of the website.

Discussion of Recommendation

Integrity and counter-corruption messaging on the CBPnet would benefit by having a central site for all of this information. One way to centralize the content is to build an "integrity website" or webpage with links to the other related sites. This also stands to add uniformity and decrease duplication of effort.

SECTION IV. METRICS AND INFORMATION SHARING PROCESS

The study team, including Hillard Heintze SLC SMEs, considered CBP's existing metrics for identifying and determining the level of corruption in the workforce, focusing on whether they are sufficient to meet the information needs of CBP offices and partner agencies responsible for countering corruption and heightening integrity. We consulted with the CBP Office of Human Resources Management (HRM) and its Labor and Employee Relations Division (LER) as well as IPD. We placed particular emphasis on areas we believe could assist upper-level management and supervisors in collecting and reviewing specific data to help them be more proactive in preventing or discovering discipline violations. We also extensively reviewed the HRM LER "U.S. Customs and Border Protection Discipline Report for Fiscal Year 2010" briefing for content and statistics, as an example of disciplinary data being collected and reported.

Overview of Findings and Recommendations

- There is no comprehensive picture of workforce corruption. CBP should consider implementing a central, unified tracking system for all the important data that could be used to prevent, detect, and deter misconduct and corruption.
    - CBP should also emphasize to DHS OIG the need for transparency in cases involving CBP employees.
    - Finally, IPD Behavioral Research Branch should undertake a "Code of Silence" study.
- The organization of disciplinary data is lacking in several significant ways (e.g., some types of discipline appear to be missing from the data). CBP LER should consider the collection, breakdown, and analysis of the data sets discussed in this paper, and conduct further study to determine other data requirements.

The following is a discussion, in order, of those findings and recommendations.

Assessment

Data Collection and Reporting

Discussion of Findings

The study team found, in their research of this particular area, that there is no comprehensive picture of workforce corruption—that is, enough data to gauge the breadth and depth of this corruption problem in CBP. Without that full situational awareness,

- the extent of corruption cannot be determined, and

- the most efficient measures to address the problem cannot be determined (e.g., either prioritization of investigations, "breakpoints" for administrative adjudication, or criminal investigation and prosecution are undetermined).

CBP's greatest impediment to gathering this information is, as noted earlier, the lack of visibility of all instances of malfeasance within the agency, due to DHS OIG's withholding of allegations against CBP personnel that they have received directly. It is unclear whether an organization-wide process is in place to ensure that all cases of misconduct are being reported to the Joint Intake Center in accordance with prescribed criteria. A potential impediment to reporting misconduct is—as noted earlier, as well—the extent to which the "code of silence" exists among the workforce.

The OIA Integrity Programs Division tracks known cases of corruption as evidenced by arrests and indictments. OIA maintains a database of employee delinquency defined as all arrests, indictments, citations, and detainments for violations of law reported to the Joint Intake Center. Variables include employee demographics, organizational assignment, geographic location, and charges/offenses among many other fields. In cases of corruption and mission-compromising corruption,[79] OIA keeps a record of the investigative entity as well as any other agencies involved in the case, plus the investigative timeline from the date of the first report of investigation (ROI) to the date of arrest.

Based on these collected metrics, IPD generates the following reports:

- *Annual Report on Delinquency* – a yearly report addressing both corruption and mission-compromising corruption, distributed within OIA
- *Commissioner's Snapshot* – a monthly report on the number of each level of employee delinquency, based on a year-to-date comparison to the same time in previous fiscal years, distributed to the CBP commissioner and OIA internally
- *Weekly Update on DHS OIG Cases* - prepared jointly by OIA's IPD and Investigative Operations Division (IOD) on DHS OIG involvement in cases on CBP employees submitted to the commissioner. The report contains the total number and status (open/closed) of DHS OIG cases on CBP employees uploaded into the Joint Integrity Case Management System (JICMS), as well as the nature of DHS OIG involvement.
- *Ad Hoc Data Calls* – IPD responds to numerous questions posed by CBP constituents (e.g., commissioner and deputy commissioner offices, OIA

[79] Corruption is defined as a violation of law in which a CBP employee misuses or abuses the knowledge, access, or authority granted by virtue of official position for personal gain. Mission-compromising corruption is a violation of law in which a CBP employee misuses or abuses the knowledge, access, or authority granted by virtue of official position for personal gain, *and* the activity violates or facilitates the violation of laws that CBP enforces.

assistant commissioner [AC] and deputy AC) and external entities related to employee delinquency (e.g., DHS, Congress, and the media).

The HRM Labor and Employee Relations Division tracks the broad spectrum of disciplinary reports and actions, from removals to formal counseling to cases closed without action. This data is reported in the annual *HRM LER Discipline Report* provided to the commissioner and deputy commissioner.

Discussion of Recommendation

CBP should consider implementing a central, unified tracking system for all the important data that could be used to prevent, detect, and deter misconduct and corruption. CBP should emphasize to DHS OIG the need for transparency in cases involving CBP employees—to further add to such data to be tracked. Furthermore, the IPD Behavioral Research Branch should undertake a "Code of Silence" study.

In order to address workforce integrity issues and counter corruption, the extent of the problems must be determined. With the extent of the problems known, CBP management can identify specific measures and strategies to deal with the prevalent issues. A unified tracking system would combine OIA IPD's tracking of employee delinquency. Optimally, this data would include information on cases held by DHS OIG currently withheld from the agency.

A comprehensive picture of workforce delinquency and discipline would inform CBP training units in their development of informed measures and strategies to promote workforce integrity. The "Code of Silence Study" would not only assess the extent of the code within the CBP workforce, but also help gauge workforce integrity. Such studies are common to state and local law enforcement agencies.[80]

Data Analysis

Discussion of Findings

The OIA Integrity Programs Division conducts intelligence analysis of enforcement actions, data, and trends, and performs analysis in support of OIA investigations and pre-employment screening operations. Within IPD, the Behavioral Research Branch is a multidisciplinary unit that conducts behavioral research focused on the CBP workforce. Such research is intended to address operational issues and challenges, and to enhance the background investigation process. This nexus of the comprehensive ICE-CBP Joint Integrity Case Management System (JICMS) and other law enforcement databases, and targeted IPD analysis is an innovative best practice not seen in the vast majority of law enforcement agencies.

---

[80] Carl B. Klockars et al., "The Measurement of Police Integrity" Research in Brief, U.S. Department of Justice National Institute of Justice, NCJ 181465 (May 2000).

The HRM LER "U.S. Customs and Border Protection Discipline Report for Fiscal Year 2010" briefing provided content and statistics sufficient for an example here of disciplinary data being collected and reported. The results of that review are as follows:

- While the reporting data illustrates the types of violations and disciplinary outcomes, these two areas are not linked together in any significant way. For example, a "lack of candor" case does not indicate whether it resulted in a termination, nor does a "misuse of TECS[81]" case indicate whether it resulted in a short-term suspension. Furthermore, the gravity of cases is not made clear. Data indicates, for example, a high number of misconduct cases in San Diego, Rio Grande, Tucson and El Rio, but an area with fewer cases might have a greater percentage of the more serious ones.
- Some types of discipline appear to be missing from the data that are typically found in law enforcement agencies that do a good job of tracking their discipline cases. The most important missing item is what most agencies term a "Failure to Supervise." We found no data indicating that CBP was initiating disciplinary cases against supervisors who fail to do their jobs. There does not even appear to be a separate classification for this level of misconduct. Instead, violations such as these are most likely categorized as policy and procedures violations.
- A specific misconduct violation commonly defined as Failure to Report Misconduct also appears to be missing from the CBP discipline process. While this might fall under the Failure to Follow Policies and Procedures section of misconduct that could result in disciplinary or adverse actions, most progressive state and local law enforcement agencies highlight this type of misconduct in their programs.
- Another type of misconduct missing from the reporting documents is Sexual Harassment.

Discussion of Recommendation

CBP LER should consider the collection, breakdown and analysis of data sets in a way that is helpful for analyzing workforce corruption, as discussed above. For example, data points should be broken down and reported for each type of violation and individual CBP office or geographic location, and the gravity of the different cases made clear.

3,058 cases of CBP personnel misconduct were closed in FY 2010 without action. Knowing the specific outcomes for each specific misconduct violation in each location would allow management the ability to evaluate consistency in how discipline is meted out. Collecting and reporting such data would also send a message to all CBP offices that upper-level management is paying attention to these concerns at each location.

CBP should also, if they do not already do so, initiate disciplinary cases against supervisors who fail to do their jobs, and create a separate classification for this level of

[81] TECS is the Treasury Enforcement Communications System, a law enforcement database utilized by CBP and other federal agencies.

misconduct (i.e., "Failure to Supervise").We believe that there is a general consensus among state and local police administrators that an agency's first-line supervisors are the key to ensuring adherence to policies and procedures. Progressive agencies ensure that supervisors are trained well and then held accountable for their performance.

If CBP is initiating misconduct cases for "Failure to Supervise" in its "Failure to Follow Policy" sections, CBP should consider breaking this out and highlighting it as a separate misconduct violation so that its importance is emphasized to the organization. Moreover, by specifically defining this type of misconduct, any failure to supervise misconduct would require formal action by management.

Sexual Harassment should also be included in the reporting documents as a type of misconduct, as this ethical problem—like any ethical problem—stands to be traced to other ethical problems, like corruption. While it is unclear if these are being handled under the section dealing with Policy Violations, we believe CBP should highlight its proactive efforts in addressing concerns in this area. Given the number of CBP employees—over 59,000—there are presumably some sexual harassment violations.

It would also be helpful to have data indicating the number of discipline cases for personnel whose supervisors had also been disciplined. Correlating poor performance on the part of employees as a result of poor supervision could be helpful for a variety of management reasons, including training.

Although the number of misconduct cases for drug violations is identified, along with the results for random drug testing, we suggest breaking this data down even further. What drugs were involved? In which CBP offices and locations do these employees work—and has management in these offices been informed? Has CBP management taken any steps to determine whether the drugs employees were using in any given area were those most likely being transported illegally at the specific locations where the employees are working? For example, are CBP employees, stationed in certain offices along the Southwest Border, using cocaine in proportions greater than other types of drugs, and is cocaine the most predominant drug being smuggled in their assigned area? Data providing answers to these kinds of questions might provide red flags for management, indicating that some CBP employees might be acquiring their drugs through their CBP positions.

Identifying employees with a disciplinary record receiving further discipline is another extremely valuable piece of information warranting further analysis. For example, in FY 2010, among the general observations reported on the outcomes of the Discipline Review Boards, one indicated that 44 percent of the DRB cases involved employees with a prior disciplinary record. We recommend making this category a subject for further analysis with the following data provided:

- Types of misconduct involved, both in the present cases and in the prior cases
- Number of misconduct cases involving employees with either one, two, three or more prior cases
- Number of cases involving front-line employees and, separately, supervisors

- Average length of time between prior and current misconduct cases

The length of the DRB process itself also warrants scrutiny. The following data would reveal potential inefficiencies and reasons for protracted cases:

- The number of union requests for information and the types of cases involved
- Specific data on the time it took to schedule oral replies and the types of cases involved
- The number of Douglas Factors cases, and the types of cases involved
- The number of cases in which a case was delayed due to a change by a deciding official as well as the location and type of cases involved

If management is to be proactive in its efforts to address misconduct in a timely manner and track the effectiveness of its discipline process, this data is critical.

CBP should also conduct further study to determine other data requirements. There are data-related best practices currently being implemented within state and local law enforcement agencies that could provide CBP with the ability to do a much better job of informing it about the real-time state of its integrity assurance efforts.

Finally, HRM LER should consider a unit dedicated to analyzing data, with the goal of providing guidelines to upper-level management and supervisors on ways to deter, prevent, and mitigate misconduct. This analysis unit could also provide inputs to CBP training programs to assist in the development of training curricula and modules dealing with workforce integrity and counter-corruption subjects.

SECTION V. PREVENTION, DETECTION, MONITORING, AND INVESTIGATIVE PROGRAMS AND INITIATIVES

In addition to the focal areas addressed thus far, U.S. Customs and Border Protection has a broad array of programs and initiatives designed to promote workforce integrity, and to prevent, detect, monitor and investigate corruption. The expanse of programs and initiatives across the agency is significant and testifies to the concern and attention that CBP leadership and management place on workforce integrity and counter-corruption measures. To help frame our survey of these activities, the CBP Office of Human Resource Management provided the study team with a matrix of programs and initiatives developed by the Labor and Employee Relations Division in June 2011. Expanding that list to over 40 agency-wide programs and initiatives, we sought to get a better understanding of these endeavors—as well as to identify any other related programmatic efforts—through interviews and further research. Our goal was to determine if there are any gaps in current integrity and counter-corruption programs and initiatives.

Rather than discuss all of the programs and initiatives (see appendix C for the list), we chose to highlight a few that we believe merit further attention, either because they represent a best practice or because they may offer opportunities for more improvement and examination.

Overview of Findings and Recommendations

- The Employee Assistance Program (EAP) demonstrates that CBP has taken seriously its responsibility to provide remediation, education, and work-life support to its employees—including the types of counseling that can help CBP prevent or mitigate misconduct and corruption. CBP should consider implementing two additional programs that would complement the CBP EAP's other work-life support initiatives: Peer Support Programs (PSPs) and Crisis Intervention Teams (CITs).

- The HRM Benefits, Medical and Worklife (BMWL) Division administers a random drug testing program that results in less than one percent positive results in FY 2010. Random drug testing should continue across the agency. Any changes in testing should contemplate a more strategic approach and ought to consider the inclusion of testing for commonly abused prescription drugs. The program may more appropriately belong in another part of the agency to avert any potential stigma of this detection program on BMWL employee assistance initiatives.

- The Analytical Management Systems Control Office (AMSCO) has, for the three years since its inception, identified and corrected operational vulnerabilities that would have allowed potential opportunities for employee corruption. CBP should continue to pursue the AMSCO program's full potential.

- The training currently provided to CBP integrity officers includes informal training at headquarters, largely on-the-job training within AMSCO. Integrity Officer Program managers should consider a more structured training syllabus, to include instruction in the broad range of workforce integrity and counter-corruption programs and initiatives that could assist and inform activities in the field.
- The operational environment that the U.S. Border Patrol's Integrity Advisory Committee monitors and addresses in their deliberations is dynamic. The committee and its chair should consider more frequent meetings.
- There are a number of noteworthy research initiatives within the two programs of the OIA Office of Integrity Programs that contribute to the CBP's efforts to prevent, detect, monitor, and investigate integrity and corruption issues. The proactive research, analysis, and reporting conducted by OIA IPD should be regarded as a best practice for consideration throughout the law enforcement community.
- The Integrated Policy Coordination Cell for Integrity (Integrity IPCC) has yet to adopt and implement a charter governing its activities—without which there is no clear articulation of the cell's vision, purpose, goals, objectives, structure and methodologies. The Integrity IPCC should develop and implement a charter, including consideration of its activities since inception to broaden the scope of its initial intent.

The following is a discussion, in order, of those findings and recommendations.

Assessment

Employee Assistance Program

Discussion of Findings

The CBP Employee Assistance Program administered by the BMWL Division offers employees and their family members counseling regarding issues that, if not dealt with, could foster corruption. The services are available 24/7 via an 800 number or on the dedicated EAP website. The voluntary confidential counseling services cover work-related problems, marital and family issues, life adjustments, medical situations, alcohol and drug abuse, and crisis intervention.[82] The EAP website has a special section dedicated to helping supervisors recognize personal problems that their employees may be experiencing, providing online training as well as guidance for making referrals. There is also a section on the website dedicated to suicide prevention, which is an excellent resource to address the agency's troubling suicide rate.[83]

[82] U.S. Customs and Border Protection, "Employee Assistance Program" (brochure, n.d.).

[83] The CY 2010 suicide rate in CBP was 20.73 suicides per 100,000 people. CBP's rates exceed those of several comparison groups, most notably the general population (11.26), law

The program in its entirety demonstrates that CBP has taken seriously its responsibility to provide remediation, education, and work-life support to its employees. The EAP website appears to be a best practice, as it meets or exceeds the quality of similar websites widely recognized within local and state law enforcement as being models.[84]

Discussion of Recommendation

CBP should consider implementing two additional programs that would complement the CBP EAP's other work-life support initiatives: Peer Support Programs (PSP) and Crisis Intervention Team (CIT) Programs. Progressive law enforcement agencies across the nation have implemented PSPs to provide training to rank and file employees, so they are able to support colleagues that are struggling to address various personal issues outlined in the EAP. Similarly, CIT programs provide specialized training to members of an organization who have gone through highly stressful experiences, either on- or off-duty, so they are able to offer assistance and mentoring to other employees going through similar experiences. We recommend CBP explore these programs and consider them for CBP due to the immense value they have provided to other law enforcement agencies. Peer support and CIT programs go a long way in signaling to all members of an organization that top management places a great value on the well being of each individual within the larger organization; such programs become even more important when managing an organization as large as CBP.

Random Drug Testing Program

Discussion of Findings

HRM BMWL administers the random drug testing program for the CBP workforce with ten percent of the population tested annually. The testing not only detects employees who use certain illicit substances, but also serves as a deterrent to those considering the use of drugs. In FY 2010, 5,083 random drug tests were conducted with 8 positive results (.16 percent; 7 actual positive results and 1 refusal to submit to the test).[85] While recognizing such yield is very small, it is critical for a law enforcement agency the size of CBP—which is involved in drug interdiction at so many levels—to continue to conduct such testing.

Supervisors may request authorization for employee drug testing by phone, but must follow up with a written request shortly thereafter.[86] Standard random drug testing includes a sampling of personnel at all levels of rank within the CBP organization. This is standard practice for most local law enforcement agencies—based on the premise that

enforcement (18.1), and the U.S. Army (20.6). Interview with CBP OIA IPD staff, November 22, 2011.

[84] Hillard Heintze subject matter experts, who specifically analyzed the EAP's offerings, suggested this about the EAP website.

[85] *U.S. Customs and Border Protection Discipline Report for Fiscal Year 2010*, slide 25.

[86] During their El Paso activities field visit, members of the study team spoke with CBP supervisors who were unaware of the availability of this testing.

leaders should be modeling the way their organization takes a stand against the use of illegal drugs.

Discussion of Recommendation

Random drug testing should continue across the agency. Any changes in testing should contemplate a more strategic approach and ought to consider the inclusion of testing for commonly abused prescription drugs. The program may more appropriately belong in another part of the agency to avert any potential stigma of this detection program on BMWL employee assistance initiatives. Each of these recommendations is discussed in order below.

First, we present the "more strategic approach." Rather than increasing the number of random drug tests that are administered, we believe it would be wiser and more cost-effective to be more strategic in terms of determining who is tested. CBP management should determine which employees are most at risk for exposure to illegal drugs and test them. Some agencies make such drug testing a condition of entry into high-risk units (e.g., many local law enforcement agencies test those who go into narcotics enforcement or vice squads). Implementing such a policy may require interaction and potential negotiation with CBP employee labor representatives, but local law enforcement has laid the groundwork for such policies. We also suggest consideration be given to testing these high-profile individuals annually.

Additionally, because the abuse of legally prescribed drugs has become a major issue in law enforcement agencies across the country, CBP should consider including testing for such drugs and reporting such abuse. While various legal considerations would need to be addressed, it may be worthwhile to consider developing a policy requiring employees to self-report when they are taking legally prescribed drugs that may have an intoxicating effect on an employee while at work (such as muscle relaxers or other pain medications). That would work to support the testing for the commonly abused prescription drugs. Steroid abuse is another ongoing problem for law enforcement agencies, so CBP should consider testing for steroids as well.

Finally, we recommend that CBP consider relocating the random drug testing program to an office or another division more suitable to its mission. The program, a misconduct detection and deterrence effort, currently resides in the Benefits, Medical and Worklife Division. This dichotomy has the potential to present a stigma on the employee assistance initiatives.

Analytical Management Systems Control Office Program

Discussion of Findings

AMSCO uses CBP's automated systems to analyze crossing, referral, and results data to identify anomalies that may be indicative of integrity issues. OFO works collaboratively with the local integrity officer and, if necessary, the Office of Internal Affairs to resolve any anomalies identified by AMSCO and to determine the nature of the aberration. By developing and leveraging programs such as the Enforcement Link Mobile Operations – Red Flag (ELMO-RF), ASMCO works with field integrity components to monitor

frontline activity through the use of integrity-based rule sets. ELMO-RF uses CBP data and systems capabilities to provide frontline supervisors immediate feedback on processing anomalies. This allows supervisors to have immediate interaction with front line staff to discuss transaction anomalies.

In the three years since its inception, AMSCO has identified and corrected operational vulnerabilities that would have allowed potential opportunities for employee corruption. Insights gained through AMSCO operations have also allowed the development of new methodologies and applications that bear the potential to identify performance deficiencies and to counter acts of corruption in the field, as well as to serve as a training and instructional tool. The Border Patrol has a pilot program underway to look into the applicability of AMSCO to its operations.

Discussion of Recommendation

CBP should continue to pursue the AMSCO program's full potential. AMSCO has proven to be a highly effective tool to identify field operations workplace vulnerabilities and counter workforce integrity issues. AMSCO is a best practice with the potential for adaptation to other high-volume, structured enterprises.

The effectiveness of AMSCO operations is dependent on teamwork between the OFO staff, integrity officers in the field, and IA special agents. For example, the study team has learned anecdotally there have been occasions when the point at which AMSCO data inquiry ends and the IA investigative work begins is not well understood by the parties. The AMSCO collaborators should develop guidelines to resolve these ambiguities.

Integrity Officer Program

Discussion of Findings

OFO has implemented an Integrity Officer Program that assigns experienced, supervisory level (GS13s) officers to each of the 18 field offices. Integrity officers focus explicitly on integrity-related matters. Working directly for the port of entry (POE) director of field operations (DFO), the integrity officer addresses the DFO's concerns and acts as a liaison to the workforce at the POEs and headquarters integrity counterparts. These officers provide training in classrooms and musters, support AMSCO headquarters inquiries, and provide law enforcement agencies with technical assistance on operational matters and investigations. Other duties include post-corruption case analysis and vulnerability assessments in the field.

In addition to having previous supervisory experience, integrity officers must have technical expertise with the CBP data collection systems, inspections, analysis, intelligence examinations and enforcement activities. Selectees for the program receive informal training at headquarters (where they are provided job aids), in addition to an on-the-job training period within the AMSCO office. That experience acquaints the trainees with AMSCO systems, databases, and techniques. Once in the field, the integrity officer corps is kept informed on program developments through regular correspondence and conference calls.

Discussion of Recommendation

Integrity Officer Program managers should consider a more structured training syllabus, to include instruction in the broad range of workforce integrity and counter-corruption programs and initiatives that could assist and inform activities in the field. The study team considers a dedicated integrity officer at each OFO field office as a best practice. However, we believe that training for such officers could be enhanced by drawing upon additional resources and knowledge existing throughout CBP, to include many of the programs and initiatives discussed within this section.

U.S. Border Patrol Integrity Advisory Committee

Discussion of Findings

The Integrity Advisory Committee's (IAC) mission is to "create strategic recommendations to combat corruption and promote integrity among all U.S. Border Patrol employees."[87] A review of the committee's charter indicates a well-structured organization and methodology, and defined goals and objectives. The committee provides strategic analysis of the Border Patrol's vulnerabilities as they relate to mission critical corruption: smuggling, bribery, conspiracy, and money laundering. The committee is responsible for developing options and recommendations to effectively combat corruption with the Border Patrol, addressing concerns related to agent and civilian employees. They also provide a variety of analyses (vulnerability analysis and post-corruption analysis), as well as develop recommendations regarding training and awareness programs. All Border Patrol workforce integrity and counter-corruption initiatives that are brought to the attention of the IAC as best practices are shared with the sectors. The Border Patrol chief receives any strategic recommendations that the committee makes.

Discussion of Recommendation

The committee and its chair should consider more frequent meetings. The IAC charter calls for quarterly meetings; however, in practice, meetings are held semiannually. Given the dynamic operational environment that the IAC monitors and addresses in their deliberations, it might be beneficial to convene more frequently.

Office of Internal Affairs, Integrity Programs Division (multiple programs and initiatives)

Discussion of Findings

The Office of Internal Affairs' Integrity Programs Division (IPD) conducts research and analysis and develops education programs aimed at preventing, deterring, and detecting employee misconduct and corruption. There are two programs within the OIA Office of Integrity Programs that are of special interest to the study team: the Proactive Research

[87] U.S. Customs and Border Protection, U.S. Border Patrol Integrity Advisory Committee briefing, May 2011.

and Analysis Operational Teams and the Behavioral Research Branch. Both of these programs leverage the division's existing research and resources in order to better understand and detect vulnerabilities in the CBP workforce.

Determining the effectiveness of these programs, as well as how their information is used, is not within the scope of the current task. However, there are a number of noteworthy research initiatives within the two programs that contribute to the CBP's efforts to prevent, detect, monitor, and investigate integrity and corruption issues. The following discusses some of them.

Proactive Research and Analysis Operational Teams

The Proactive Research and Analysis Operational (PROA) Teams were established to provide research aimed at detecting, deterring, and preventing corruption within the CBP workforce. The teams concentrate their efforts and expertise on a single operational area of vulnerability to determine where potential instances of misconduct or corruption may exist.[88] Research areas to date have included the following:

- Operation Side Door – evaluates the data and lead information from the Credibility and Assessment Division (CAD) polygraph examinations, where the applicants admitted to significant involvement with drugs or aliens. The data is examined to identify any nexus to existing CBP employees. PROA also looks for links between existing employees and any applicants who declined to take the polygraph.[89]
- Operation Red Flag – evaluates data derived from AMSCO (described above) and a variety of other CBP systems to identify potential anomalies or areas of vulnerability within the workforce.[90]
- Operation Hometown – evaluates the vulnerability of deployment of CBP and Border Patrol personnel to their respective "hometowns," focusing on high-threat areas along the Southwest border.[91]
- Operation Southern Exposure – the PROA Team evaluates post-seizure data from internal and external sources to identify possible indicators of CBP employee misconduct.[92]

[88] U.S. Customs and Border Protection, Office of Internal Affairs, Integrity Programs Division, "Proactive Research and Analysis Operational Teams," IPD Standard Operating Procedure #7, n.d.

[89] U.S. Customs and Border Protection, Office of Internal Affairs, Integrity Programs Division, "Proactive Research and Analysis Operational Teams, Operation Side Door," IPD Standard Operating Procedure #7a, n.d.

[90] U.S. Customs and Border Protection, Office of Internal Affairs, Integrity Programs Division, IPD Standard Operating Procedures, "Proactive Research and Analysis Operational Teams, Operation Red Flag," IPD Standard Operating Procedure #7b, n.d.

[91] U.S. Customs and Border Protection, Office of Internal Affairs, Integrity Programs Division, IPD Standard Operating Procedures, "Proactive Research and Analysis Operational Teams, Operation Hometown," IPD Standard Operating Procedure #7d, n.d.

When applicable, the PROA teams use their research and analysis to generate IPD cases for further investigation by the DHS OIG, ICE OPR, and/or the OIA/IPD. The teams look at other areas as well, such as financial analysis, toll analysis, and asset forfeiture.

Behavioral Research Branch

The Behavioral Research Branch is a multidisciplinary research unit that studies internal threats (at the individual, cultural, and organizational levels) that may compromise the integrity of CBP. The branch is comprised of individuals with experience in forensic psychology, criminology, sociology, and psychology. Staff members conduct research and analysis, perform evaluation, mine data, and provide consultations and training. The branch responds to ad hoc requests for data from the Office of Internal Affairs, other CBP constituents (e.g., the commissioner's office), as well as Congress and DHS.

The BRB's research agenda addresses various aspects of prevention (e.g. studying ways to build a better background investigation), detection (e.g., examining data from polygraphs to detect misconduct), and investigation (e.g., providing real time situational awareness on the prevalence of employee delinquency reported to the JIC and identifying trends over time). The branch provides monthly snapshots on delinquency, weekly DHS OIG case inventories, and annual reports on delinquency in the agency. The BRB's Corruption Case Studies research provides operational analysis of all known cases in which a CBP employee misused or otherwise abused his or her official position for personal gain, providing useful information to IA personnel in their work to prevent, detect, and investigate corruption in the CBP workforce.[93] The branch has also looked into a number of important issues surrounding integrity and corruption, to include studying code of silence issues and employee suicides, and identifying relevant best practices from other organizations.

Discussion of Recommendation

The proactive research, analysis and reporting conducted by OIA IPD should be regarded as a best practice for consideration throughout the law enforcement community. Their capabilities and products are a valuable resource both internally and externally, and should be promoted as such. The placement of IPD within OIA and co-located with complementary databases and functions—the Investigative Operations Division, the Joint Intake Center, the Personnel Security Division, and the Credibility Assessment Division—allows synergies uncommon in law enforcement. The OIA organization is a law enforcement best practice.

It is important to ensure that the information developed by the PROA teams and the BRB are shared with individuals who are responsible for promoting integrity and deterring corruption throughout the organization. Their analyses have direct implications for hiring,

[92] U.S. Customs and Border Protection, Office of Internal Affairs, Integrity Programs Division, IPD Standard Operating Procedures, "Proactive Research and Analysis Operational Teams, Operation Southern Exposure," IPD Standard Operating Procedure #7c, n.d.

[93] U.S. Customs and Border Protection, Office of Internal Affairs, Integrity Programs Division, "Behavioral Research Branch" (PowerPoint presentation, n.d.).

training, detecting, and investigating corruption and misconduct and could help inform efforts to develop an agency-wide integrity strategy.

Integrated Policy Coordination Cell for Integrity

Discussion of Findings

On March 28, 2011 CBP Commissioner Alan Bersin issued a "CBP Statement of Policy and Intent: Integrity" that clarified the integrity initiatives and goals under his leadership and outlined the principles that serve as a basis for all operational, staffing, budget, and resource decisions across CBP. (See appendix H for the full statement.) In order to ensure the implementation of the provisions of that policy, the commissioner established the Integrity IPCC under his office shortly thereafter. The cell's membership includes workforce integrity and counter-corruption functionaries from across CBP, and its departmental and interagency partners—including the DHS Office of Inspector General, Immigration and Customs Enforcement's Office of Professional Responsibility, and the FBI's Public Corruption Unit.

Since its inception, the Integrity IPCC has yet to adopt and implement a charter governing its activities. Without a charter, there is no clear articulation of the cell's vision, purpose, goals, objectives, structure and methodologies.

Discussion of Recommendation

The Integrity IPCC should develop and implement a charter. The charter should include the commissioner's "Statement of Policy and Intent: Integrity" initiatives, goals, and principles, and the methods to ensure their implementation. The charter should also consider the activities the cell has engaged in since inception to determine if it needs to broaden the scope beyond its initial intent. The IPCC should review its membership for inclusiveness to ensure that it is comprised of all the divisions that have roles in promoting integrity and addressing corruption. For example, the Integrity Programs Division—with its many integrity-related programs and initiatives—is not a standing member.

Given the members' broad representation and common interests in workforce integrity and counter-corruption, the cell could act as the nexus (i.e., point of coordination) of all related programs and initiatives across the agency.

SECTION VI. CONCLUSIONS

The wide range and number of CBP programs and initiatives on workforce integrity and counter-corruption measures testify to the concern and attention that CBP leadership and management give to the critical attribute—and issue—that is *integrity*.

Ethics and integrity training and continuing education at the entry, supervisory, and other leadership levels imbue and promote these principles in the workforce throughout their careers. Programs are in place to prevent and deter the occurrence of corruption in the workplace. Internal controls are set up to detect corruption or ill intent, and to monitor and administer the workforce for misconduct that indicates or could lead to corruption. Processes and resources focus on the investigation of both criminal and non-criminal allegations. CBP's aggressive approach to workforce integrity and counter-corruption measures has resulted in a number of law enforcement community best practices.

Nevertheless, corruption exists in CBP, as the arrest, charge, or conviction of over one hundred agents and officers in the past seven years testifies. Improvements and enhancements are possible, both internally and externally, in CBP's efforts to stem corruption. CBP's considerable number of programs and initiatives need comprehensive guidance in the form of a workforce integrity strategy. The agency should not only rethink its disciplinary system (including the way disciplinary data is handled), but also the organizational structure it shares with DHS OIG for the reporting, assignment, investigation, and disposition of CBP workforce investigations. Organizational matters external to CBP that bear on CBP need rethinking as well: OPM suitability guidelines for CBP national security positions, for example. Including CBP IA special agents in the national and regional BCTFs is an "organizational structure" that need no rethinking—it should continue, fostering further effective criminal investigations and efficiencies in combined counter-corruption efforts.

Perhaps the greatest enhancement can come from the individual CBP themselves, across the organization: CBP should emphasize in its ethics and integrity training exactly what the agency wants its employees to be doing daily in applying those principles.

CBP is neither alone nor unique in confronting issues with workforce integrity. State and local law enforcement agencies over the last several years have spent a great deal of time reviewing and improving their internal affairs and workforce management processes. CBP is poised to do the same.

Areas for Further Study

In the course of this project, the study team realized a number of areas that were beyond the scope of the task yet merit further study. The following subjects are recommended for CBP consideration.

Disciplinary Process

CBP should undertake a study to consider revisions to the current CBP disciplinary process. Initially established by the U.S. Customs Service in 1999 to service a population

of 22,000 employees, the process now deals with a 59,000-member workforce, many of whom operate in a highly volatile border environment. LER staff are overburdened with caseloads. The 151 days in FY10 from a Discipline Review Board to a final decision, noted earlier, is an inordinate amount of time. A study should consider measures introducing efficiencies while ensuring fairness.

Ethics and Integrity Training

The study team recommends that the Office of Training and Development consider a more in-depth review of training issues to help to determine what additional steps could be taken to enhance CBP's training in the areas of ethics and integrity. Such an effort should assist in highlighting the practical application of ethics concepts within the day-to-day work of both first-line employees and supervisors, as well as inform CBP of what organization-wide efforts may be taken to help bolster training efforts to meet the expectations set by CBP management.

"Code of Silence"

A proposed "Code of Silence Study" should be undertaken by the Integrity Programs Division Behavioral Research Branch in order to gauge workforce integrity and determine the extent the code exists within CBP ranks.

Surge Hiring

If DHS OIG provides CBP with information of the cases it currently holds, then the agency may wish to consider conducting analyses of the tenure of the persons who are currently under investigation, to assess when these individuals were hired. The compiled data may confirm or deny any links to the hiring surge and workforce corruption. If it is found that a statistically significant portion of the sample was recruited during the hiring surge, additional research should be undertaken to determine if there were any aspects of the vetting process that may have led to the hiring of unsuitable candidates.

Disciplinary Data Requirements

We recommend CBP consider a study to further determine the collection, breakdown, and analysis of the disciplinary data requirements toward more substantive analysis—to inform CBP leadership, management, supervisors, and the training establishment.

Early Warning Systems Implementation

One of the ways that state and local law enforcement agencies have improved their internal affairs and workforce management processes is in gathering, analyzing, and reporting their misconduct case statistics. These developments have led to the implementation of early warning systems (data-based police management tools designed to identify officers whose behavior is problematic, and to provide a measure for intervention to correct that performance). As existing employ behavior-related database systems are adapted and improved, CBP should consider the future implementation of an early warning system.

Future Threats and Vulnerabilities

CBP should consider a study to explore where future threats and vulnerabilities might lie. For example, if CBP considers the current corruption problem as an example of threat-shifting—we hardened our borders, making it more difficult for people to get in on their own, so they're relying upon insiders to help them—then the agency should consider conducting an analysis to determine what other types of threat-shifting behaviors may occur in the future that CBP will need to be prepared to address. The key to success is to think ahead to prevention versus reactionary response.

APPENDIX A. INTERVIEW ISSUES AND QUESTIONS FOR CBP HEADQUARTERS OFFICIALS

General Issues and Questions

1. What is the role of your organization/office in the CBP workforce integrity/counter-corruption enterprise?
    a. Are there particular aspects of the enterprise that you see as particularly effective or efficient?

2. What do you see as the key workforce integrity/counter-corruption issues facing CBP today? What are the highest-priority workforce integrity/counter-corruption issues facing your office?
    a. What do you feel are the solutions to these issues?
    b. Why?

3. What constraints or obstacles (if any) limit your office's ability to carry out its workforce integrity/counter-corruption role?
    a. These may include legal constraints and regulations, CBP and interagency policies, access to or budget for particular technologies, etc.
    b. Are you able to gather and/or access the information you need to support your efforts to counter corruption?

4. Are you aware of any external or internal influences that make you more or less concerned about corruption in the CBP workforce?
    a. If so, what are these influences?

5. Regarding the CBP workforce integrity/counter-corruption enterprise:
    a. Are there particular aspects that you see as in need of improvement, or areas in which you think CBP could benefit from understanding interagency best practices?
    b. Of the policies and procedures your office has in place in implementing your role, which do you see as most effective? Does your office have a particular program or policy that you see as a best practice applicable to other CBP offices?

6. How does your office define corruption? Integrity? Ethics?
    a. Does your definition(s) differ from the definitions used by others within CBP?
    b. If so, how? Why do you use this definition versus those being used by others within CBP?

7. With which offices do you collaborate or exchange information as part of efforts to counter corruption?

a. Include offices within CBP as well as interagency offices.

8. What workforce integrity/counter-corruption issues/lines of inquiry do you feel the Institute should pursue?
    a. Why?
    b. Whom should we talk to/where should we go to explore these issues?

9. Regarding the workforce integrity/counter-corruption enterprise, are there any best practices which you are aware of and would recommend for CBP implementation?

10. The Institute intends to conduct field studies as part of our research.
    a. Would you recommend any particular activities which would best inform our work?
    b. Why?

11. What other CBP organizations/offices do you recommend we confer with?
    a. Why?
    b. Is there any individual in particular whom you recommend?

12. Are there any interagency organizations/offices that you recommend we confer with?
    a. Why?
    b. Is there any individual in particular whom you recommend?

APPENDIX B. CBP OFFICES AND ACTIVITIES AND FEDERAL INTERAGENCY COUNTERPARTS INTERVIEWED

CBP Headquarters Offices and Divisions

Deputy Commissioner

Chief Counsel
- Associate Chief Counsel, Houston, TX

Assistant Commissioner (AC) Office of Field Operations
- Deputy Assistant Commissioner (DAC)
- Executive Director for Field Operations
- Analytic Management Systems Control Office (AMSCO)
- Incident Management Division

Deputy Chief Office of Border Patrol
- Strategic Planning, Policy and Analysis Division
- Integrity Advisory Committee

AC Office of Air and Marine

AC Office of Intelligence and Investigative Liaison (OIIL)
- Deputy Assistant Commissioner OIIL

AC Office of Human Resources Management
- Labor and Employee Relations Division
- Benefits, Medical and Worklife Division
- Personnel Research and Assessment Division
- Hiring Operations, Programs and Policy Division
    - Minneapolis Hiring Center

AC Office of Training and Development
- DAC Office of Training and Development
- Executive Director
    - Field Operations Academy
    - Border Patrol Academy
    - Advanced Training Center

AC Office of Internal Affairs
- DAC Office of Internal Affairs
    - Integrity Programs Division
        - Behavioral Research Branch
    - Investigative Operations Division
        - Joint Intake Center
    - Personnel Security Division
    - Credibility Assessment Division

AC Office of Congressional Affairs

Integrated Policy Coordination Cell for Integrity (Integrity IPCC)

CBP Field Activities – El Paso, Texas

Office of Field Operations Field Office
- Assistant Director
- Line supervisors
- Integrity Officer

U.S. Border Patrol Sector
- Chief
- Integrity representative
- Field supervisors

Office of Internal Affairs Field Office
- Special agent in charge (SAC)
- Deputy SAC
- Resident agents

El Paso Border Corruption Task Force
- FBI resident agent

Los Cruces, New Mexico Border Corruption Task Force
- FBI resident agent
- CBP Internal Affairs resident agent

DHS Office of Inspector General special agent

DHS and Federal Interagency

Department of Homeland Security
- Office of Inspector General – Assistant IG for Investigations
- Immigration and Customs Enforcement
  - Office of Professional Responsibility
- Transportation Security Administration
  - Office of Professional Responsibility
  - Inspections and Investigations Division

Department of Justice
- Office of Inspector General
- Federal Bureau of Investigation
  - Criminal Investigative Division
    - Public Corruption Unit
      - National Border Corruption Task Force
  - Inspections Section Internal Investigative Unit

Department of the Treasury
- Office of Inspector General

Department of Defense
- Office of Inspector General

Environmental Protection Agency
- Office of Inspector General – Assistant IG for Investigations

APPENDIX C. WORKFORCE INTEGRITY AND COUNTER-CORRUPTION PROGRAMS AND INITIATIVES

Focus Point	Program/Initiative	Lead Identity	Description
Prevention	Employee Assistance Program (EAP)	HRM/BMWL	The EAP provides all employees with 24/7 free, confidential counseling, information, and outside referrals for financial, stress, depression, parenting,
	WorkLife4You (Healthier CBP)	HRM/BMWL	WorkLife4You provides employees with 24/7 information, events, and activities that support work-life-balance and help employees become more resilient to day-to-day challenges in the job and at home.
	Integrity Officer Program	OFO	Integrity Officers are field operations officers who are specially selected and trained to promote integrity in the field offices. Special training includes four months working with AMSCO officers to learn the sophisticated IT tools that detect anomalies in the field operations. The Integrity Officers work directly for
	Integrity Committee	OFO	The purpose of the Integrity Committee is to ensure that the American public has absolute confidence in the integrity of CBP OFO employees. The committee reviews misconduct cases looking for vulnerabilities in order to prevent future corruption. The committee is comprised of CBP personnel from the entire agency include representatives from the Border Patrol the Employee Assistance Program.
Prevention	Integrity Advisory Council (IAC)	USBP	The IAC makes strategic recommendations Border Patrol Chief to combat corruption and promote integrity among all US Border Patrol employees. The council has broad representation from the USBP and has advisors and subject matter experts across CBP offices. The council is responsible for strategic analysis of four vulnerabilities: individual, operational, organizational, and leadership in
	Mandatory Supervisor Rotation	OFO/USBP	The mandatory supervisor rotation policy was recommended by the USBP's Integrity Advisory Council. The policy requires 25 percent of the BP's field supervisors to rotate annually.
	Electronic Integrity Messaging	USBP	24/7 integrity messages delivered to USBP stations via the Information Display System (IDS). The messaging includes videos on integrity that are based on real-life scenarios.

Focus Point	Program/Initiative	Lead Identity	Description
	Pre-employment Screening	HRM/IA	Pre-employment screening is preliminary screening of all applicants to determine potential background investigation issues. Applicants self-admitting to an issue who are selected are given an alternate tentative select letter that states that due to the self-admitted issue, they may be unsuitable for employment. At that time they are given an opportunity to respond (explain) to the suitability issue or opt out of the process by declining to respond.
Prevention	Background Investigations	HRM/IPD	[illegible] history to determine suitability for employment with CBP.
	Pre-employment Polygraphs	OIA/IPD	The Anti-border Corruption Act of 2010 requires that by January 1, 2013 all CBP law enforcement applicants receive a polygraph examination before being hired.
	Vulnerability Assessments	USBP	[illegible] based scenarios for corruption; the analysis helps to eliminate gaps through procedural changes, policy, oversight, and review (e.g., International Liaison Units ensure further vetting of personnel).
	Field Office Vulnerability Assessments	OFO	A vulnerability assessment of field operations helps to identify areas that may be a possible threat of corruption.
	[illegible] Integrity Visits	OFO/USBP	[illegible]
	Integrity Awareness Training for New Employees	OIA/IPD	The integrity briefing is incorporated into the New Employee Orientation Program (NEOP).
	Integrity Training for First Line Supervisors	OIA/IPD	[illegible] first line supervisors) undergo integrity training. The briefing is entitled "Leadership for Preventing Corruption."
	Integrity Training for Incumbent Second-Level Supervisors	OIA/IPD	The objectives of this training are to: (1) define ethics and ethical leadership; (2) recognize and avoid ethical traps in the workplace and elsewhere; and (3) follow a process for ethical decision making and apply it in future leadership decisions.
Prevention	Integrity Briefings for Foreign Posts	OIA/IPD	[illegible] assignment locations with a focus on container security.
	Integrated Policy Coordination Cell on Integrity (Integrity IPCC)	Commissioner's Office	Commissioner Bersin established the Integrity IPCC to ensure the implementation of the "Principles of Policy" articulated in his March 2011 "CBP Statement of Policy and Intent: Integrity". Those propositions form the basis for all operational, staffing, budget and resource decisions across CBP.

Focus Point	Program/Initiative	Lead Identity	Description
	Trust Betrayed Website	OIA/IOD	The CBPnet Trust Betrayed webpage features employees who have been convicted
	Integrity Toolkit Training	OFO	Integrity Toolkit training is provided to all OFO employees at the two, five, and ten-year career marks.
	Just in Time Training	HRM/LER	Just in Time training is provided upon request by LER specialists to new
	Annual VLC Integrity Awareness Training	OIA/IPD	This online training fulfills the mandatory annual certification requirement for integrity issues that is delivered via the CBP Virtual Learning Center (VLC).
Prevention	"Think Before You Act" Off-duty Arrest Initiatives	HRM	The "Think Before You Act" initiative disseminates recurring integrity-related messages from the Assistant Commissioner, HRM. The messages are disseminated via email and local musters. These messages address the obligation to report corruption, arrests, and other related misconduct. Initial initiative began with information and resources related to alcohol and impaired driving including EAP guidance, red asphalt videos, and goggles which simulate driving under the
	Disciplinary Penalties (Doesn't go here)	HRM/LER	Disciplinary penalties – adverse actions and disciplinary actions – are imposed to correct behavior and teach the subject and others that certain actions are unacceptable for CBP employees. The Table of Offenses and Penalties serves as a
Detection	Random Drug Testing	HRM/BMWL	Random drug testing is conducted on ten percent of the incumbent CBP workforce per year.
	Proactive Research and Analysis Operational Teams	OIA/IPD	IPD teams conduct research, evaluation and analysis on employees, enforcement actions, and other strategic factors, such as post-seizure data, AMSCO identified
	Behavioral Research Branch	OIA/IPD	The Behavioral Research Branch is a multidisciplinary research unit that studies internal threats to the integrity of CBP at the individual, cultural, and organizational levels. The branch conducts research, evaluation, data mining, consultations, training, and information sharing. The disciplines represented

Focus Point	Program/Initiative	Lead Identity	Description
Monitoring	Operational Systems Analysis (AMSCO)	OFO/AMSCO (USBP Pilot Study)	[redacted] through analysis of OFO systems data using sophisticated IT tools. The systems track four behaviors: self-inquiry, override of 72 hour check point seizures, override of license plate readers, and TEXT record lookouts. Integrity issues are referred to OIA for further action.
	SOPs for Reporting Possible Corruption	USBP	The SOPs provide guidance for reporting suspicious activity or potential corruption.
	Amendments to CBP Standards of Conduct for Reporting Off-Duty Arrests	HRM/LER	The amendments provide increased specificity on reporting requirements.
	Periodic Reinvestigations	OIA/PSD	CBP employees are mandated to undergo periodic reinvestigations to certify the employee is suitable for continued employment with CBP. These investigations are initiated every five years.
	Misconduct Tracking and Analysis	OIA/IPD	[redacted] trends and patterns.
	OFO and USBP Post Corruption Analysis	USBP/Field Managers and OFO, IC/Field Managers	USPB and OFO post corruption analysis is a "Lessons Learned" field review of corruption cases following conviction.
	[redacted]	[redacted]	[redacted]
Investigative	Management Inquiry Team	USBP	These USBP teams conduct post corruption on mission critical corruption at the sector-level. The teams look for "red flags" for detecting corruption after an agent has been identified as engaging in corrupt activities.
	(Insider) Corruption Case Study	[redacted] Behavioral Research Branch	[redacted] employees who have misused/abused their position or authority for personal gain focused on identifying behavior that is indicative of corrupt activity.
	Employee Delinquency Study	OIA/IPD/ Behavioral Research Branch	The study tracks and analyzes incidents reported to the JIC in order to provide situational awareness on threats to the integrity of CBP employees. The study informs integrity messaging efforts and aids in the development of the awareness campaigns.

Focus Point	Program/Initiative	Lead Identity	Description
	Operation Side Door	OIA/IPD/ Proactive Research and Analysis Operational Teams	This initiative evaluates data and lead information from the Credibility Assessment Division (CAD) polygraph examinations where the applicant has admitted to significant involvement with drugs or aliens. Operation Side Door also studies [illegible]
	Operation Red Flag	OIA/IPD/ Proactive Research and Analysis Operational Teams	This analytic study evaluates data anomalies and lead information from AMSCO to determine if there is any misconduct.
	Operation Hometown	OIA/IPD/ Proactive Research and Analysis Operational Teams	This study evaluates the vulnerability of deploying CBO and Border Patrol personnel to their respective "hometowns." Where applicable, team generates IPD cases for further investigation by DHS-OIG, ICE-OPR and/or CBP OIA Investigations/Operations Division.
Investigative	Operation Southern Exposure	OIA/IPD/ Proactive Research and Analysis Operational Teams	This study evaluates the post-seizure data derived from the Office of Intelligence and Operations Coordination and state and local law enforcement.
	Misconduct and Corruption Investigations	DHS OIG, ICE OPR, OIA IOD	Investigations conducted to determine if an employee has engaged in criminal activity.
	Criminal Analysis and Investigative Support	OIA/IPD	Research and analysis conducted in support of pre-employment screening and CBP employees who are under investigation by DHS-OIG, ICE-OPR, and/or CBP-OIA.
	Investigative Polygraph Examination	OIA/CAD	Polygraph examinations conducted in support of misconduct and/or corruption investigation of CBP employees.

APPENDIX D: HILLARD HEINTZE PROFILES

Hillard Heintze believes that immediate access to trusted counsel, critical insights, and the full scope of information vital to strategic decision making is absolutely essential. As a key component of the firm, the Hillard Heintze Senior Leadership Council is an independent panel of retired major city police chiefs and senior federal, state and local law enforcement leaders. Comprised of select senior law enforcement executives with outstanding career-long records of leadership and achievement, the council is dedicated to bringing national and international best practices to the pursuit of excellence in policing and public safety. It supports the ability of mayors, police chiefs, sheriffs, city managers, council members and regulators in government agencies, as well as their executive decision-making teams worldwide, to identify, evaluate, prioritize and implement opportunities to enhance and improve policing and public safety. Key focus areas include command, control and communications; recruitment and training; information sharing and intelligence; collaboration and public/private partnerships; use of technology; and ethics, workforce integrity and public trust.

Six members of the Hillard Heintze team, including the Senior Leadership Council, contributed directly to the analysis, assessment and research at the core of this study. These individuals are:

Robert Davis – As a 30-year veteran of the San Jose, California Police Department (SJPD), Davis rose from patrol officer to Chief of Police of the tenth-largest city in the nation (2004-2010) as a result of factors such as his progressive use of technology, sensitivity to the diversity of the citizens under his protection, and internationally lauded model of gang prevention, intervention and suppression. Davis oversaw what has historically been the lowest-staffed police department of any major city in the country – with only 1.2 sworn officers per 1,000 residents (the national average is approximately 2.6 officers per 1,000 residents). According to the FBI, San Jose is routinely ranked one of the safest "big cities" in America. This distinction is even more remarkable given that the Department received this accolade amid seven straight years of budget cuts while fighting crime in a city that adds 15,000 to 20,000 new residents every year. Davis has earned international recognition as an expert in addressing gangs and gang violence, having served as a consultant for the U.S. State Department on five separate occasions. Davis is a former President of the Major Cities Chiefs Association.

Thomas Streicher – As the former Chief of the Cincinnati Police Department, a position he held for over ten years, Streicher earned the Department both local and national recognition for his leadership and accomplishments. With Streicher at the helm, the Department has been awarded a number of distinctions, such as the ACLU Leadership Award (2000), the International Association of Chiefs of Police (IACP) Weber Seavey Award (2008) and the IACP West Award for Investigative Excellent (2009). During this period, Cincinnati was also recognized by the United States Department of Justice for successfully meeting the requirements of a Memorandum of Agreement designed to improve aspects of policing including, but not limited to use of force procedures, use of canines, procedures dictating citizen complaint processing, training, inspection and police-community relations. Additionally, the Cincinnati Police Department has been recognized for successfully completing the historic Collaborative Agreement, under the auspices of the United States Court for the Southern District of Ohio, in what former

United States Attorney General John Ashcroft termed a historic agreement, which has never before been attempted by any law enforcement agency in the United States.

Matthew W. Doherty – Widely recognized across the United States as among the most experienced senior experts in assessing an individual's potential for danger and preventing targeted violence against our nation's leaders and national critical infrastructure as well as major events and the corporate workplace, Doherty has managed training on threat assessment and targeted violence prevention for over 70,000 federal, state and local law enforcement personnel. He created the first information-sharing database (TAVISS) for the prevention of violence against protected officials, including the U.S. President, Vice-President, cabinet secretaries and governors. He developed and supervised numerous research projects on targeted violence including the Secret Service partnerships with Carnegie Mellon University for the Insider Threat Study (ITS) and with Harvard University and the Department Education for the Bystander Study. Frequently called on to testify as an expert before Congress, Doherty has also routinely briefed Justice Department officials and members of Congress on threat assessment methodologies. Featured in numerous magazines, newspapers and television news media for major articles on insider threats, assassinations and school shootings, Doherty also serves on two Advisory Boards: the U.S. Marshal Service Judicial Threats Center and the U.S. Capitol Police Threat Assessment Section.

Kenneth A. Bouche – Over nearly two decades, Bouche has established a career as an executive leader and senior advisor at the forefront of applying best practices in technology, information sharing and intelligence to the highly specialized needs of law enforcement, homeland security, justice, emergency preparedness and crisis response. In addition to his executive responsibilities, Bouche leads the firm's focus in two areas: (1) helping government clients (justice and homeland security decision-makers) understand and embrace strategic information-sharing opportunities to advance their missions of understanding trends, preventing crime and terrorism, and catching criminals, and (2) helping the firm's commercial clients and partners align their value offerings and service delivery with the needs of specific public sector organizations. From 2001 to 2006, Bouche was the chairman of the Global Justice Information Sharing Initiative. In this capacity, he served as a national leader in improving America's information-sharing capacity and implementing post 9/11 intelligence reforms.

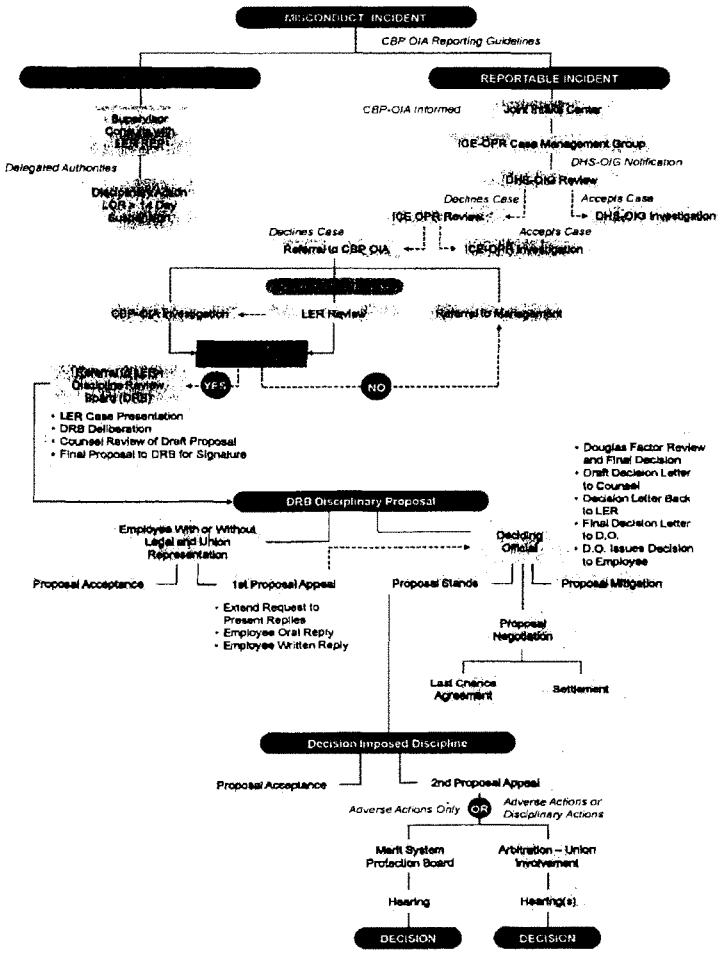
Terry G. Hillard – Until 2003, as Chicago Police Superintendent, Terry Hillard led 13,500 officers in protecting one of the country's largest metropolitan centers. Hillard is nationally regarded for his results-driven leadership as well as his intensely personal commitment to individuals. At the helm of the Chicago Police Department, he created one of the most collaborative cultures in the history of law enforcement. During his tenure as the head of the nation's second largest police department, he initiated innovative, community-sponsored crime-prevention programs to protect and serve the citizens of Chicago – programs that today still help define national standards in community-based policing. Hillard earned the CPD's highest rank and distinction the old-fashioned way: one step at a time – evolving first from a Patrol Officer to a Gang Crimes Specialist and member of the mayoral Executive Security Detail and later to Intelligence Division Sergeant, District Commander, Chief of Detectives, Coordinator of the Chicago Terrorist Task Force and Lieutenant in Gang Crimes and Narcotics Sections. In fact, the programs and initiatives of his administration transformed the CPD into a best practice-setting, 21st Century law enforcement agency – with changes that spanned

critical law enforcement domains such as technology, information exchange, community policing and police accountability.

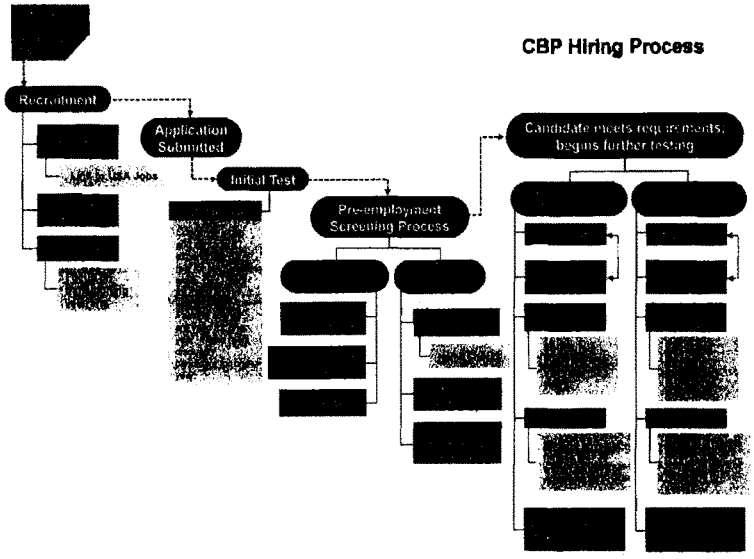
Arnette F. Heintze – Based on nearly three decades of experience working at the highest levels of Federal, state and local law enforcement, Arnette Heintze has an exceptionally strategic perspective on security. As the U.S. Secret Service Special Agent in Charge in Chicago, Heintze planned, designed and implemented successful security strategies for U.S. presidents, world leaders, events of national significance and the nation's most critically sensitive assets. Earlier in his distinguished public service career, Heintze served with the Louisiana State Police, Louisiana Attorney General's Office, and the Baton Rouge City Police. In 1990, Heintze was part of the Presidential Protective Division, where he served for more than four years on the permanent detail protecting President and Mrs. Bush and President and Mrs. Clinton. In Washington D.C., Heintze also coordinated the 160 foreign embassies in the city and acted as the Secret Service spokesperson and agent in charge of the Public Affairs Office, where he led the crisis communications team during some of the nation's most trying times. In 1998, Heintze was accorded the honor of being chosen as the Treasury Department's representative to attend the National War College's elite program for select military officers and ranking federal civilians, where he earned a Master of Science degree in national security strategy. In 2000, Heintze's strategic leadership qualifications led to his appointment as a member of the Senior Executive Service and his selection as the Special Agent in Charge of the Chicago field office.

APPENDIX E. CBP DISCIPLINARY FLOW CHART

CBP Disciplinary Flow Diagram



APPENDIX F. RECRUITING AND VETTING FLOW DIAGRAM



APPENDIX G. CBP TRAINING MATERIALS REVIEWED AND NEXT-STEP RECOMMENDATIONS

Training Materials Reviewed and Considered in the Study

As noted at the start of section III, OTD provided courseware on CBP's training on workforce integrity/ethics/code of conduct. The Hillard Heintze SLC training subject matter experts (SMEs) reviewed the material—specifically, the following:

1. Overview of the Border Patrol Academy's Integrity/Ethics/Code of Conduct Training, as prepared by Mark Brazill, Training Operations Specialist, dated April 27, 2011
2. Overview of the Advance Training Center's Integrity/Ethics/Code of Conduct Training, as prepared by Todd Fraser, Course Developer/Instructor, dated May 2, 2011
3. Overview of the Field Operations Academy's Integrity/Ethics/Code of Conduct Training, as prepared by Joseph E. Trevathan, Branch Chief, dated May 31, 2011
4. Overview of the Training Production and Standards Division's Integrity Plus IPCC, as prepared by Susan Farrell, Instructional Systems Specialist, dated May 31, 2011
5. Instructor's Guide for the Second-Level Command Preparation Course on Ethical Decision Making (Lesson Four: Ethical Decision Making), dated September 2011

The findings and recommendations from the review of these materials are in section III of the report.

Recommendations for Next Steps

While a more in-depth review of training issues would help determine what additional measures should be taken, the following are some of the steps that could be taken to assist in this effort:

- Conduct face-to-face interviews with CBP training instructors who actually deliver the ethics training at one or more of CBP's training academies or supervisors' courses. Of specific interest would be the trainers' take on how effective the training is, what constraints there are in presenting the course material, how much interaction and coordination exists between them and other CBP training groups in terms of training design and delivery, what kinds of question they field from trainees, and a review of the trainees' post-course evaluations on the effectiveness of the training. Such information would serve not only to inform the trainers about what could be improved in their sessions, but could also serve to inform CBP management about what steps they may need

to take to provide the training groups with specific CBP-wide expectations regarding "bright line" behavior expectations.

- Conduct interviews with members of the CBP Office of Internal Affairs and the DHS Office of the Inspector General's to determine what they would like CBP-wide training to cover in their ethics courses. Focus particularly on determining exactly what proactive steps could be taken by first-line employees and their supervisors to address corruption.

- Conduct interviews with some field office and sector managers to determine what they see lacking in the performance of their supervisors that could be addressed through training that emphasizes the practical application of anti-corruption efforts.

- Conduct interviews with both senior and new supervisors to determine what they feel may be needed in terms of providing them with the training necessary to be part of a CBP-wide effort to address corruption. This learning-needs assessment could go a long way not only to enhance the quality of the training they receive, but also to boost their morale when they recognize that CBP management is very interested in including them in the organization-wide effort to combat corruption within their ranks.

- Attend a presentation of at least one of CBP's courses on ethics to determine whether the training is in sync with the lesson plans, as well as to observe the effectiveness of the course material and delivery. Emphasis on such reviews should be placed upon the basic academy courses and the supervisors' ethics training sessions, if possible, as these would seem to hold the most opportunity to provide a positive impact for CBP.

- Review some of the written evaluations that trainees may have completed at the end of a CBP course on ethics. Also get access to the student critiques of all ethics instruction courses to include the DHS OIG courses.

- Make written recommendations to CBP, based on the results of the reviews noted above, about what additional or alternative material or learning methodologies could be incorporated into CBP's ethics training that addresses the current needs of CBP. Specifically, the focus should be on the proactive steps CBP is taking to address corruption issues.

- Consider conducting the same type of reviews as outlined above for the courses that address training CBP's Internal Affairs and the Integrity Programs Division personnel on how to do their jobs more effectively. Review whether the training focuses on how they can perform their duties more effectively in an environment that requires a great deal of interaction, communication, and cooperation with other government agencies and a host of different field offices.

- Meet with some managers at an organizational level identified by CBP management and determine what characteristics and qualities the ideal supervisor possesses who successfully prevents or handles ethical dilemmas and corruption

issues in the field. Using this information, tailor specific checklists that emphasize these characteristics and qualities for consideration in incorporating them in the ethics training for CBP supervisors.

- Coordinate these reviews and recommendations with the efforts of others working the CBP Vulnerability Analysis. Determine what recommendations could be made to CBP management to enhance their ability to speak with one voice to all of their employees in the effort to combat corruption.

APPENDIX H. CBP STATEMENT OF POLICY AND INTENT: INTEGRITY

U.S. Department of Homeland Security
Washington, DC 20229

U.S. Customs and
Border Protection

Commissioner

[SPI-11-OA]

CBP Statement of Policy and Intent: Integrity

End State:

- Our **workforce** is strengthened when every member of the team can be counted on to perform according to the highest standards of integrity. From the most junior member of the organization to the Commissioner, there is only one standard for integrity: the CBP standard as set forth herein. It is absolute. We do not compromise our oath. We do not lie. We do not cheat. We do not steal. We are accountable to the nation and to one another.
- Each member of our **workforce** is accountable for his or her choices and actions. Employees who violate the public trust for personal gain or other personal motives in individual cases pose as much of a threat to the integrity of CBP as employees who choose to assist adversaries seeking to compromise the workforce in a systematic manner.
- Our **adversaries** must be deterred by the belief and absolute knowledge that our borders, ports of entry and overseas operations are secured by a workforce of the utmost integrity.
- Our **nation** must feel a profound sense of confidence and trust that its borders are protected by the finest and best-trained of its citizens who possess the utmost integrity. Their confidence and trust are sacred charges. We shall never betray that trust.

Foundation:

As U.S. Customs and Border Protection fulfills its potential and moves from a great agency to a greater agency, corruption of the CBP workforce is a dagger pointed at the heart of our organization. Absolute integrity is the keystone of our obligation to protect the United States and the American people.

As Federal civil servants, we take a solemn oath of office by which we swear to support and defend the Constitution of the United States of America, and to faithfully discharge our duties. The very first law passed by the very first Congress implemented Article VI of the Constitution by setting out this simple oath in law for members of Congress: "I ... do solemnly swear or affirm (as the case may be) that I will support the Constitution of the United States." 1 Stat. 23 (1789). This commitment continues to be reflected in statute, regulation and policy, including the basic obligation of ethical service set forth in federal regulations at 5 C.F.R. § 2365.101. Trust and integrity are at the very foundation of our government, and what sets our nation apart.

Integrity-CBP Statement of Policy and Intent
Page 2

Failure to continuously and proactively detect and eliminate corruption at the earliest possible opportunity and to our greatest ability poses a grave risk to homeland security by providing transnational and other criminal organizations with the ability to circumvent CBP enforcement efforts at and between ports of entry. Our adversaries will seek to exploit individual, operational, organizational, and leadership vulnerabilities as a tool to undermine the significant enhancements in personnel, technology and infrastructure effected by CBP in recent years and planned for the future. The corruption of any employee – including those in administrative, professional and technical positions – harms the organization and threatens the ability of CBP to fulfill its mission.

CBP's commitment to integrity, however, goes further than the need to address this threat. It is a way of life and commitment as an organization that begins at the time of application for employment with CBP and continues throughout an employee's career. It defines our relationship with our adversaries, one another and those we serve in this nation. It is essential to the morale and well-being of the workforce and to securing and retaining the trust of the American people. Integrity, as that principle is articulated in this intent statement, applies with equal force to all of our personnel. Corruption in all of its forms, including but not limited to theft, fraud, bribery and misuse of government systems, is antithetical to the CBP mission and the values of our organization.

CBP is transitioning from a period of historic growth in its workforce and the integration of multiple legacy components to a single, full operational capability. CBP's size, geographic, and mission diversity, non-stop border and port operations, and high-threat environment are unique in law enforcement. We are aware of the fact that we will continue to be targeted for corruption, and will be relentless in our efforts to combat this threat.
Reinforcing the culture of a highly ethical and incorruptible workforce and taking swift, unyielding action in response to acts of corruption are among our highest priorities. It is the predicate for all of our other initiatives. CBP's leaders, beginning with the Commissioner, are responsible for creating and maintaining an organization in which all employees have the strength of character and support to reject all attempts at corruption, in whatever form these may take. This mindset begins with entry into the CBP workforce and continues throughout the careers of our officers, agents and mission-support personnel.

The following propositions shall form the basis for all operational, staffing, budget and resource decisions across CBP:

Principles of Policy

1. The enforcement of CBP's integrity standards is core to our mission and shall be designed, prioritized and implemented as such. CBP is responsible for border security and the facilitation of trade, and we shall cooperate with our law enforcement partners to ensure the integrity of the CBP workforce to achieve this end.
2. Upon receipt of credible information indicating that an employee is engaged in corruption, appropriate and timely administrative action should be taken to neutralize any threat to CBP's mission. Appropriate action can include placement of the employee on limited administrative leave or administrative duties, indefinite

Integrity-CBP Statement of Policy and Intent
Page 3

suspension, reassignment, withdrawal of law enforcement duties and—in those cases when misconduct can be proven by a preponderance of the evidence—suspension or removal.

3. This default rule should apply unless a decision is made by CBP leadership in combination with CBP's law enforcement partners to allow a criminal investigation to proceed that is likely to result in a conviction and/or further indictments of co-conspirators, while continuing to take all necessary steps to maintain officer and public safety as well as border security. This default in favor of prompt administrative action will be implemented and deconflicted in a manner that does not compromise existing criminal investigations but shall be implemented aggressively and consistently. CBP will continue to make every effort to support information-sharing and joint task force law enforcement with investigative agencies within DHS and the federal government in support of this policy.
4. To the maximum extent possible, operational information and intelligence should support integrity efforts, and the results of integrity analysis, testing and operations should be used to support CBP operational efforts.
5. Integrity testing and training should commence during recruitment at our academies and continue throughout an employee's career.
   a. CBP should utilize the maximum extent of its authority to require testing, including polygraph examination, of officer and agent applicants prior to entering on duty as law enforcement officers.
   b. Polygraph testing, background investigations and other pre-employment screening should be sequenced in a manner that maximizes the efficiency of application and integrity assurance processes.
   c. Adverse results of pre-employment screening should be shared to the maximum extent possible with investigative agencies in order to support the overall border law enforcement efforts of the United States government.
   d. CBP should maintain an active program for assessing employee integrity throughout an employee's career, including through the effective use of workload monitoring programs and planned integrity testing.
6. CBP shall ensure that integrity programs complement employee wellness and support programs, and are understood as part of a continuum of employee well being.

By the authority vested in me as Commissioner of U.S. Customs and Border Protection, I direct the foregoing policy and intent regarding integrity be communicated to the workforce through the leadership of CBP and implemented forthwith.

Signature _____ **Date** 3/28/2011

MEMORANDUM OF UNDERSTANDING
BETWEEN
THE UNITED STATES SECRET SERVICE
AND THE OFFICE OF THE INSPECTOR GENERAL
DEPARTMENT OF HOMELAND SECURITY

The United States Secret Service (USSS), an organizational component of the Department of Homeland Security (DHS), operates within the Department under the authority and responsibilities enumerated in Title VIII, Subtitle C of the Homeland Security Act of 2002, as amended (the Act), and includes those responsibilities described generally in Section 1512 of the Act, as well as in various delegations of authority issued by the Secretary of DHS (the Secretary). The agency's dual statutory missions of protection and criminal investigations are more fully enumerated at Title 18, United States Codes, Section 3056 (Section 3056), and Title 3, United States Code, Section 202 (Section 202), and various other statutes.

The Office of the Inspector General (OIG), an organizational component of DHS, operates within the Department under the authority and responsibilities enumerated in Title VIII, Subtitle B of the Act, as amended, and the Inspector General Act of 1978, as amended, and includes authority and responsibility acquired pursuant to Section 1512 of the Act.

To prevent duplication of effort and ensure the most effective, efficient and appropriate use of resources, the Secret Service and the OIG enter into this Memorandum of Understanding.

The categories of misconduct listed below shall be referred to the OIG. Such referrals shall be transmitted by the USSS Office of Inspection immediately upon the receipt of adequate information or allegations by the USSS Office of Inspection to reasonably conclude that misconduct may have occurred, and no investigation shall be conducted by the USSS Office of Inspection prior to the referral. In cases involving exigent circumstances, if the OIG decides to investigate the allegation but is unable to do so immediately, the USSS Office of Inspection will conduct the investigation until the OIG is able to take it over. In cases not involving exigent circumstances, the OIG will determine within one business day of the referral whether to investigate the allegation itself or to refer the matter back to the USSS Office of Inspection for investigation. If no determination is communicated to the USSS Office of Inspection within one business day of the referral, the USSS Office of Inspection may initiate the investigation. The acceptance of a referral by the OIG reflects a determination that available investigative resources will be able to conclude the referred investigation within a reasonable time. This will afford the agency a reasonable opportunity to act expeditiously, if necessary, regarding the allegations.

- All allegations of criminal misconduct against a USSS employee;
- All allegations of misconduct against employees at the GS-15, GM-15 level or higher, or against employees in the USSS Office of Inspection;
- All allegations regarding misuse or improper discharge of a firearm (other than accidental discharge during training, qualifying or practice);

- All allegations of fraud by contractors, grantees or other individuals or entities receiving Department funds or otherwise engaged in the operation of Department programs or operations.

In addition, the IG will investigate allegations against individuals or entities who do not fit into the categories identified above if the allegations reflect systemic violations, such as abuses of civil rights, civil liberties, or racial and ethnic profiling; serious management problems within the Department, or otherwise represent a serious danger to public health and safety.

With regard to categories of misconduct not specified above, the USSS Office of Inspection should initiate investigation upon receipt of the allegation, and shall notify within five business days the OIG's Office of Investigations of such allegation. The OIG shall notify the USSS Office of Inspection if the OIG intends to assume control or become involved in an investigation, but absent such notification, the USSS Office of Inspection shall maintain full responsibility for these investigations.

Pursuant to Section 811(a) of the Act, OIG audits, investigations, and subpoenas which, in the Secretary's judgment, constitute a serious threat to the protection of any person or property afforded protection pursuant to Section 3056 or Section 202, or any provision of the Presidential Protection Assistance Act of 1976, may be prohibited. Accordingly, to assure proper and timely responses to OIG requests for information or records, all OIG plans for audits involving the Secret Service shall be communicated via entrance letter by the OIG either directly to the USSS Office of Inspection or to the Office of the Deputy Director; any OIG investigation shall be communicated orally or via e-mail to the same entities. Any Secret Service Headquarters' concern under section 811(a) regarding the scope or direction of a planned audit or investigation will be raised and resolved expeditiously with OIG officials, or immediately communicated to the Secretary in the absence of resolution.

The USSS Office of Inspection shall provide a monthly report to the OIG on all open investigations. In addition, the USSS Office of Inspection, upon request, shall provide the OIG with a complete copy of the Report of Investigation, including all exhibits, at the completion of the investigation. Similarly, the OIG shall provide the USSS Office of Inspection, upon request, with a complete copy of any Report of Investigation relating to the Secret Service, including all exhibits, at the completion of the investigation. The OIG shall have the right to request more frequent or detailed reports on any investigations and to reassert at any time exclusive authority or other involvement over any matter within its jurisdiction.

This MOU shall be effective upon the signature of both parties and shall remain in effect until revoked by one party upon thirty day's written notice to the other.

W. Ralph Basham
Director of the United States
Secret Service

Dated: 12/5/03

Acting Inspector General

Dated: 12/8/03

U.S. Citizenship and Immigration Services I-765 Application for Employment Authorization Approvals by Class Preference Fiscal Years: 2007-2011			
FORM NUMBER	FISCAL YEAR	CLASS PREFERENCE	APPROVALS
I-765	2007		
		(blank)	2
		A02	1,312
		A03	36,341
		A04	351
		A05	71,577
		A06	777
		A07	14
		A08	297
		A09	2,533
		A10	6,759
		A11	38
		A12	250,667
		A13	426
		A14	65
		A15	4,174
		A16	601
		A17	5,995
		A18	15,819
		A19	1
		C01	1,817
		C011	6
		C02	58
		C031	80,626
		C032	83
		C033	2,023
		C034	4
		C03B	1
		C04	1,752
		C05	8,524
		C06	306
		C07	359
		C08	82,390
		C09	587,272
		C091	15
		C10	18,331
		C11	35,006
		C12	11
		C13	2
		C14	17,062

		C16	33
		C171	444
		C172	396
		C173	3
		C18	6,946
		C19	4,862
		C20	691
		C21	141
		C22	15,569
		C24	4,507
		C25	342
		C29	2
		C30	1
		C31	920
		D	1
		NONE	786
2007 Total			**1,269,041**
I-765	**2008**		
		(blank)	4
		A02	559
		A03	63,600
		A04	672
		A05	43,262
		A06	381
		A07	13
		A08	251
		A09	1,413
		A10	9,773
		A11	360
		A12	224,996
		A13	82
		A14	9
		A15	1,831
		A16	503
		A17	5,918
		A18	16,509
		A19	63
		A20	12
		C01	1,764
		C011	42
		C02	51
		C031	53,973
		C032	89
		C033	1,414
		C034	4
		C03A	1,332

		C03B	26,291
		C03C	927
		C04	2,071
		C05	7,755
		C06	227
		C07	345
		C08	63,973
		C09	715,970
		C091	5
		C10	17,501
		C11	29,326
		C12	8
		C13	1
		C14	18,145
		C16	32
		C16P	1
		C171	376
		C172	314
		C173	5
		C18	9,739
		C19	1,317
		C20	421
		C21	185
		C22	5,243
		C24	2,105
		C25	433
		C31	670
		NONE	1,012
2008 Total			**1,333,278**
I-765	**2009**		
		A02	377
		A03	79,280
		A04	1,024
		A05	52,383
		A06	562
		A07	35
		A08	482
		A09	1,058
		A10	10,026
		A11	1,270
		A12	288,958
		A13	65
		A14	14
		A15	1,834
		A16	333
		A17	6,222

		A18	16,300
		A19	6,033
		A20	797
		C01	2,077
		C011	28
		C02	51
		C031	326
		C032	60
		C033	1,397
		C034	1
		C03A	3,370
		C03B	81,868
		C03C	5,902
		C04	2,106
		C041	1
		C05	8,425
		C06	234
		C07	359
		C08	54,835
		C09	527,047
		C10	19,499
		C11	24,949
		C12	6
		C14	15,528
		C152	1
		C16	82
		C171	363
		C172	354
		C173	4
		C18	11,253
		C19	1,336
		C20	335
		C21	24
		C22	2,993
		C24	1,112
		C25	146
		C31	332
		C9	2
		MULT	2
		NONE	1,177
2009 Total			**1,234,645**
I-765	**2010**		
		(blank)	19
		A02	452
		A03	70,923
		A04	239

		A05	49,267
		A06	336
		A07	19
		A08	509
		A09	706
		A10	11,823
		A11	2,158
		A12	199,686
		A13	43
		A14	8
		A15	1,257
		A16	485
		A17	5,074
		A18	13,691
		A19	10,296
		A20	5,524
		C01	1,688
		C011	25
		C012	2
		C02	32
		C031	95
		C032	59
		C033	1,261
		C03A	3,067
		C03B	83,624
		C03C	10,423
		C04	2,085
		C05	7,068
		C06	220
		C07	303
		C08	47,944
		C09	429,142
		C091	11
		C09P	1
		C10	27,613
		C11	23,972
		C12	6
		C13	2
		C14	12,022
		C16	20
		C171	372
		C172	308
		C173	3
		C18	14,068
		C19	43,345
		C20	220
		C21	14

		C22	823
		C24	448
		C25	272
		C31	490
		C9	1
		NONE	767
2010 Total			**1,084,331**
I-765	**2011**		
		(blank)	103
		A02	351
		A03	56,772
		A04	158
		A05	37,691
		A06	134
		A07	22
		A08	410
		A09	192
		A10	12,455
		A11	465
		A12	113,060
		A13	58
		A14	1
		A15	1,445
		A16	585
		A17	5,306
		A18	17,482
		A19	10,389
		A20	6,993
		C01	1,929
		C011	11
		C02	35
		C03	1
		C031	50
		C032	30
		C033	1,456
		C034	3
		C03A	3,143
		C03B	89,237
		C03C	13,179
		C04	2,080
		C05	7,141
		C06	165
		C07	371
		C08	47,215
		C09	362,599
		C091	11

		C09P	72,678
		C10	41,476
		C11	27,108
		C12	4
		C13	1
		C14	8,690
		C16	23
		C171	345
		C172	297
		C173	2
		C18	18,064
		C19	7,482
		C20	177
		C21	38
		C22	684
		C24	155
		C25	395
		C31	746
		C32	1
		C9	3
		NONE	323
2011 Total			**971,420**

Report Created: May 7, 2012, Updated May 10, 2012
System: CIS Consolidated Operational Repository (CISCOR) - DARB I-765 Receipts/Completions Database
By: Office of Performance and Quality (OPQ), Data Analysis and Reporting Branch (DARB), AC, Update NP
Parameter
Date: FY2007 - FY2011
Form Type(s): I-765
Class Pref: All
Location: All
Data Type: I-765 Approvals by Class Preference

SUBMISSIONS FOR THE RECORD

U.S. Senator Chuck Grassley • Iowa

Ranking Member • Senate Judiciary Committee

http://grassley.senate.gov

Prepared Statement of Ranking Member Grassley of Iowa
U.S. Senate Committee on the Judiciary
Hearing on "Oversight of the Department of Homeland Security"
April 25, 2012

Mr. Chairman, oversight is a critical function and a constitutional responsibility of the legislative branch. Hearings like this one are an avenue for Congress to raise questions, concerns, and suggestions for improving government functions. This hearing should also be an avenue for us to evaluate how the Department of Homeland Security (DHS) carries out its mission. It should also be an opportunity for the Department to take responsibility for its actions and policies.

Before I begin to discuss the issues that pertain to this committee, I would like to voice frustration at the non-responsive letters I have received from DHS. In fact, 99% of the time, when I write to the Secretary, I don't get a response directly from her. The responses come from the Office of Legislative Affairs. But more frustrating is that my questions are rarely, if ever answered. Unbelievably, the Secretary just responded to questions we posed at the last Judiciary Committee oversight hearing, which took place in October of last year. I hope the Secretary will respect the oversight role that some of us in Congress take seriously. The Department needs to be held accountable to Congress and to the American people, and it should be forthcoming so we can take steps to ensure the government is acting appropriately in carrying out our laws.

U.S. SECRET SERVICE INVESTIGATION

We continue to learn more each day about the ongoing investigation into agents of the U.S. Secret Service who were removed from Colombia following allegations that they had foreign national prostitutes in their rooms. While I commend Director Sullivan for immediately removing these agents from Colombia and for initiating an investigation into this matter, more work remains. For example, the Inspector General for the Department of Homeland Security needs to be involved to make this investigation impartial and credible. The Secret Service has a long and distinguished history. This entire incident is a black eye for an agency full of hard working and dedicated agents and officers. This matter needs to be resolved soon given the serious national security issues associated with this alleged conduct.

At the beginning of his administration, President Obama released a memorandum entitled "Transparency and Open Government" and stated, "My administration is committed to creating an unprecedented level of openness in government." We have seen time and again that this administration has contradicted that goal set by President Obama. However, it's my hope that the White House will provide details to Congress about the internal review that took place last weekend with regard to the Secret Service and White House Office of Advance.

According to the White House spokesman, that investigation was conducted by the White House Counsel's Office, despite the fact that on Friday the White House apparently didn't see the need to look into this further. This raises a lot of questions about how deep an inquiry was conducted, especially given it was completed in just two days. I want to know if the investigation involved pulling any hotel records in Colombia or whether we are to simply take the White House at their word. This is not a fishing expedition; it is a logical extension of the Secret Service investigation. Given the serious national security concerns that any vulnerability in the President's protection could come from having unauthorized guests, we need to get to the bottom of this and the White House should cooperate immediately. I look forward to hearing from the Secretary about her views on this matter and what steps she has taken to help the Director and Inspector General get to the bottom of this matter.

IMMIGRATION

Today's hearing is an opportunity to assess this administration's immigration policies, and to raise questions about whether these policies are consistent with the laws on the books. I have serious concerns not only about policies put forth by the Department, but also the manner in which such policies have been rolled out.

The President announced a new campaign slogan called "We Can't Wait" to justify why his administration continues to circumvent Congress and the democratic process. The administration continues to put out memos and directives that have not gone through the rule-making process. I got my first glimpse into this campaign when I uncovered the memo titled, "Administrative Alternatives to Comprehensive Immigration Reform." For years, the administration has been intent to act unilaterally, and in doing so, they have disregarded the rule of law.

Let's consider the President's immigration policies in the last two years alone.

In a departmental memo last March, ICE Director John Morton outlined new enforcement priorities and encouraged the use of "prosecutorial discretion" for illegal aliens who did not meet these priorities. The memo prescribed guidelines for limiting the detention of certain illegal aliens. Then, in a memo sent out in June of 2011, Director Morton discouraged ICE agents from enforcing immigration laws against certain segments of the illegal alien population, including aliens who essentially qualify for the DREAM Act.

Last August, Secretary Napolitano announced a case-by-case review of all aliens currently in or who will be entering deportation proceedings in order to determine who will be granted administrative amnesty. The Secretary claimed that this process would allow the government to direct resources at higher priority cases. This so-called "pilot" program has been carried out in Baltimore and Denver, and will expand to seven additional immigration courts.

This year, U.S. Citizenship and Immigration Service unveiled a new policy allowing certain aliens to bypass the statutory 3 and 10 year bars on inadmissibility. Generally speaking, the 3 and 10-year bars were created to deter illegal immigration and marriage fraud. Yet, the

administration wants to ignore the law that Congress passed in this regard, and provide waivers for an untold number of people who would normally be subject to the bars.

In January, the President issued an Executive Order to increase tourism to the United States, which would allow visa applicants to undergo less scrutiny by consular officers. Prior to September 11, 2001, consular officers were allowed to waive an interview for a visa applicant seeking entry into the United States. Sadly, only two of the nineteen hijackers had been personally interviewed by the U.S. Government to get their visa. As a result of 9/11, Congress established that all visa applicants be required to go through the interview process, with limited exceptions. The tourism initiative announced by the President would allow officers to waive in-person interviews for individuals reapplying for temporary admission to the United States. The law was written to specifically limit any exceptions to the in-person interview. Once again, the Administration is blatantly ignoring the safeguards that Congress put in place to prevent another terrorist attack.

In addition to implementing several initiatives that disregard the rule of law, the Administration has taken an inconsistent position on state and local governments that enact their own immigration laws and ordinances. The Administration has filed suit against Arizona, South Carolina, Utah, and Alabama. Moreover, in retaliation for Alabama's state law, the department halted the implementation of Secure Communities.

I find it frustrating that the Administration has challenged several states for passing laws that aim to protect their citizens while essentially turning a blind eye to jurisdictions that actively promote safe harbor policies. If the Administration truly believes immigration law is only to be enforced by the Federal government, as it has argued before several courts, it should adhere to that position and consider taking action against jurisdictions that actively thwart effective Federal enforcement of the laws.

Then there are policies that leave taxpayers footing the bill for benefits to people who are here unlawfully.

In February, ICE Director Morton announced that illegal immigrants residing in the country would have a lobbyist at headquarters to "serve as a point of contact for individuals, including those in immigration proceedings, NGOs, and other community and advocacy groups, who have concerns, questions, recommendations or important issues they would like to raise." The rationale behind this new position is not very clear, and I'd be interested in learning more from the Secretary about what this person does on a day-to-day basis.

Also in February, ICE announced changes to its detention standards, providing more accommodations and benefits to illegal aliens. For example, aliens will now receive physical education classes and internet access. And, taxpayers will help pay for costs associated with abortions and transgender hormone therapies. Also, taxpayers will be footing the bill for luxuries and services that are not afforded to other criminals.

I'd also like to hear from the Secretary about the state of the border. Americans have long been demanding that the federal government control its borders. Yet, the President announced last week that 900 of the 1,200 National Guard Troops at the Border will be sent

home. Taxpayers are left questioning the priorities of this President when illegal aliens get an advocate in Washington, and when resources from the border are diverted to plush detention facilities.

I also remain concerned about the "Get to Yes" philosophy that U.S. Citizenship and Immigration Service has espoused. In January, an Inspector General's report found that line officials at USCIS are pressured to approve applications by supervisors. The report says that a quarter of the immigration service officers interviewed felt pressure to approve questionable applications, and 90 percent of respondents felt they didn't have sufficient time to complete interviews of those who seek benefits, concluding that the speed at which these applications must be processed leaves ample room for error and leaves the U.S. open to national security dangers. I plan to ask the Secretary about this pressure, including information that has come to my attention about a particular case highlighted by the mainstream media. I want to know if adjudication decisions are being reversed after sympathetic news reports.

FREEDOM OF INFORMATION ACT (FOIA)

I also have concerns about how the Department is treating citizens who oppose the administration's policies. U.S. citizens who oppose the administration's policies should not be viewed or treated as "enemies." And they shouldn't become the subject of government monitoring because they oppose the administration's policies.

I am troubled by news reports that the Department is monitoring citizens who speak out against the Obama administration's policies and, in particular, its immigration policies. According to reports, a review of a 2011 reference guide for Homeland Security analysts reveals that DHS is tracking opponents. It appears that the DHS may be directing its analysts to identify and monitor media reports that reflect adversely on the DHS, and to track reports on the administration's policy changes in immigration, and the term "illegal immigration" in particular. This monitoring goes beyond reviewing news stories. It apparently includes monitoring social media, such as Twitter and Facebook.

I have to question why the Department is gathering this information on U.S. citizens. And I have to ask how far the information gathering goes and what the Department is doing with this information?

These reports renew my concerns about how the DHS treats requesters of information under the Freedom of Information Act (FOIA).

Perhaps the most dramatic and troubling departure from President Obama's vow to usher in "a new era of open government" was revealed in Homeland Security e-mails obtained by the *Associated Press* (AP) in July of 2010. According to the AP, in July 2009, in connection with requests under the FOIA, the Department introduced a directive requiring a wide range of information to be vetted by political appointees. Career employees were ordered to provide Secretary Napolitano's political staff with information about the people who asked for records and about the organizations where they worked. According to the AP, anything related to an Obama policy priority was pegged for this review. Also included was anything that touched on a controversial or sensitive subject that could attract media attention. Anything requested by

lawmakers, journalists, activist groups or watchdog organizations had to go to the political appointees.

Under the FOIA, people can request copies of records without specifying why they want them and are not obligated to provide personal information about themselves other than their name and an address where the records should be sent. Yet political appointees at the DHS researched the motives or affiliations of the requesters.

On March 30, 2011, the House Committee on Oversight and Government Reform released its 153-page report on its investigation of the Department's political vetting of FOIA requests. The Committee reviewed thousands of pages of internal DHS e-mails and memoranda and conducted six transcribed witness interviews. It learned through the course of an eight-month investigation that political staff under Secretary Napolitano had exerted pressure on FOIA compliance officers, and undermined the federal government's accountability to the American people.

The Department's political screening of FOIA requests is disturbing and I continue to have concerns about it, even though the Department maintains that it has stopped.

MANAGEMENT AT DHS

A serious, but often overlooked matter that we all should be concerned with is management of the federal government agencies we oversee. Management problems at the top of an agency can trickle down to problems in the field. As the buck should stop with the Secretary, I think it is worth noting that last month, for the sixth year in a row, DHS was awarded an abysmal score by the Partnership for Public Service's Best Place to Work. DHS ranked 31 out of 33 federal organizations. This included a four point drop from last year. DHS placed in the bottom three spots in almost every category evaluated, and placed dead last in "effective leadership." These are poor scores that indicate serious problems with management at DHS. Effective leadership starts at the top and I want to hear from Secretary Napolitano what she is doing to fix this leadership deficiency at DHS.

DHS ROLE IN ADDRESSING CYBERSECURITY:

Congress is currently debating legislation to enhance our national capability to protect and defend against cyber-attacks. There are a number of different proposals pending before the House and Senate that contain varying policy approaches. There are a number of areas of agreement across party lines on certain provisions, including information sharing, research and development, criminal law reforms, and updating the Federal Information Security Management Act (FISMA). However, the biggest point of contention remains whether to increase the size of the federal government by adding new regulatory powers for oversight of Cybersecurity to the mission of the DHS. I strongly oppose any expansion of DHS's power. The documented failures of the Chemical Facility Anti-Terrorism Standards (CFATS) should be a clear warning that the Department is simply not up to the task it was created to do.

In October 2006, President Bush signed the Department of Homeland Security Appropriations Act of 2007, which provides DHS the authority to regulate the security of high-risk chemical

facilities. To implement this authority, in 2007 DHS issued the Chemical Facility Anti-Terrorism Standards Interim Final Rule (CFATS Final Rule). These regulations required a number of regulated industries, including chemical manufacturers and distributors, to prepare site security plans (SSPs) to determine whether a facility would fall under DHS's regulatory authority. These SSPs were expensive and DHS estimated that compliance with the regulations could cost up to $5000 per site, just to complete the SSP. SSPs were then to be returned to DHS where a determination would be made as to what additional security would be ordered for a specific site.

Almost immediately after the regulations were issued, problems arose. For example, DHS's determination as to who qualified for a SSP under the regulations included any site with over 1,000 gallons of propane. Effectively, this would have required virtually every family farm or rural homestead with an individual use propane tank to complete a SSP as a chemical facility. While DHS ultimately corrected this anomaly, it merely highlighted problems to come.

More recently, it has been reported that despite this regulation, DHS has spent nearly $500 million in the last four years with nothing to show for it. In fact, DHS has yet to approve a single site security plan for the 4,200 entities that submitted one. Further, the CFATS computer program at DHS made significant errors in calculating risk at chemical plants in both 2009 and 2010, but the errors were not reported up the management chain and did not come to light until just last summer. Further, congressional investigators have started to review DHS's actions under CFATS to determine where nearly $480 million was spent given DHS has yet to approve a single SSP. Rand Beers, the Undersecretary in charge of the program, nevertheless claims that progress has been made despite the problems.

However, a crucial internal document written by DHS officials working for Undersecretary Beers tells a much different story. In a memorandum dated November 10, 2011, the Director and Deputy Director of the Infrastructure Security Compliance Division of the Office of Infrastructure Protection informed Beers of the total failure of their division in implementing CFATS. This document is perhaps the most critical internal review a government agency has ever written about itself.

For example, the document details how after four years DHS has yet to approve a single site security plan and is not even ready to conduct a compliance inspection. The memorandum states that the reasons for the failure include inadequate training, overreliance on external experts, poor hiring decisions including hiring those who do not have the necessary skills to perform the job, poor staff morale, management and leadership without experience in the field or knowledge of the subject-matter, lack of regulatory compliance experts, lack of transparency, ineffective communications, union problems, and a "catastrophic failure to ensure personal and professional accountability."

Most notably, the memorandum states, "It has become apparent that our inspector cadre lacks sufficient expertise to effectively evaluate chemical facility compliance with Risk Based Performance Standard (RBPS) 8, cyber security." Simply put, DHS's own internal review of the last major regulatory undertaking Congress authorized the agency to do has found that the agency cannot meet its mission. It highlights a bureaucracy so incompetent that it cannot make basic hiring and staffing decisions. This memorandum should be praised for its candor and those

who authored it should be commended. However, it shows a broken agency with failed leadership that needs to be reined in, lest the federal taxpayers provide another half-billion dollars and get nothing for it.

As if this internal review wasn't enough to signal how DHS is unable to take on the cybersecurity mission, the Government Accountability Office (GAO) issued a report in July 2008 titled, "Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability." This report found numerous challenges that DHS faced including: filling key management positions, identifying and acquiring technological tools to strengthen cyber analytical capabilities, expeditiously hiring sufficiently trained cyber analysts, engaging appropriate stakeholders in federal and nonfederal entities to develop trusted relationships, and ensuring distinct and transparent lines of authority and responsibility. Further, GAO found deficiencies in response by United States Computer Emergency Readiness Team (US-CERT); deficiencies in warning notifications that are targeted and actionable, deficiencies in analysis and ability to investigate incidents, and deficiencies in monitoring a comprehensive baseline understanding of the nation's critical information infrastructure. Nearly four years after the issuance of this report, all ten of GAO's recommendations to DHS remain open and unimplemented.

Taken together, the many failures of CFATS and the outstanding questions GAO highlighted lead me to question whether DHS could handle a new regulatory mission addressing cybersecurity. At the very least, DHS has a lot of house cleaning to do before Congress should even consider consolidating cybersecurity matters at DHS, let alone to create an entirely new regulatory bureaucracy covering both the public and private sectors.

FAST AND FURIOUS

Finally, I'd like to say something about my Fast and Furious investigation.

One year ago when we had an oversight hearing with the Secretary , I asked whether she realized that Immigration and Customs Enforcement (ICE) had an agent assigned to Fast and Furious. That ICE agent was involved enough in Fast and Furious that he was designated as a co-case agent for the operation. ICE kept a totally separate case file from ATF's, and the case file that was stored in ICE's system runs to 2,000 pages.

An ICE agent was there on May 29, 2010, when the main target of Operation Fast and Furious was stopped at the border trying to enter Mexico with 74 rounds of ammunition and an illegal alien. He was part of the interview where the target was caught lying to federal agents, then allowed to take his cargo into Mexico after simply agreeing to call a phone number the ATF agent wrote on a ten dollar bill. As far as we know, he didn't call. He wasn't arrested until seven months later, after the death of Border Patrol Agent Brian Terry.

Customs officers were also present for this May 29, 2010, incident. It's unclear what kind of pressure they felt from ATF to let this criminal go. No doubt they had no idea that guns he had trafficked would be found at the murder scene of their colleague, Agent Terry.

However, it's clear that Fast and Furious wasn't just a Justice Department problem. I have been told that law enforcement from many agencies realized something was fishy with ATF's "big case." I would like the Homeland Security Department's cooperation in getting to the bottom of this.

Thanks to the Secretary for appearing before us today. I look forward to hearing from Secretary Napolitano.

Opening Statement of Chairman Patrick Leahy
Oversight of the Department of Homeland Security
April 25, 2012
Senate Judiciary Committee

We welcome Secretary Napolitano back to the Judiciary Committee as we continue our important oversight of the Department of Homeland Security and the work that the women and men of the agencies within the Department do every day to keep Americans safe.

Much attention has been focused on an incident prior to President Obama's attendance at the recent Summit of the Americas in Cartagena, Colombia. I have spoken privately with Secret Service Director Sullivan since the incident and met with him yesterday. I know that he shares my view that the alleged conduct was unacceptable. He seems to be doing all that he can to ensure a timely and thorough investigation and accountability for behavior that failed to meet the standards he expects and that the President and the American people deserve.

Last week I arranged for a bipartisan briefing for Judiciary Committee staff with the Secret Service and officials for the Department of Homeland Security's Office of the Inspector General. I have asked Director Sullivan to be available to come back and meet with Members of this Committee as the investigation continues.

I have no doubt you are treating this situation with equal seriousness. No one wants to see the President's security compromised or America embarrassed. Senators on this Committee will be very interested to hear from you on this matter today.

You told this Committee at your first appearance as Secretary that you would focus on using limited Federal law enforcement resources in a smarter, more effective manner when enforcing our immigration laws. You and Immigration and Customs Enforcement (ICE) Director John Morton are following through. The implementation of ICE's prosecutorial discretion policy is a positive step forward in meeting the goal of smarter immigration enforcement. If this new policy has the effect of apprehending more individuals who are legitimate threats to public safety, and providing some measure of relief to those who pose no threat, then that is an improvement. You are standing by your commitment to focus first and foremost on the most dangerous among the undocumented population.

My view is that you are doing the best you can in the absence of Congress taking up meaningful and comprehensive immigration reform. As we hold this hearing today, the Supreme Court is hearing argument on the constitutionality of an Arizona immigration enforcement law. The Constitution of the United States declares that Congress and the Federal Government shall have the power to establish a uniform "Rule of Naturalization." Accordingly, national immigration policy is properly a subject we need to act upon. It should not be left to a hodgepodge of conflicting state laws. We came close to enacting comprehensive, fair-minded, bipartisan immigration reform a few years ago before we were derailed by anti-immigrant forces. I look forward to our achieving that goal.

In 2010, Congress passed an emergency appropriations measure to provide $600 million for border security enhancements. You have reported that we have made significant strides in securing our borders and in our overall immigration enforcement activities. I understand that illegal border crossings on the Southern border have declined, and that we have seen steady increases in the numbers of Border Patrol and Customs and Border Protection Officers that are monitoring our borders and ports of entry. I take special notice, as well, that you are working with Canadian officials on the "Beyond the Border" initiative to coordinate resources and address challenges involving the security of our shared northern border. I am encouraged by these improvements and I look forward to hearing more about the Department's progress and your continuing challenges.

In Vermont many business people look forward to our friends from Canada visiting and enjoying all that Vermont has to offer. We want to continue to improve on that relationship and the ways we can safely accommodate foreign travel, tourism and investment.

I was pleased to see that the EB-5 Regional Center Program was among your recommendations and those of the President's Council on Jobs and Competitiveness. This job-creating, immigration-through-investment visa helps harness our immigration system to strengthen our economy and help our business leaders attract talented people from around the world. I look forward to the reauthorization of this program. Senator Grassley and I have been working together to get this and other expiring visa programs reauthorized in a bipartisan manner. As we move forward, I also hope to continue working with you and with USCIS Director Mayorkas to strengthen and improve the EB-5 program so that it may continue to be a job creator for our communities, and to ensure that the agency has the tools it needs to maintain the highest level of integrity in the program.

I have raised the issue of screening procedures and technology in our airports and I continue to have questions about these policies, their impact on the privacy and health of Americans, and whether this technology is the most effective use of resources. I look forward to discussing this issue further today.

I want to work with you to ensure that Americans' privacy rights and civil liberties are safeguarded as we work to enhance our national cybersecurity, and also to enact better privacy protections to keep Americans' safe from identity thieves in cyberspace.

Finally, I want to commend the women and men who work in the agencies of your Department. Many are Vermonters who are working hard to adjudicate immigration benefits at the Vermont Service Center, and contributing to our immigration enforcement and border security efforts at the Law Enforcement Support Center and other ICE and CBP facilities in the State. I understand that the Vermont Service Center is expanding its workforce in St. Albans, Vermont, which is welcome news and is a credit to the dedicated employees and managers at the facility.

# # # # #

Statement for the Record

Secretary Janet Napolitano

U.S. Department of Homeland Security

Before the

United States Senate

Committee on the Judiciary

April 25, 2012

Chairman Leahy, Ranking Member Grassley, and Members of the Committee:

I am pleased to join you today, and I thank the Committee for your strong support for the Department of Homeland Security (DHS) over the past three years and, indeed, since the Department's founding more than nine years ago. I look forward to continuing to work with you to protect the American people as we work to advance our many shared goals.

Today, ten years after the September 11th attacks, America is stronger and more secure, thanks to the support of the Congress, the work of the men and women of DHS, and our federal, state, local, tribal, and territorial partners across the homeland security enterprise.

More than 230,000 DHS employees ensure the safety and security of the American people every day, in jobs that range from law enforcement officers and agents to disaster response coordinators, from those who make sure our waterways stay open to commerce to those who make sure our skies remain safe. The men and women of DHS are committed to our mission, and I thank every one of them for their service.

As I have said many times, homeland security begins with hometown security. As part of our commitment to strengthening hometown security, we have worked to get information, tools, and resources out of Washington, D.C., and into the hands of state, local, tribal, and territorial officials and first responders.

This has led to significant advances. We have made great progress in improving our domestic capabilities to detect and prevent terrorist attacks against our people, our communities, and our critical infrastructure. We have increased our ability to analyze and distribute threat information at all levels. We have invested in training for local law enforcement and first responders of all types in order to increase expertise and capacity at the local level. And we have supported and sustained preparedness and response capabilities across the country through approximately $35 billion in homeland security grants since 2002.

We work with a vast array of partners, from local law enforcement, the private sector, and community leaders across the country, all of whom understand our shared responsibility for public safety and are committed to doing their part to help keep America safe.

To continue to build on these efforts, the Administration has proposed a new homeland security grants program in Fiscal Year 2013 designed to develop, sustain, and leverage core capabilities across the country in support of national preparedness, prevention, and response. The Fiscal Year 2013 National Preparedness Grant Program (NPGP) will help create a robust national preparedness capacity based on cross-jurisdictional and readily deployable state, local, tribal, and territorial assets. Using a competitive, risk-based model, the NPGP will use a comprehensive process for identifying and prioritizing deployable capabilities, limit periods of performance to put funding to work quickly, and require grantees to regularly report progress in the acquisition and development of these capabilities.

Our experience over the past several years also has made us smarter about the terrorist threats we face and how best to deal with them. We have learned that an engaged, vigilant public is

essential to efforts to prevent acts of terrorism, which is why we have continued to expand the "If You See Something, Say Something™" campaign nationally. We also continue to expand our risk-based, intelligence-driven security efforts. By sharing and leveraging information, we can make informed decisions about how to best mitigate risk, and the more we know, the better we become at providing security that is seamless and efficient. We also free up more time and resources, giving us the ability to focus those resources on those threats or individuals that we know less about.

Additionally, over the past several years, we have deployed unprecedented levels of personnel, technology, and resources to protect our nation's borders. These efforts have achieved significant results, including historic decreases in illegal immigration as measured by total apprehensions, and increases in seizures of illegal drugs, weapons, cash, and contraband.

We also have focused on smart and effective enforcement of immigration laws while streamlining and facilitating the legal immigration process. Our enforcement resources prioritize the identification and removal of criminal aliens and repeat immigration law violators, recent border entrants, and immigration fugitives. We also are identifying and sanctioning employers who knowingly hire workers, not authorized to work in the United States, and—by doing so—undercut employers who follow the rules.

The Department also continues to lead the federal government's efforts to secure civilian government computer systems and works with industry and state, local, tribal, and territorial governments to secure critical infrastructure and information systems. We are deploying the latest tools across the federal government to protect critical civilian systems, while sharing timely and actionable security information with public and private sector partners to help them protect their own operations. Together with our public and private sector partners, we are protecting the systems and networks that support the financial services industry, the electric power industry, and the telecommunications industry, to name a few.

Strengthening homeland security also includes a significant international dimension. To most effectively carry out our core missions – including preventing terrorism, securing our borders and enforcing immigration laws, and protecting cyberspace – we partner with countries around the world. This work ranges from strengthening cargo, aviation, and supply chain security to joint investigations, information sharing, and science and technology cooperation. Through collaborations with other federal agencies and our foreign counterparts, we not only enhance our ability to prevent terrorism and transnational crime; we also leverage the resources of our international partners to more efficiently and cost-effectively secure global trade and travel, in order to ensure that dangerous people and goods do not enter our country.

In my time today, I would like to provide an update on the key areas of the DHS mission that fall within the Committee's jurisdiction, our priorities for the coming year, and our vision for working with the Congress to build on the substantial progress we have achieved to date and must continue to sustain in the months and years ahead.

Preventing Terrorism and Enhancing Security

While the United States has made significant progress, threats from terrorism—including, but not limited to al-Qaeda and al-Qaeda affiliated groups—persist and continually evolve, and the demands on DHS continue to grow. Today's threats are not limited to any one individual, group or ideology and are not defined or contained by international borders. Terrorist tactics can be as simple as a homemade bomb and as sophisticated as a biological threat or a coordinated cyber attack.

DHS and our partners at the federal, state, tribal, and local levels have had success in thwarting numerous terrorist plots, including the attempted bombings of the New York City subway and Times Square, foiled attacks against air cargo, and other attempts across the country. Nonetheless, recent attacks overseas, including the attacks in Toulouse, France last month and the continued threat of homegrown terrorism in the United States, demonstrate how we must constantly remain vigilant and prepared.

To address these evolving threats, DHS employs risk-based, intelligence-driven operations to prevent terrorist attacks. Through a multi-layered detection system focusing on enhanced targeting and information sharing, we work to interdict threats and dangerous people at the earliest point possible. We also work closely with federal, state, and local law enforcement partners on a wide range of critical homeland security issues in order to provide those on the frontlines with the information and tools they need to address threats in their communities.

Sharing Information, Expanding Training, and Raising Public Awareness

The effective sharing of information in a way that is timely, actionable whenever possible, and adds value to the homeland security enterprise is essential to protecting the United States. As part of our approach, we have changed the way DHS provides information to our partners by replacing the old color-coded alert system with the new National Terrorism Advisory System, or NTAS, which provides timely, detailed information about credible terrorist threats and recommended security measures.

We also have continued to enhance our analytic capability through the 77 designated fusion centers, resulting in unprecedented information sharing capabilities at the state and local levels. DHS has supported the development of fusion centers through deployed personnel, training, technical assistance, exercise support, security clearances, connectivity to federal systems, technology, and grant funding.

We currently have more than 90 DHS intelligence officers deployed to fusion centers, working side by side with their federal, state, and local counterparts. Sixty-three fusion centers can now receive classified and unclassified threat information through the Homeland Secure Data Network, or HSDN.

We are also working to ensure that every fusion center supported by DHS maintains a set of core capabilities that includes the ability to assess local implications of national intelligence, share

information with federal authorities so we can identify emerging national threats, and ensure the protection of civil rights, civil liberties and privacy.

Specifically, we are encouraging fusion centers to develop and strengthen their grassroots analytic capabilities so that national intelligence can be placed into local context, and the domestic threat picture can be enhanced based on an understanding of the threats in local communities. We are partnering with fusion centers to establish more rigorous analytic processes and analytic production plans, increasing opportunities for training and professional development for state and local analysts, and encouraging the development of joint products among fusion centers and federal partners.

Over the past three years, we also have transformed how we train our nation's frontline officers regarding suspicious activities, through the Nationwide Suspicious Activity Reporting Initiative. This initiative, which we conduct in partnership with the Department of Justice, is an administration effort to train state and local law enforcement to recognize behaviors and indicators related to terrorism and terrorism-related crime; standardize how those observations are documented and analyzed; and ensure the sharing of those reports with the Federal Bureau of Investigation-led Joint Terrorism Task Forces (JTTFs) for further investigation.

More than 213,000 law enforcement officers have now received training under this initiative, and more are getting trained every week. The training was created in collaboration with numerous law enforcement agencies, and with privacy, civil rights and civil liberties officials. DHS also has expanded the Nationwide Suspicious Activity Reporting Initiative to include our nation's 18 critical infrastructure sectors. Infrastructure owners and operators from the 18 sectors are now contributing information, vetted by law enforcement through the same screening process otherwise used to provide information to the JTTFs.

Because an engaged and vigilant public is vital to our efforts to protect our communities from violence, including that resulting from terrorism, we also have continued our nationwide expansion of the "If You See Something, Say Something™" public awareness campaign. This campaign encourages Americans to contact law enforcement if they see something suspicious or potentially dangerous. To date, we have expanded the campaign to federal buildings, transit systems, major sports and entertainment venues, some of our nation's largest retailers, as well as many law enforcement partners. We will continue to expand the campaign even further this year.

Countering Violent Extremism

At DHS, we believe that local authorities and community members are often best able to identify individuals or groups residing within their communities exhibiting dangerous behaviors—and intervene—before they commit an act of violence. Countering violent extremism (CVE) is a shared responsibility, and DHS continues to work with a broad range of partners to gain a better understanding of the behaviors, tactics, and other indicators that could point to terrorist activity, and the best ways to mitigate or prevent that activity.

The Department's efforts to counter violent extremism are three-fold. We are working to better understand the phenomenon of violent extremism, and assess the threat it poses to the Nation as a whole, and within specific communities. We are bolstering efforts to address the dynamics of violent extremism and strengthen relationships with those communities targeted for recruitment by violent extremists. We are also expanding support for information-driven, community-oriented policing efforts that have proven effective in preventing violent crime across the nation for decades.

As part of this approach, and consistent with the Administration's strategy released in August 2011and the related Strategic Implementation Plan released in December 2011, we are implementing a CVE curriculum for state and local law enforcement that is focused on community-oriented policing, which will help frontline personnel identify activities that are potential indicators of potential terrorist activity and violence. We piloted the curriculum in San Diego in January 2012, and we are working with the International Association of Chiefs of Police (IACP) to implement the curriculum in law enforcement academies nationwide. We are also developing a similar curriculum with the Federal Law Enforcement Training Center (FLETC) for federal law enforcement officers.

With local communities and the Department of Justice, we have published guidance on best practices for community partnerships to prevent and mitigate homegrown threats. And we have issued, and continue to release, unclassified case studies that examine recent incidents involving terrorism so all of us can better understand the potential warning signs of violent extremism.

Protecting Our Aviation System

We have continued to strengthen protection of our aviation sector through a layered detection system focusing on risk-based screening, enhanced targeting, and information-sharing efforts to interdict threats and dangerous people at the earliest point possible.

The Department is focused on measures to evolve aviation security from a "one size fits all" approach for passenger screening to a risk-based approach to security. In doing so, TSA utilizes a range of measures, both seen and unseen. Our nation's aviation sector continues to be a high threat terrorist target. There is currently no silver bullet; however we utilize a layered approach that seeks to both protect the aviation system and expedite passenger travel.

The Transportation Security Administration (TSA) has deployed approximately 650 Advanced Imaging Technology (AIT) units to airports across the United States to assist our Transportation Security Officers in safely screening passengers for metallic and non-metallic threats. TSA has now installed new software on all millimeter wave AIT machines to enhance privacy by eliminating passenger-specific images and TSA is working closely with the vendor to deploy this capability to backscatter units as quickly as possible. TSA also continues to deploy Explosives Detection Systems to airports to efficiently screen baggage for explosives while reducing the number of physical bag searches

Additionally, TSA has added more canine teams, which serve as an important layer of security to complement passenger checkpoint screening at airports, assist in air cargo screening, and

enhance security in the mass transit environment. And through Secure Flight, TSA is now pre-screening 100 percent of all travelers flying within, to, or from the United States against terrorist watchlists before passengers receive their boarding passes.

As we have taken these actions to strengthen security, we also have focused on expediting trade and travel for the millions of people who rely on our aviation system every day. One key way we have done this is through expansion of trusted traveler programs.

For instance, the Global Entry program, which is managed by U.S. Customs and Border Protection (CBP), is allowing us to expedite entry into the United States for pre-approved, low-risk air travelers. More than one million passengers have already joined Global Entry, and we are expanding the program as part of the Administration's efforts to foster travel and tourism.

Global Entry participants are also eligible for TSA Pre√™. TSA Pre√™ is a domestic expedited traveler initiative that enhances security by allowing us to focus on passengers we know less about and those who are considered high-risk, while providing expedited screening for travelers who volunteer information about themselves prior to flying. Efforts like TSA Pre√™ represent an important evolution in the way we handle airline security, as we shift away from the one-size-fits-all model of passenger screening to one that is risk-based.

In our increasingly interconnected world, we also work beyond our own airports to protect both national and economic security through partnerships with international allies and other Federal agencies, and enhanced targeting and information-sharing efforts to interdict threats and dangerous people and cargo at the earliest point possible.

For example, through the Pre-Departure Targeting Program and Immigration Advisory Program and enhanced in-bound targeting operations, CBP has improved its ability to identify high-risk travelers who are likely to be inadmissible into the United States and make recommendations to commercial carriers to deny boarding before a plane departs.

Through the Visa Security Program and with Department of State concurrence, U.S. Immigration and Customs Enforcement (ICE) has deployed trained special agents overseas to high-risk visa activity posts to identify potential terrorist and criminal threats before they reach the United States.

Through preclearance agreements, CBP is also inspecting passengers internationally prior to takeoff through the same process a traveler would undergo upon arrival at a U.S. port of entry, allowing us to extend our borders outward while facilitating a more efficient passenger experience.

Our continued use, analysis, and sharing of Passenger Name Record (PNR) data has allowed us to better identify passengers we should pay more attention to before they arrive at the airport they are departing from overseas. In December 2011, we signed a new agreement with the European Union to continue the transfer of PNR data, an important milestone in our collective efforts to protect the international aviation system from terrorism and other threats.

Visa Waiver Program

With our partners overseas, we also have acted to strengthen the Visa Waiver Program (VWP), which allows eligible nationals of 36 countries to travel to the United States without a visa and remain in our country for up to 90 days for tourist or business purposes. Since its inception in the mid-1980s, the VWP has become an essential tool for increasing security standards, advancing information sharing, strengthening international relationships, and promoting legitimate travel to the United States.

Over the last several years, DHS has focused on bringing VWP countries into compliance with information sharing agreement requirements of The Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act), Pub. L. No.110-53. As of January 2012, all VWP countries have completed an exchange of diplomatic notes or an equivalent mechanism for the requirement to enter into an agreement to share information on lost and stolen passports with the United States through INTERPOL or other designated means.

DHS also has signed Preventing and Combating Serious Crime (PCSC) agreements with 22 VWP countries which facilitate the sharing of information about terrorists and criminals. Negotiations on four additional PCSC Agreements with VWP countries have been completed, and we have an equivalent agreement already in force with the United Kingdom.

Additionally, DHS developed the Electronic System for Travel Authorization (ESTA) as a proactive online system to determine whether an individual is eligible to travel to the United States under the VWP, and whether such travel poses any law enforcement or national security risks. The system was created in response to a requirement in the 9/11 Act, which mandated that all citizens of VWP eligible countries who plan to travel to the United States under the VWP, must obtain an electronic travel authorization prior to boarding a U.S.-bound commercial flight or cruise ship.

Overstays and Exit Capabilities

Over the past year, we also have worked to better detect and deter those who overstay their lawful period of admission. The ability to identify and sanction overstays derives from the ability to determine who has arrived and departed from the United States. By matching arrival and departure records and using additional data collected by DHS, we can better determine who has overstayed their lawful period of admission.

In May 2011, DHS began a coordinated effort to vet all potential overstay records against Intelligence Community and DHS holdings for national security and public safety concerns. In total, using those parameters, we reviewed the backlog of 1.6 million overstay leads within the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program and referred leads based on national security and public safety priorities to ICE for further investigation.

A beneficial by-product of this vetting effort has been the identification of efficiencies gained through automation, as well as other enhancements. Through a new automated system, we will be able to enhance automated matching, eliminate gaps in travel history, and aggregate information from multiple systems.

In October 2011, I proposed a strategy to Congress to utilize DHS funds to implement an automated vetting and enhanced biographic exit capability. This strategy will allow the Department to significantly enhance our existing capability to identify and target for enforcement action those who have overstayed their authorized period of admission, and who represent a public safety and/or national security threat by incorporating data contained within law enforcement, military, and intelligence repositories.

This strategy also will enhance our ability to identify individual overstays and determine overstay percentages by country; provide the State Department with information to support visa revocation, prohibit Visa Waiver Program travel, and place "lookouts" for individuals, in accordance with existing Federal laws; establish greater efficiencies to our Visa Security Program; and enhance the core components of an entry-exit and overstay program.

I have directed the Science and Technology Directorate (S&T) to establish criteria and promote research for emerging technologies that would provide the ability to capture biometrics at a significantly lower operational cost. S&T is working closely with the National Institute of Standards and Technology (NIST) on this initiative, and S&T expects to have a report shortly detailing potential next steps and a road map for the next several years concerning potential capabilities for a future biometric air exit system, including how anticipated technology enhancements can fit within the DHS operational environment.

Following this analysis, we anticipate beginning controlled and scenario-based lab testing within the year and operational testing in less than three years. Overall, if the evaluated approach is determined to be cost effective, the Department will be able to consider deployment of a biometric exit capability within four years.

In addition, we are working toward a system to create an exit program on the United States northern land border to facilitate the exchange of U.S. and Canadian entry records, so that an entry to one country becomes an exit from another.

We support carefully managed expansion of the VWP to countries that meet the statutory requirements, and are willing and able to enter into a close security relationship with the United States. To this end, we support current bi-partisan efforts by the Congress to expand VWP participation and also to promote international travel and tourism to the United States while maintaining our strong commitment to security.

Protecting Surface Transportation

Beyond aviation, we have worked with transportation sector entities and companies across the United States to enhance security of surface transportation infrastructure through risk-based security assessments, critical infrastructure hardening, and close partnerships with state and local law enforcement partners.

Because of its open access architecture, surface transportation has a fundamentally different operational environment than aviation. As a result, our approach is necessarily different. To

protect surface transportation, we have conducted compliance inspections throughout the freight rail and mass transit domains; critical facility security reviews for pipeline facilities; comprehensive mass transit assessments that focus on high-risk transit agencies; and corporate security reviews conducted in multiple modes of transportation on a continuous basis to elevate standards and identify security gaps.

We also have continued to support Visible Intermodal Prevention and Response (VIPR) teams, including 12 multi-modal teams. VIPR teams are composed of personnel with expertise in inspection, behavior detection, security screening, and law enforcement for random, unpredictable deployments throughout the transportation sector to prevent potential terrorist and criminal acts.

These efforts have been supported by more than $1.6 billion in DHS grant funding awarded through the Transit Security Grant Program to harden assets, improve situational awareness, and build national capabilities to prevent and respond to threats and incidents across the transportation sector.

Global Supply Chain Security

Securing the global supply chain system is integral to securing both the lives of people around the world, and maintaining the stability of the global economy. We must work to strengthen the security, efficiency, and resilience of this critical system. Supply chains must be able to operate effectively, in a secure and efficient fashion, in a time of crisis, recover quickly from disruptions, and continue to facilitate international trade and travel.

Earlier this year, I announced on the behalf of the President the U.S. National Strategy for Global Supply Chain Security. This new Strategy provides a government-wide vision of our goals, approach, and priorities to strengthen the global supply chain system. The Strategy establishes two explicit goals: promoting the efficient and secure movement of goods and fostering resilient supply chain systems. As we work to achieve these goals, we will be guided by the overarching principles of risk management and collaborative engagement with key stakeholders who also have key supply chain roles and responsibilities.

DHS is now working in close partnership with other federal departments and agencies to translate the high-level guidance contained in the Strategy into concrete actions. We are focusing our immediate efforts on the priority action areas identified in the Strategy. Some of these efforts include:

- Threat and Risk: Working in concert with other agencies to develop the nation's first Global Supply Chain Threat Assessment and Risk Characterization
- Information Sharing: advancing the development and government-wide utilization of the International Trade Data System for the collection, use, and dissemination of commercial data.
- Targeting Capabilities: Improving the capabilities of targeting systems used to identify high-risk cargo by obtaining additional information from stakeholders as early in the process as possible.

- Infrastructure Resilience: Exploring expanding DHS's Resilience STAR program into the transportation sector, to highlight and advance security and resiliency standards for key supply chain nodes and infrastructure.
- Partnership Programs: Reviewing the variety of US "public-private" partnership programs, with an eye towards opportunities to harmonize them to enhance efficiencies, reduce costs, and better leverage federal resources.
- Technology: Prioritizing research and development needs, both within DHS and across the interagency, based upon an assessment of current capabilities and an understanding of evolving threats and vulnerabilities.

In addition to some of these specific efforts to implement the National Strategy for Global Supply Chain Security, DHS continues to advance a range of other measures and programs to strengthen different components of this vital system.

We are strengthening the global system by working with multilateral organizations such as the International Maritime Organization (IMO), the International Civil Aviation Organization (ICAO), the World Customs Organization (WCO), and the Asia-Pacific Economic Cooperation (APEC) as well as bilaterally with trading partners. Our efforts are not only directed toward achieving specific objectives within the organizations but also on promoting collaboration between them.

For example, we are working with the IMO, WCO, and APEC on developing global systems for managing trade recovery in the event of large scale disruptions. Our engagement with APEC has resulted in their identification of the specific information that governments and the private sector need to be ready to exchange in order to support trade recovery efforts.

We are also working closely with industry and foreign government partners to identify and address high-risk shipments as early in the shipping process as possible by collecting and analyzing advance electronic commercial data. This allows DHS to make risk informed decisions about what cargo is safe to be loaded onto vessels and aircraft prior to their departure from a foreign port and facilitates the clearance of those shipments upon their arrival in the United States.

In the aviation environment, we are working with leaders from global shipping companies and the International Air Transport Association (IATA) to develop preventive measures, including terrorism awareness training for employees and vetting personnel with access to cargo. We now allow participating shippers to screen air cargo, following strict standards to support the requirements of the 9/11 Act for cargo transported on passenger aircraft. We are reviewing our foreign partners' cargo screening to determine whether their programs provide a level of security commensurate with U.S. air cargo security standards. Those who meet these requirements are officially recognized to conduct screening for cargo traveling to the U.S., further strengthening the security of the global supply chain while facilitating the flow of legitimate commerce by screening cargo throughout the supply chain.

DHS is also focused on preventing the exploitation of the global supply chain by those seeking to use the system to transport dangerous, illicit, contraband, contaminated, and counterfeit products.

Under Program Global Shield, just one example of these efforts, we are working with more than 80 countries to prevent the illegal theft or diversion of precursor chemicals that can be used to make Improvised Explosive Devices, or IEDs. Through these efforts we have already seized more than 62 metric tons of these deadly materials.

DHS, through ICE, also continues to investigate U.S. export control law violations, including those related to military items, controlled "dual-use" commodities, and sanctioned or embargoed countries. We are committed to making sure foreign adversaries do not illegally obtain U.S. military products and sensitive technology, including weapons of mass destruction and their components, or attempt to move these items through the global supply chain. In Fiscal Year 2011, ICE initiated 1,780 new investigations into illicit procurement activities, made 583 criminal arrests, and made 2,332 seizures valued at $18.9 million. ICE also manages and operates the Export Enforcement Coordination Center (E2C2), an interagency hub for streamlining and coordinating export enforcement activities and exchanging information and intelligence.

Countering Chemical, Biological, Radiological, and Nuclear Threats

Countering biological, nuclear, and radiological threats requires a coordinated, whole-of-government approach. DHS, through the Domestic Nuclear Detection Office (DNDO) and Office of Health Affairs (OHA), works in partnership with agencies across federal, state, and local governments to prevent and deter attacks using nuclear and radiological weapons through nuclear detection and forensics programs. OHA also provides medical and scientific expertise to support bio preparedness and response efforts.

Through the Securing the Cities program, for example, nearly 11,000 personnel in the New York City region have been trained in preventive radiological and nuclear detection operations and nearly 6,000 pieces of radiological detection equipment have been deployed. DNDO also has facilitated the delivery of radiological and nuclear detection training to more than 4,700 state and local officers and first responders.

Through the BioWatch program, an environmental surveillance system that provides early detection of biological agents, OHA has collected over 200,000 samples in more than 30 cities nationwide to enhance protection and preparedness for high-consequence biological threats. Last year, OHA also conducted the first-ever detailed testing on automated biodetection systems for national application. These detectors analyze samples and relay results to public health officials, and will significantly reduce the time needed to detect a biological attack, potentially saving thousands of lives.

Last year, the DHS National Biodefense Analysis and Countermeasures Center (NBACC) laboratory, which is managed by DHS S&T, also received its accreditation with the Centers for Disease Control & Prevention (CDC) and the U.S. Department of Agriculture to begin research and diagnostics on pathogens to understand the scientific basis of the risks posed by biological threats and to attribute their use in bioterrorism events.

Under the leadership of the Office of Science and Technology Policy, DHS S&T, in collaboration with NIST, also published "The National Strategy for Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE) Standards," which lays out the federal vision and goals to achieve a comprehensive structure for the coordination, prioritization, establishment and implementation of CBRNE equipment standards by 2020.

Securing and Managing Our Borders

DHS secures the nation's air, land, and sea borders to prevent illegal activity while facilitating lawful travel and trade. The Department's border security and management efforts focus on three interrelated goals: effectively securing U.S. air, land, and sea borders; safeguarding and streamlining lawful trade and travel; and disrupting and, in coordination with other federal agencies, dismantling transnational criminal and terrorist organizations.

Southwest Border

To secure our nation's Southwest border, we have continued to deploy unprecedented amounts of manpower, resources, and technology, while expanding partnerships with federal, state, tribal, territorial, and local partners, as well as the Government of Mexico.

Simply put, the Obama administration has undertaken the most serious and sustained actions to secure the Southwest border in our nation's history. We have increased the number of Border Patrol agents nationwide from approximately 10,000 in 2004 to more than 21,000 today with nearly 18,500 "boots on the ground" along the Southwest border. Working in coordination with state and other federal agencies, we have deployed a quarter of all ICE operational personnel to the Southwest border region –the most ever – to dismantle criminal organizations along the border.

We have doubled the number of ICE personnel assigned to Border Enforcement Security Task Forces, which work to dismantle criminal organizations along the border. We have tripled deployments of Border Liaison Officers, who facilitate cooperation between U.S. and Mexican law enforcement authorities on investigations and enforcement operations, including drug trafficking (coordinated with the Drug Enforcement Administration). We also have increased the number of intelligence analysts working along the U.S.-Mexico border

In addition, we have deployed dual detection canine teams as well as non-intrusive inspection systems, Mobile Surveillance Systems, Remote Video Surveillance Systems, thermal imaging systems, radiation portal monitors, and license plate readers to the Southwest border. These technologies, combined with increased manpower and infrastructure, give our personnel better awareness of the border environment so they can more quickly act to resolve potential threats or illegal activity. We also are screening southbound rail and vehicle traffic looking for the illegal weapons and cash that are helping fuel the cartel violence in Mexico.

We also have completed 650 miles of fencing out of nearly 652 miles mandated by Congress as identified by Border Patrol field commanders, including 299 miles of vehicle barriers and 351 miles of pedestrian fence.

To enhance cooperation among local, tribal, territorial, state and federal law enforcement agencies, we have provided nearly $205 million in Operation Stonegarden funding since 2009. In that time, Southwest border law enforcement agencies received over $167 million in grants through the Operation Stonegarden program.

Our work along the border has included effective support from our partners at the Department of Defense (DOD). In addition to continuing support from DOD's Joint Task Force-North and the National Guard, in 2010, President Obama authorized the temporary deployment of up to 1,200 National Guard troops to the Southwest Border to contribute additional capabilities and capacity to assist law enforcement agencies as a bridge to longer-term enhancements in the efforts to target illicit networks' smuggling of people, drugs, illegal weapons, money, and the violence associated with these illegal activities.

Beginning in March 2012, DOD's National Guard support to CBP began to transition from ground support to air support, essentially moving from boots on the ground to boots in the air with state of the art aerial assets equipped with the latest detection and monitoring capabilities.

These aerial assets, which include both rotary and fixed-wing aircraft, supplement the CBP Office of Air and Marine aerial assets and support the Border Patrol's ability to operate in diverse environments, expand our field of vision in places with challenging terrain, and help us establish a greater visible presence from a distance, which increases deterrence.

The U.S. Coast Guard also is continuing its integral role in our border enforcement strategy through its maritime operations at the Joint Interagency Task Force (JIATF)-South, the U.S. Southern Command entity that coordinates integrated interagency counter drug operations, the Caribbean Sea, Gulf of Mexico, and the eastern Pacific. In Fiscal Year 2011, the Coast Guard removed nearly 75 metric tons of cocaine, and more than 17 metric tons of marijuana. CBP Office of Air and Marine P-3 aircraft also have been an integral part of successful counter-narcotic missions operating in the Source and Transit Zones in coordination with JIATF-South.

The results of these comprehensive and coordinated efforts have been striking. Border Patrol apprehensions—a key indicator of illegal immigration—have decreased 53 percent in the last three years and are less than 20 percent of what they were at their peak. Indeed, illegal immigration attempts have not been this low since 1971. Violent crime in U.S. border communities has also remained flat or fallen over the past decade, and statistics have shown that some of the safest communities in America are along the border. From Fiscal Years 2009 to 2011, DHS also seized 74 percent more currency, 41 percent more drugs, and 159 percent more weapons along the Southwest border as compared to Fiscal Years 2006 to 2008.

To further deter individuals from illegally crossing our Southwest border, we also directed ICE to prioritize the apprehension of recent border crossers and repeat immigration violators, and to support and supplement Border Patrol operations. Between Fiscal Years 2009 and 2011, ICE made over 30,936 criminal arrests along the Southwest border, including 19,563 arrests of drug smugglers and 4,151 arrests of human smugglers.

Over the past year we made several announcements that will continue to support this work and expand the collaboration necessary to sustain the progress we have achieved. For example, in July 2011, the Obama Administration released the 2011 National Southwest Border Counternarcotics Strategy, a key component of federal efforts to enhance security along the Southwest border. The strategy outlines federal, state, local, tribal, and international actions to reduce the flow of illicit drugs, cash, and weapons across the border, and highlights the Obama Administration's support for promoting strong border communities by expanding access to drug treatment and supporting programs that break the cycle of drug use, violence, and crime.

The *Declaration on 21st Century Border Management*, issued by President Obama and President Calderon last year, signals the United States government's commitment to increase collaboration with Mexico; both to facilitate legitimate trade and travel at the border and to continue combating transnational crime. As part of this effort, we are working closely with our Mexican counterparts on critical infrastructure protection and expansion of trusted traveler and shipper programs.

In addition to our efforts to strengthen border security, we made great strides in expediting legal trade and travel, working with local leaders to update infrastructure and reduce wait times at our Southwest border ports of entry. Along the Southwest border, new initiatives have included outbound infrastructure improvements and port hardening, which when completed, will expand our outbound inspection capabilities, enhance port security, and increase officer safety. We also have implemented Active Lane Management, which leverages Ready Lanes, Dedicated Commuter Lanes, and LED signage to dynamically monitor primary vehicle lanes and re-designate lanes as traffic conditions and infrastructure limitations warrant.

These efforts are not only expediting legitimate trade, they are also stopping contraband from entering and leaving the country. In Fiscal Year 2011, DHS interdicted goods representing more than $1.1 billion in Manufacturer's Suggested Retail Price. Further, the value of consumer safety seizures including pharmaceuticals totaled more than $60 million, representing a 41 percent increase over Fiscal Year 2010.

Northern Border

Along the Northern border, we have continued to deploy technology and resources to protect the border, invest in port of entry improvements to enhance security and improve trade and travel, and deepen our already strong partnership with Canada.

For instance, CBP expanded unmanned aerial surveillance coverage along the Northern border into eastern Washington, now covering 950 miles of the Northern border. In 2011, CBP Office of Air and Marine provided nearly 1,500 hours of unmanned aerial surveillance along the Northern Border.

In 2011, CBP also opened the Operations Integration Center in Detroit—a multi-agency communications center for CBP, DHS, and other federal, state, local, and Canadian law enforcement agencies on the northern border. The Operations Integration Center increases information sharing capabilities leading to seizures of drugs, money and illegal contraband along

the U.S - Canada border within the Detroit Sector. S&T is also evaluating new surveillance technologies for CBP in Swanton Sector, Vermont that can operate in harsh and remote environments and use renewable energy such as solar and wind power. Sharing surveillance data with Canada to combat illegal border entries is also in progress.

We also have continued to invest heavily in infrastructure improvements at our ports of entry, including over $400 million in Recovery Act funds to modernize older facilities along our Northern border to meet post-9/11 security standards.

Through the Beyond the Border Action Plan released by President Obama and Prime Minister Harper in December 2011, we are also enhancing cooperation with Canada through greater information sharing, more coordinated passenger and baggage screening, and integrated law enforcement operations. .As part of this action plan, we are working with our U.S. and Canadian partners to develop the next generation of integrated cross-border law enforcement, interoperable radio communications, border wait time measurements, and enhanced air/land/maritime domain awareness, as well as a multitude of initiatives to streamline trusted trader and traveler programs and expedite legitimate travel and trade.

With Canada's Public Safety Minister Vic Toews, I announced the Joint Border Threat and Risk Assessment, highlighting our nations' shared commitment to identifying and mitigating potential threats of terrorism and transnational organized crime along the border.

Enforcing and Administering our Immigration Laws

DHS has undertaken a historic effort to enforce and administer immigration laws in a cohesive way that is smart, effective, and that maximizes the resources that the Congress has given us to do this important job. We have worked, and continue to work, to make sure that our limited resources are applied consistently and in a manner that enhances public safety, border security, and the integrity of the immigration system, while respecting the rule of law and staying true to our history as a nation of immigrants.

Targeting Criminal and Other Priority Aliens

We have established as a top priority the identification and removal of public safety and national security threats. To this end, we have expanded the use and frequency of investigations and programs that track down criminals and other public safety and national security threats on our streets and in our jails.

Overall, in Fiscal Year 2011, ICE removed nearly 397,000 individuals. Ninety percent of these removals fell within one of ICE's priority categories, and 55 percent, or more than 216,000 of the people removed, were convicted criminal aliens – an 89 percent increase in the removal of criminals from Fiscal Year 2008. This total includes more than 87,000 individuals convicted of homicide, sexual offenses, dangerous drugs, and driving under the influence. Of those removed in Fiscal Year 2011 without a criminal conviction, more than two-thirds fell into our priority categories of recent border crossers or repeat immigration law violators.

In a single "Cross Check" enforcement operation conducted over a six-day period this year, ICE arrested more than 3,100 convicted criminal aliens, immigration fugitives and immigration violators. This operation was the largest of its kind, involving the collaboration of more than 1,900 ICE officers and agents. Arrests occurred in all 50 states, four U.S. territories, and the District of Columbia.

Through the Secure Communities program, ICE uses biometric information to identify criminal and other priority aliens found in state prisons and local jails so that ICE can prioritize them for removal. It remains an important tool in ICE's efforts to focus its immigration enforcement resources on individuals within ICE's priorities, particularly those who pose a threat to public safety or national security.

We have expanded the Secure Communities program from 14 jurisdictions in 2008 to 2,304 today, including all jurisdictions along the Southwest border. We are on track to deploy this program to all jurisdictions nationwide by 2013. Since its inception, more than 135,400 immigrants convicted of serious crimes, including aggravated felony offenses like murder, rape and sexual abuse of children, have been removed from the United States after identification through Secure Communities.

Nevertheless, we recognize that there is always room to improve any program, and we are mindful of concerns raised about Secure Communities. Under the leadership of ICE Director John Morton, we have taken significant action to improve the program and clarify its goals to law enforcement and the public.

We are committed to ensuring the Secure Communities program respects civil rights and civil liberties. To that end, ICE is working closely with law enforcement agencies and stakeholders across the country to ensure the program operates in the most effective manner possible and respects community policing efforts critical to public safety. ICE and CRCL are developing videos for state and local law enforcement agencies on how Secure Communities works and how it relates to laws governing civil rights and civil liberties. They also are conducting a regular statistical analysis of the program to identify any signs of potential abuse, and they have announced a complaint investigation protocol where individuals or organizations who believe civil rights violations connected to Secure Communities have occurred can file a complaint with ICE or CRCL. We also are reviewing the findings and recommendations of the DHS Homeland Security Advisory Council (HSAC) Secure Communities Task Force.

In addition, as part of its enforcement approach, ICE has issued additional guidance to its personnel to ensure that those enforcing immigration laws make appropriate use of the discretion they already have in deciding the types of individuals we prioritize for removal from the country. President Obama and I have both made clear that we will continue to enforce the laws in a smart and effective manner, and part of this is exercising discretion on a case by case basis where DHS feels it enhances our ability to meet our priorities.

With the cooperation of the Department of Justice, we continue to review incoming cases and existing caseloads to ensure they correspond with our enforcement priorities and support our mission to protect public safety and ensure border security. This effort has led to an

unprecedented collaboration among federal agencies to focus taxpayer resources devoted to immigration enforcement on priority cases.

Deterring Employment of Aliens Not Authorized to Work

In the worksite category, we have eliminated high-profile raids that did little to enhance public safety, instead promoting compliance with worksite-related laws through criminal prosecutions of egregious employer violators, Form I-9 inspections, civil fines, and debarment, as well as education and compliance tools.

Since January 2009, ICE has audited more than 7,001 employers suspected of knowingly hiring workers unauthorized to work in the United States, debarred 594 companies and individuals, and imposed more than $79.9 million in financial sanctions—more than the total amount of audits and debarments during the entire previous administration.

Employer enrollment in E-Verify, our on-line employee verification system managed by U.S. Citizenship and Immigration Services (USCIS), has more than doubled since January 2009, with more than 358,000participating companies representing more than 1.1 million hiring sites. USCIS has continued to promote and strengthen E-Verify, developing a robust customer service and outreach staff to increase public awareness of E-Verify's benefits and inform employers and employees of their rights and responsibilities. In Fiscal Year 2011 alone, USCIS informed tens of millions of people about E-Verify through radio, print, and online ads in English and Spanish, and hundreds of thousands more through live presentations, conference exhibitions, live webinars, and distribution of informational materials.

More than 17 million queries were processed in E-Verify in Fiscal Year 2011, allowing businesses to verify the eligibility of their employees to work in the United States. Last year, we also launched the E-Verify Self Check program, a voluntary, free, fast, and secure online service that allows individuals in the United States to confirm the accuracy of government records related to their employment eligibility status before seeking employment.

Detention Reform

As a part of ongoing detention reform efforts, ICE continues to identify systematic ways to reform and improve medical and mental health care at detention facilities, including an increase in medical case management and quality management activities, assigning field medical coordinators to each ICE Field Office to provide ongoing case management; simplifying the process for detainees to receive authorized health care treatments; and developing a medical classification system to support detainees with unique medical or mental health needs.

ICE also has issued revised detention standards. The new standards, known as Performance-Based National Detention Standards 2011 (PBNDS 2011), reflects ICE's ongoing effort to tailor the conditions of immigration detention while maintaining a safe and secure detention environment for staff and detainees. In developing the revised standards, ICE incorporated the input of many agency employees and stakeholders, including the perspectives of nongovernmental organizations and ICE field offices. PBNDS 2011 is crafted to improve

medical and mental health services, increase access to legal services and religious opportunities, improve communication with detainees with limited English proficiency, improve the process for reporting and responding to complaints, detect and prevent sexual assault and abuse, and increase visitation.

ICE has hired additional detention service managers to increase onsite federal oversight and ensure that facilities are in compliance with its detention standards while increasing announced and unannounced inspections by other staff. CRCL has assisted in training these ICE employees and reviewing the standards they enforce. CRCL has also stepped up oversight of immigration facilities, conducting numerous on-site inspections, and additional reviews specifically relating to medical care.

Additionally, instead of housing the vast majority of immigrant detainees in small groups in jails across the country, ICE has initiated a consolidation effort which includes the addition of larger, civil detention facilities to its inventory.

Last year, ICE opened two such facilities in California and New Jersey and opened the first true civil detention facility in Texas in February 2012. The acquisition of these facilities has enabled ICE to reduce the number of transfers and detain individuals closer to their arrest locations, families, legal service providers, and other community support organizations.

ICE will continue building on these ongoing detention reform efforts. It expects to implement a new Risk Classification Assessment nationwide to improve transparency and uniformity in detention custody and classification decisions and to promote identification of vulnerable populations. In addition, ICE will continue its implementation of the new Transfer Directive, which is designed to minimize long-distance transfers of detainees within ICE's detention system, especially for those detainees with family members, local attorneys, or pending immigration proceedings in the area where they are detained.

Improving Legal Immigration

Our nation's founding is rooted in immigration and immigrants have contributed to the richness of our culture, the strength of our character, and the advancement of our society. To continue to promote legal immigration to the United States and the process by which we naturalize new American citizens each year, we have worked to reduce bureaucratic inefficiencies in visa programs, streamline the path for entrepreneurs who wish to bring their business to America, and improve our systems for providing immigration benefits and services.

In 2011, USCIS held more than 6,000 naturalization ceremonies for approximately 692,000 lawful permanent residents who became U.S. citizens, including more than 10,000 members of the U.S. Armed Forces.

To help combat fraud and exploitation of our immigration system, USCIS launched the Unauthorized Practice of Immigration Law (UPIL) initiative, a national, multi-agency campaign that spotlights immigration-services scams and the problems that can arise for immigrants when legal advice or representation is given by people who are not attorneys or accredited

representatives. The UPIL initiative began in seven cities in 2011 and will expand nationwide in 2012.

USCIS also launched a series of policy, operational, and outreach efforts to support economic growth and stimulate investment by attracting foreign entrepreneurs who can create jobs, form startup companies, and invest capital in areas of high unemployment.

USCIS also announced the Entrepreneurs in Residence initiative to ensure that its policies and practices better reflect business realities of industries that regularly use visa categories for immigrant investors, job-creating entrepreneurs, and workers with specialized skills, knowledge, or abilities.

These efforts have included enhancements to streamline the Employment Creation immigrant visa program, commonly known as the EB-5 Program, including conducting a top to bottom review of EB-5 business processes, and hiring economists and business analysts to support EB-5 adjudications.

USCIS also has provided clarification on how H-1B visas, which allow U.S. employers to temporarily employ foreign workers in specialty occupations, and EB-2 National Interest Waivers, which offer a streamlined eligibility for immigrant visas to certain foreign workers with advanced degrees and/or exceptional ability in the arts, sciences, or business, may be utilized by foreign-born entrepreneurs.

In addition, last year USCIS launched the Citizenship Public Education and Awareness Initiative to promote awareness of the rights, responsibilities and importance of U.S. citizenship and the free naturalization preparation resources available to permanent residents and immigrant-serving organizations. This multilingual effort is designed to reach nearly 8 million permanent residents eligible to apply for citizenship. And in September 2011, USCIS awarded $9 million in Citizenship and Integration Grants to 42 organizations to expand citizenship preparation programs for permanent residents across the country. The President's Fiscal Year 2013 budget request includes $11 million to continue support for USCIS immigrant integration efforts through funding of citizenship and integration program activities including competitive grants to local immigrant-serving organizations to strengthen citizenship preparation programs for permanent residents.

In January, USCIS also proposed a regulatory change that would significantly reduce the time that U.S. citizens are separated from their spouses and children as they go through the process of obtaining visas to become legal immigrants to the United States. The proposed rule change would minimize the extent to which delays separate Americans from their families by allowing family members, under certain circumstances, to have their waiver applications processed in the United States and receive a provisional waiver determination before they complete the visa process outside the United States.

USCIS also has made significant strides in the development of its Electronic Immigration System (ELIS) to begin the agency's transition from a paper-based to an electronic, online organization. USCIS is currently testing the system and will begin its public releases this year.

And to further enhance our nation's economic, scientific and technological competitiveness, last year I also announced the launch of the Study in the States initiative, an effort aimed at encouraging the best and the brightest international students from around the world to study in the U.S. by finding new and innovative ways to streamline the international student visa process. As part of the initiative, the Study in the States website provides coordinated information in a comprehensive, user-friendly, and interactive way to prospective and current international students, exchange visitors and their dependents about opportunities to study in the United States and learn about expanded post-graduate opportunities.

In March 2012, I also announced the formation of the Homeland Security Academic Advisory Council (HSAAC), comprised of university presidents and academic leaders who will provide advice and recommendations to me and senior DHS leadership on issues related to student and recent graduate recruitment, international students, academic research, campus and community resiliency, security and preparedness, and faculty exchanges.

Safeguarding and Securing Cyberspace

Our daily life, economic vitality, and national security depend on a safe, secure, and resilient cyberspace. A vast array of interdependent IT networks, systems, services, and resources are critical to communication, travel, powering our homes, running our economy, and obtaining government services.

DHS is the federal government's lead agency for securing civilian government computer systems and works with our industry and state, local, tribal, and territorial government partners to secure critical infrastructure and information systems. DHS analyzes and mitigates cyber threats and vulnerabilities; distributes threat warnings; provides solutions to critical research and development needs; and coordinates the vulnerability, mitigation, and consequence management response to cyber incidents to ensure that our computers, networks, and information systems remain safe.

The United States confronts a dangerous combination of known and unknown vulnerabilities in the cyber domain, strong and rapidly expanding adversary capabilities, and limited threat and vulnerability awareness. While we are more network dependent than ever before, increased interconnectivity increases the risk of theft, fraud, and abuse. No country, industry, community or individual is immune to cyber risks.

Cyber incidents have increased dramatically over the last decade. There have been instances of theft and compromise of sensitive information from both government and private sector networks, undermining confidence in our systems, information sharing processes, and the integrity of the data contained within these systems. Last year, the DHS U.S. Computer Emergency Readiness Team (US-CERT) received more than 100,000 incident reports, and released more than 5,000 actionable cybersecurity alerts and information products.

Recognizing the serious nature of this challenge, President Obama made cybersecurity an Administration priority upon taking office. In his Cyberspace Policy Review in 2009, which established a strategic framework for advancing the Nation's cybersecurity policies, the President declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation."

DHS works with federal agencies to secure unclassified federal civilian government networks and works with owners and operators of critical infrastructure to secure their networks through risk assessment, mitigation, and incident response capabilities.

To protect Federal civilian agency networks, we are deploying technology to detect and block intrusions in those agencies with supp-ort from interagency partners. We also work to provide agencies with assistance in the implementation of guidance and standards issued by NIST. In addition, DHS is responsible for coordinating the national response to significant cyber incidents, consistent with the National Response Framework, and for creating and maintaining a common operational picture for cyberspace across the government.

With respect to critical infrastructure, DHS and the sector specific agencies work with the private sector to help secure the key systems upon which Americans rely, such as the financial sector, the power grid, water systems, and transportation networks. We do this by sharing actionable cyber threat information with the private sector, helping companies to identify vulnerabilities before a cyber incident occurs, and providing forensic and remediation assistance to help response and recovery after we learn of a cyber incident.

Last year, the DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) conducted 78 assessments of control system entities which helped companies identify security gaps and prioritize mitigations. We also empower owners and operators to help themselves by providing a cyber self-evaluation tool, which was utilized by over 1,000 companies last year, as well as in-person and on-line training sessions.

In addition, DHS S&T works collaboratively across federal agencies, private industry, academic networks and institutions, and global information technology owners and operators to research, develop, test, and transition deployable solutions to secure the nation's current and future cyber and critical infrastructures. For example, S&T is partnering with the Financial Services Sector Coordinating Council (FSSCC) to provide identity proofing solutions at financial institutions in order to reduce identity impersonation. The Financial Institution- Verification of Identity Credential Service (FI-VICS) effort is focused on creating a single interface from financial institutions to authoritative identity credential issuers (such as state Department of Motor Vehicles) to provide required authentication and authorizations between the financial institution requester and government identity credential issuer.

To combat cyber crime, DHS works with the Federal Bureau of Investigation and leverages the skills and resources of the U.S. Secret Service, ICE, and CBP to support prosecutions of cyber criminals brought by the Department of Justice. In Fiscal Year 2011 alone, DHS prevented $1.5 billion in potential losses through cyber crime investigations, resulting in prosecutors bringing charges against 72 individuals for their alleged participation in an international criminal network

that sought the sexual abuse of children and the creation and dissemination of graphic images and videos of child sexual abuse throughout the world.

DHS also serves as a focal point for national cybersecurity outreach, cyber awareness, and workforce development efforts. Raising the cyber education and awareness of the general public creates a more secure environment in which the personal or financial information of individuals is better protected. DHS recognizes that partnership and collaboration are crucial to ensuring that all Americans take responsibility for their actions online. To that end, we are continuing to grow the Department's ***Stop.Think.Connect.™*** Campaign, which is a year-round national public awareness effort designed to engage and challenge Americans to join the effort to practice and promote safe online practices.

As we perform this work, we are mindful that one of our missions is to ensure that privacy, confidentiality, and civil liberties are not diminished by our efforts. The Department has implemented strong privacy and civil rights and civil liberties standards into all its cybersecurity programs and initiatives from the outset to ensure the highest standards of transparency and accountability. DHS has performed Privacy Impact Assessments (PIAs) of our key cybersecurity programs such as EINSTEIN, which provides intrusion detection capabilities to the civilian federal agencies. DHS also receives regular counsel on cybersecurity activities from the Data Privacy and Integrity Advisory Committee (DPIAC), a body of outside experts who advise the Department on ways to address privacy and civil liberties concerns. This year, US-CERT and CRCL also launched a training effort for all US-CERT personnel focused on identifying and preventing civil rights and civil liberties issues in US-CERT's cybersecurity activities.

The Department of Defense is a key partner in our cybersecurity mission. In 2010, I signed a Memorandum of Understanding with then-Secretary of Defense Robert Gates to formalize the interaction between DHS and DOD to protect against threats to our critical civilian and military computer systems and networks. Congress mirrored this division of responsibilities in the National Defense Authorization Act for Fiscal Year 2012. We are currently working with the Defense Industrial Base as well as other critical infrastructure sectors, such as the Banking and Finance Sector, to exchange actionable information about malicious activity.

While the Administration has taken significant steps to protect against evolving cyber threats, we must acknowledge that the current threat outpaces our current authorities. DHS executes its portion of the cybersecurity mission under an amalgam of existing statutory and executive authorities that fail to keep up with the responsibilities with which we are charged. Our cybersecurity efforts have made clear that our nation cannot improve its ability to defend against cyber threats unless certain laws that govern cybersecurity activities are updated.

In May 2011, the Obama Administration provided a pragmatic and focused cybersecurity legislative proposal for Congress to consider. We believe this proposal, as well as the Cybersecurity Act of 2012, provide important steps in improving the cybersecurity posture of the United States. I hope that the current legislative debate maintains the bipartisan tenor it has benefitted from so far, and builds from the consensus that spans two Administrations and Congress' efforts of the last several years.

All sides agree that federal and private networks must be better protected, and information about cybersecurity threats should be shared more easily while ensuring that privacy and civil liberties are protected through a customized framework of information handling policies and oversight. Both the Administration's proposal and the bi-partisan Cybersecurity Act of 2012 currently before the Senate would improve operations in those areas by providing DHS with clear statutory authority commensurate with our cybersecurity responsibilities, although the Administration would still like to discuss certain concerns with specific parts of the Cybersecurity Act of 2012.

In addition, many agree with the House Republican Cyber Task Force when it said, "Congress should consider carefully targeted directives for limited regulation of particular critical infrastructures to advance the protection of cybersecurity." Both the Administration's proposal and the Senate legislation recognize the severity and urgency to secure critical infrastructure and take some basic steps in this area.

Accordingly, the Administration has proposed risk mitigation guidance to ensure that companies providing the Nation's most essential services are instituting a baseline level of cybersecurity. This proposal would leverage the expertise of the private sector requiring the Nation's most critical infrastructure adopt the cybersecurity practices, technologies, and performance standards that work best on their networks.

There is also broad support for increasing the penalties for cyber crimes and for creating a uniform data breach reporting regime to protect consumers. The Administration's proposal will help protect the American people by enhancing our ability to prosecute cyber criminals and by establishing national standards requiring businesses that have suffered an intrusion to notify affected individuals if the intruder had access to the consumers' personal information.

I believe we have made great progress toward reaching a consensus that will help protect the American people, Federal government networks and systems, and our Nation's critical infrastructure. The time to act is now: to improve cybersecurity coordination, strengthen our cybersecurity posture, and protect all elements of our economy against this serious and growing threat, while protecting privacy, confidentiality, and civil liberties.

Conclusion

We have come a long way over the past year, and in the ten years since 9/11, to enhance protection of the United States and engage our full range of partners in this shared responsibility. Together, we have made significant progress to better secure our country, but we are aware of the challenges that remain.

Threats against our nation, whether by terrorism or otherwise, continue to exist and evolve. And DHS must continue to evolve as well. We continue to be ever vigilant to protect against terrorist attacks while promoting the movement of goods and people and protecting our essential rights and liberties.

I thank the Committee for your continued partnership and guidance as together we work to keep our nation safe. I look forward to your questions.

Assistant Secretary of Legislative Affairs
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

April 24, 2012

The Honorable Jon Kyl
United States Senate
Washington, DC 20510

Dear Senator Kyl:

Thank you for your recent letter regarding policies enacted by local law enforcement jurisdictions that undermine enforcement of federal immigration laws. Specifically, you expressed concern with the Ordinance passed by the Cook County Board of Commissioners on September 7, 2011, entitled "Policy for Responding to ICE [U.S. Immigration and Customs Enforcement] Detainers" (the Ordinance). The Ordinance directs the Sheriff of Cook County to disregard immigration detainers, bars ICE officials from County facilities when enforcing immigration laws, and prohibits County personnel from responding to ICE inquiries. The Department of Homeland Security (DHS) shares your concern that this ordinance undermines public safety and hinders ICE's ability to enforce the Nation's immigration laws and appreciates the opportunity to describe the actions it has taken to resolve this issue.

ICE initially engaged Cook County officials at the local level, explaining that jurisdictions that ignore ICE detainers risk exposing their communities to public safety risks from suspected sex offenders, weapons violators, drunk drivers, and other violent criminals. Because of the gravity of these concerns, ICE requested that the Cook County Board of Commissioners amend the Ordinance to avoid any legal conflict with federal law and to restore sensible cooperation between Cook County and ICE, especially when it comes to identifying and removing criminal aliens incarcerated in Cook County jails.

Subsequently, as you know, ICE Director John Morton sent letters to Toni Preckwinkle, Cook County Board President, on January 4, 2012 and February 13, 2012, expressing ICE's concern and indicating ICE's commitment to work with the County to mitigate costs associated with ICE detainers. In his second letter, among other proposals, Director Morton offered to reimburse the county for expenses incurred as a result of holding individuals on ICE detainers. Ms. Preckwinkle has not meaningfully responded to Director Morton's offer.

Since the Ordinance was enacted on September 7, 2011, ICE has lodged detainers against more than 432 removable aliens in Cook County's custody who have been charged with or convicted of a crime, including serious and violent offenses. Cook County has not honored any of these 432 detainers. This has prevented ICE from considering removal proceedings against all but 38 of these individuals whom ICE had to locate independently and arrest following their release into the community. The potential gravity of Cook County's actions is highlighted in very real terms in a recent *Chicago Tribune* article concerning the case of Saul Chavez, an alien who was charged with killing a pedestrian while driving intoxicated. Mr. Chavez fled Cook County after being released on bond, despite an ICE detainer that had been lodged.

In addition to undermining local public safety, the Ordinance may also violate federal law. The *Immigration and Nationality Act* provides that a "local government entity may not prohibit, or in any way restrict, any government entity or official from sending to, or receiving from, [ICE] information regarding the citizenship or immigration status, lawful or unlawful, of any individual." *See* 8 U.S.C. § 1373(a). This provision is designed to ensure that ICE's ability to enforce immigration law in our communities is not unduly obstructed by state or local laws or policies. The Ordinance nevertheless prohibits County personnel from responding to ICE inquiries or communicating with ICE regarding an individual's incarceration status or release date.

In addition to engaging Cook County officials directly, ICE has noted that the Ordinance inhibits ICE's ability to validate Cook County's annual request for State Criminal Alien Assistance Program (SCAAP) funding. Under the auspices of SCAAP, the Federal Government, through DOJ, reimbursed Cook County nearly $3.4 million in 2010 and nearly $4.4 million in 2009 for the cost of detaining criminal aliens in Cook County detention facilities. In administering SCAAP, DOJ requires DHS to verify the immigration status of inmates for whom state and local agencies seek reimbursement. Without access to the Cook County jails, ICE's ability to accurately verify the immigration status of criminal aliens detained by Cook County becomes more difficult and may result in a denial of reimbursement to the State for costs of incarcerating criminal aliens under SCAAP. Moreover, it is fundamentally inconsistent for Cook County to request federal reimbursement for the cost of detaining aliens who commit or are charged with crimes while at the same time thwarting ICE's efforts to remove those very same aliens from the United States.

Additionally, in your January 30 letter, you asked DHS to advise you on whether DHS and ICE will take steps to activate Secure Communities in Cook County earlier than previously planned. As you may be aware, Secure Communities is currently active in 26 jurisdictions in Illinois and ICE is currently executing activations scheduled for Fiscal Year (FY) 2012 with nationwide activation, including all remaining Illinois jurisdictions, to be completed in FY 2013.

DHS and ICE are committed to ensuring the safety of American communities and will continue to consider all options, both financial and legal, to encourage Cook County officials to honor ICE detainers. The Senators who co-signed your letter will receive separate, identical responses.

Thank you again for your letters. Should you wish to discuss this further, please do not hesitate to contact me at (202) 447-5890.

Respectfully,

Nelson Peacock
Assistant Secretary for Legislative Affairs

cc: The Honorable Ronald Weich
Assistant Attorney General for Legislative Affairs

○